

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНОВ РОССИИ (ИБРР-2013)

VIII САНКТ-ПЕТЕРБУРГСКАЯ МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ

Санкт-Петербург, 23-25 октября 2013 г.

МАТЕРИАЛЫ КОНФЕРЕНЦИИ

Санкт-Петербург
2013



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНОВ РОССИИ (ИБРР-2013)

VIII САНКТ-ПЕТЕРБУРГСКАЯ МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ

Санкт-Петербург, 23-25 октября 2013 г.

МАТЕРИАЛЫ КОНФЕРЕНЦИИ

Санкт-Петербург

2013

http://spoisu.ru

УДК (002:681):338.98

И 74

И 74 **Информационная** безопасность регионов России (ИБРР-2013). VIII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 23-25 октября 2013 г.: Материалы конференции / СПОИСУ. – СПб., 2013. – 293 с.
ISBN 978-5-906555-02-1

Сборник охватывает широкий круг направлений: Государственная политика обеспечения информационной безопасности регионов России, Правовые аспекты информационной безопасности, Безопасность информационных технологий, Современные средства защиты информации, Информационная безопасность телекоммуникационных сетей, Информационная безопасность в критических инфраструктурах, Информационно-экономическая безопасность, Информационная безопасность в гидрометеорологии, Информационная безопасность в экологии, Информационная безопасность в социокомпьютинге, Подготовка и переподготовка кадров в области обеспечения информационной безопасности, а также включает материалы Круглого стола «Информационная безопасность – информационная культура XXI века» и Молодежной научной школы «Безопасные информационные технологии».

Предназначен для широкого круга руководителей, представителей органов государственной власти, научных работников и специалистов, занимающихся вопросами сохранения и развития единого защищенного информационного пространства России, обеспечения безопасности и эффективности использования региональных информационных ресурсов, защиты информации в региональных информационных и телекоммуникационных системах, подготовки и переподготовки кадров в области обеспечения информационной безопасности.

УДК (002:681):338.98

Редакционная коллегия: *Б.Я. Советов, Р.М. Юсупов, В.П. Заболотский, В.В. Касаткин*
Компьютерная верстка: *А.С. Михайлова, Л.Н. Федорченко*

Публикуется в авторской редакции

Подписано в печать 25.09.2013. Формат 60x84⅛. Бумага офсетная.
Печать – ризография. Усл. печ. л. 34,1. Тираж 500 экз. Заказ № 4231
Отпечатано в ООО «К-8»
190005, Санкт-Петербург, Измайловский пр., 18-д

ISBN 978-5-906555-02-1

© Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления (СПОИСУ), 2013 г.
© Авторы, 2013 г.



INFORMATION SECURITY OF RUSSIAN REGIONS (ISRR-2013)

VIII ST. PETERSBURG INTERREGIONAL CONFERENCE

St. Petersburg, October 23-25, 2013

PROCEEDINGS OF THE CONFERENCE

St. Petersburg

2013

http://spoisu.ru



УЧРЕДИТЕЛИ КОНФЕРЕНЦИИ «ИБРР-2013»

- Правительство Санкт-Петербурга
- Законодательное Собрание Санкт-Петербурга
- Правительство Ленинградской области
- Министерство связи и массовых коммуникаций Российской Федерации
- Министерство образования и науки Российской Федерации
- Российская академия образования
- Отделение нанотехнологий и информационных технологий РАН
- Санкт-Петербургский научный Центр РАН
- Санкт-Петербургский институт информатики и автоматизации РАН
- Санкт-Петербургская территориальная группа Российского национального комитета по автоматическому управлению
- Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления

СОУСТРОИТЕЛИ КОНФЕРЕНЦИИ «ИБРР-2013»

- Российский фонд фундаментальных исследований
- СПб ГУП «Санкт-Петербургский информационно-аналитический центр»
- Санкт-Петербургский филиал «Ленинградское отделение Центрального научно-исследовательского института связи»
- ФГУП «НИИ «Рубин»
- ФГУП «ЦентрИнформ»
- ЗАО «Ассоциация специалистов информационных систем»
- ЗАО «Институт инфотелекоммуникаций»
- ЗАО «Институт телекоммуникаций»
- ЗАО «Метроком»
- ЗАО «Научно-технический центр биоинформатики и телемедицины «Фрактал»
- ЗАО «ТЕЛРОС»
- ОАО «Научно-производственное объединение «Импульс»
- ОАО «Северо-Западный Телеком»
- ОАО «Центр компьютерных разработок»
- ООО «Геонавигатор»
- ООО «ИнТехСервис»
- ООО «Компания «Марвел»
- ООО «Лаборатория инфокоммуникационных сетей»
- Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова
- Государственный университет морского и речного флота имени адмирала С.О. Макарова
- Петербургский государственный университет путей сообщения
- Санкт-Петербургский государственный политехнический университет
- Санкт-Петербургский государственный университет аэрокосмического приборостроения
- Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
- Санкт-Петербургский государственный университет технологии и дизайна
- Санкт-Петербургский государственный экономический университет
- Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
- Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
- Санкт-Петербургский университет МВД России
- Партнерство для развития информационного общества на Северо-Западе России
- Северо-западное отделение Российской академии образования
- Санкт-Петербургская инженерная академия
- Санкт-Петербургское отделение Академии информатизации образования
- Санкт-Петербургское отделение Международной академии информатизации

КООРДИНАЦИОННЫЙ СОВЕТ КОНФЕРЕНЦИИ «ИБРР-2013»

Полтавченко Георгий Сергеевич	Губернатор Санкт-Петербурга
Макаров Вячеслав Серафимович	Председатель Законодательного собрания Санкт-Петербурга
Дрозденко Александр Юрьевич	Губернатор Ленинградской области
Никандров Николай Дмитриевич	Президент Российской академии образования
Алферов Жорес Иванович	Вице-президент РАН, Председатель Президиума Санкт-Петербургского научного Центра РАН, Лауреат Нобелевской премии
Балыбердин Александр Леонидович	Заместитель директора Административного департамента аппарата Правительства Российской Федерации
Велихов Евгений Павлович	Академик-секретарь Отделения нанотехнологий и информационных технологий РАН
Ливанов Дмитрий Викторович	Министр образования и науки Российской Федерации
Никифоров Николай Анатольевич	Министр информационных технологий и связи Российской Федерации
Сергеев Алексей Иванович	Генеральный секретарь Совета Межпарламентской Ассамблеи государств – участников Содружества Независимых Государств
Федоров Александр Вячеславович	Заместитель председателя Следственного Комитета России

ПРЕЗИДИУМ КОНФЕРЕНЦИИ «ИБРР-2013»

Советов Борис Яковлевич	Председатель Президиума, сопредседатель Научного совета по информатизации Санкт-Петербурга
Юсупов Рафаэль Мидхатович	Председатель Организационного Комитета, директор Санкт-Петербургского института информатики и автоматизации РАН
Дивинский Игорь Борисович	Вице-губернатор Санкт-Петербурга - руководитель Администрации Губернатора Санкт-Петербурга
Громов Иван Александрович	Председатель Комитета по информатизации и связи Санкт-Петербурга
Максимов Андрей Станиславович	Председатель Комитета по науке и высшей школе Санкт-Петербурга
Демидов Александр Алексеевич	Председатель Комитета по телекоммуникациям и информатизации Ленинградской области
Васильев Владимир Николаевич	Председатель Совета ректоров Санкт-Петербурга, ректор Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики
Кучерявый Михаил Михайлович	Руководитель Управления Федеральной службы технического и экспортного контроля по Северо-Западному федеральному округу
Лопота Виталий Александрович	Президент – генеральный конструктор Ракетно-космической корпорации «Энергия» им. С.П. Королева
Пешехонов Владимир Григорьевич	Генеральный директор ГНЦ «Центральный научно-исследовательский институт «Электроприбор»
Шульц Владимир Леопольдович	Заместитель президента РАН

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ КОНФЕРЕНЦИИ «ИБРР-2013»

Председатель Организационного Комитета

Юсупов Рафаэль Мидхатович	Директор Санкт-Петербургского института информатики и автоматизации РАН

Заместитель председателя Организационного Комитета

Майоров Владимир Владимирович	Начальник Управления информационной безопасности и технической защиты информации Комитета по информатизации и связи Санкт-Петербурга

Члены Организационного Комитета

Александров Анатолий Михайлович	Заместитель начальника Центра анализа и экспертизы ОАО «Научно-производственное объединение «Импульс»
Андронова Ольга Олеговна	Главный редактор газеты «Компьютер Информ»
Бачевский Сергей Викторович	Ректор Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
Барышников Сергей Олегович	Ректор Государственного университета морского и речного флота имени адмирала С.О. Макарова
Блажис Анатолий Константинович	Генеральный директор ЗАО «Научно-технический центр биоинформатики и телемедицины «Фрактал»
Богданов Владимир Николаевич	Директор ФГУП «ЦентрИнформ»
Борисов Николай Валентинович	Директор Междисциплинарного центра Санкт-Петербургского государственного университета
Вус Михаил Александрович	Старший научный сотрудник Санкт-Петербургского института информатики и автоматизации РАН
Гирдин Сергей Алексеевич	Президент ООО «Компания «Марвел»
Григорьев Владимир Александрович	Заведующий кафедрой беспроводных телекоммуникаций Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, генеральный директор ООО «Лаборатория инфокоммуникационных сетей»
Гоголь Александр Александрович	Советник ректора, заведующий кафедрой Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
Гусаров Александр Анатольевич	Генеральный директор ЗАО «ТЕЛРОС»
Гуца Анатолий Григорьевич	Главный специалист СПб ГУП «Санкт-Петербургский информационно-аналитический центр»
Давыдов Евгений Борисович	Главный конструктор ФГУП «НИИ «Масштаб»
Демидов Алексей Вячеславович	Ректор Санкт-Петербургского государственного университета технологии и дизайна
Долгирев Валерий Алексеевич	Помощник директора Санкт-Петербургского института информатики и автоматизации РАН по защите информации
Жданов Сергей Николаевич	Заместитель генерального директора ЗАО «ВТБ-Девелопмент»
Жигадло Валентин Эдуардович	Заместитель генерального директора по развитию ЗАО «Институт телекоммуникаций»
Заборовский Владимир Сергеевич	Заведующий кафедрой телематики Санкт-Петербургского государственного политехнического университета
Захаров Юрий Никитич	Первый заместитель директора СПб ГУП «Санкт-Петербургский информационно-аналитический центр»
Зегжда Петр Дмитриевич	Директор Специализированного центра защиты информации, заведующий кафедрой информационной безопасности компьютерных систем Санкт-Петербургского государственного политехнического университета
Зубков Юрий Сергеевич	Действительный государственный советник Санкт-Петербурга 3 класса

Идрисов Рустам Фидайович	Заместитель директора Центра исследований проблем безопасности РАН
Ипатов Олег Сергеевич	Заведующий кафедрой Балтийского государственного технического университета «ВОЕНМЕХ» им. Д.Ф. Устинова
Искандеров Юрий Марсович	Заместитель директора ЗАО «Институт проблем транспорта им. Н.С. Соломенко РАН»
Касаткин Виктор Викторович	Ученый секретарь Научного совета по информатизации Санкт-Петербурга, декан ФПК Балтийского государственного технического университета «ВОЕНМЕХ» им. Д.Ф. Устинова
Кирсанов Игорь Петрович	Генеральный директор ЗАО «ВО «РЕСТЭК»
Корабельников Евгений Владимирович	Директор СПб ГУП «Санкт-Петербургский информационно-аналитический центр»
Коршунов Сергей Валерьевич	Заместитель председателя Совета УМО вузов России, проректор по учебной работе Московского государственного технического университета им. Н.Э. Баумана
Кузичкин Александр Васильевич	Заместитель директора ФГУП «Научно-исследовательский институт телевидения»
Кузьмин Юрий Григорьевич	Ученый секретарь Санкт-Петербургского Общества информатики, вычислительной техники, систем связи и управления
Кутузов Владимир Михайлович	Ректор Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина)
Максимцев Игорь Анатольевич	Ректор Санкт-Петербургского государственного экономического университета
Марков Вячеслав Сергеевич	Ученый секретарь Объединенного научного совета Санкт-Петербургского Научного центра РАН
Михайлов Николай Семенович	Технический директор Санкт-Петербургского Общества информатики, вычислительной техники, систем связи и управления
Михайлова Анна Сергеевна	Заместитель директора по связям с общественностью Санкт-Петербургского Общества информатики, вычислительной техники, систем связи и управления
Молдовян Александр Андреевич	Заместитель директора Санкт-Петербургского института информатики и автоматизации РАН по информационной безопасности
Николаев Алексей Юрьевич	Генеральный директор ЗАО «Эврика»
Оводенко Анатолий Аркадьевич	Ректор Санкт-Петербургского государственного университета аэрокосмического приборостроения
Осадчий Александр Иванович	Директор Санкт-Петербургского филиала «Ленинградское отделение Центрального научно-исследовательского института связи»
Остапенко Александр Николаевич	Генеральный директор ЗАО «Лаборатория противодействия промышленному шпионажу»
Панычев Александр Юрьевич	Ректор Петербургского государственного университета путей сообщения
Перепелица Сергей Николаевич	Генеральный директор ООО «ИнТехСервис»
Присяжнюк Сергей Прокофьевич	Генеральный директор ЗАО «Институт телекоммуникаций»
Пухов Геннадий Георгиевич	Директор ООО «Геонавигатор»
Рунеев Анатолий Юрьевич	Генеральный директор ФГУП «Научно-исследовательский институт «Рубин»
Симонов Михаил Владимирович	Главный консультант директора ФГУП «ЦентрИнформ»
Солодянников Александр Владимирович	Генеральный директор ЗАО «Ассоциация специалистов информационных систем»
Терещенко Павел Геннадьевич	Заместитель генерального директора ФГБУ «Президентская библиотека им. Б.Н. Ельцина»
Тихомиров Сергей Григорьевич	Генеральный директор ОАО «Центр компьютерных разработок»

Ткач Анатолий Федорович	Заместитель директора Санкт-Петербургского института информатики и автоматизации РАН
Устинов Игорь Анатольевич	Генеральный директор ОАО «Научно-производственное объединение «Импульс»
Уткин Виктор Викторович	Директор Центра информационных технологий управления и электронных услуг Санкт-Петербургского государственного экономического университета
Федорченко Людмила Николаевна	Старший научный сотрудник Санкт-Петербургского института информатики и автоматизации РАН
Цыулев Сергей Валентинович	Главный специалист Отдела информационно-компьютерной безопасности Комитета по информатизации и связи
Черешкин Дмитрий Семенович	Заведующий лабораторией Института системного анализа РАН
Чугунов Андрей Владимирович	Заведующий кафедрой управления государственными информационными системами, директор Центра технологий электронного правительства Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики
Шерстюк Юрий Михайлович	Генеральный директор ЗАО «Институт инфотелекоммуникаций»

ПРОГРАММНЫЙ КОМИТЕТ КОНФЕРЕНЦИИ «ИБРР-2013»

Председатель Программного Комитета

Советов Борис Яковлевич	Сопредседатель Научного совета по информатизации Санкт-Петербурга

Заместители председателя Программного Комитета

Жигадло Валентин Эдуардович	Заместитель генерального директора по развитию ЗАО «Институт телекоммуникаций»
Молдовян Александр Андреевич	Заместитель директора Санкт-Петербургского института информатики и автоматизации РАН по информационной безопасности

Члены Программного Комитета

Берекет Виктор Максимович	Генерал-майор полиции, заместитель начальника Санкт-Петербургского университета МВД России по научной работе, кандидат юридических наук, доцент
Бродовская Елена Викторовна	Руководитель Центра киберполитики и прикладных политических исследований, заведующая кафедрой политологии Института гуманитарных технологий в сфере социального компьютинга Московского государственного гуманитарного университета им. М.А. Шолохова, доктор политических наук, доцент
Бузников Анатолий Алексеевич	Профессор кафедры квантовой электроники и оптико-электронных приборов Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), доктор технических наук, профессор, заслуженный деятель науки РФ
Воробьев Владимир Иванович	Заведующий лабораторией информационно-вычислительных систем Санкт-Петербургского института информатики и автоматизации РАН, доктор технических наук, профессор
Вус Михаил Александрович	Старший научный сотрудник Санкт-Петербургского института информатики и автоматизации РАН, кандидат технических наук, дважды лауреат Премии Правительства России в области образования
Горохов Владимир Леонидович	Профессор кафедры безопасности жизнедеятельности Санкт-Петербургского государственного архитектурно-строительного университета, доктор технических наук, профессор

Домбровская Лариса Александровна	Профессор кафедры математики и информатики Санкт-Петербургского университета МВД России, кандидат педагогических наук, доцент
Жигадло Валентин Эдуардович	Заместитель генерального директора по развитию ЗАО «Институт телекоммуникаций», доктор технических наук, доцент
Зегжда Петр Дмитриевич	Директор Специализированного центра защиты информации, заведующий кафедрой информационной безопасности компьютерных систем Санкт-Петербургского государственного политехнического университета, доктор технических наук, профессор
Зикратов Игорь Алексеевич	Заведующий кафедрой «Безопасные информационные технологии» Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, доктор технических наук, профессор
Игумнов Владимир Вячеславович	Первый заместитель генерального директора, главный конструктор ОАО «Научно-производственное объединение «Импульс», кандидат технических наук
Кий Андрей Вячеславович	Старший преподаватель кафедры Военной академии связи им. С.М. Буденного, кандидат технических наук
Колбанёв Михаил Олегович	Профессор Санкт-Петербургского государственного экономического университета, доктор технических наук, профессор
Коноплев Георгий Асадович	Доцент кафедры квантовой электроники и оптико-электронных приборов Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), кандидат технических наук, доцент
Котенко Игорь Витальевич	Заведующий лабораторией проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук, доктор технических наук, профессор
Краснова Анастасия Ивановна	Доцент кафедры информационно-измерительных систем и технологий Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), кандидат технических наук, доцент
Крук Евгений Аврамович	Директор Института информационных систем и защиты информации Санкт-Петербургского государственного университета аэрокосмического приборостроения, доктор технических наук, профессор, лауреат премии Правительства Санкт-Петербурга, заслуженный деятель науки РФ
Кучерявый Михаил Михайлович	Руководитель Управления Федеральной службы технического и экспортного контроля по Северо-Западному федеральному округу, кандидат политических наук
Левкин Игорь Михайлович	Профессор Санкт-Петербургского государственного экономического университета, доктор военных наук, профессор
Майоров Владимир Владимирович	Начальник Управления информационной безопасности и технической защиты информации Комитета по информатизации и связи
Микадзе Сергей Юрьевич	Проректор Санкт-Петербургского государственного экономического университета, кандидат экономических наук, доцент
Митько Арсений Валерьевич	Доцент кафедры морских информационных систем Российского государственного гидрометеорологического университета, председатель Совета молодых учёных Севера Арктической общественной академии наук, кандидат технических наук, доцент

Митько Валерий Брониславович	Профессор кафедры морских информационных систем Российского государственного гидрометеорологического университета, председатель Санкт-Петербургского отделения секции геополитики и безопасности Российской академии естественных наук, президент Арктической общественной академии наук, доктор технических наук, профессор
Молдовян Николай Андреевич	Заведующий лабораторией криптологии Санкт-Петербургского института информатики и автоматизации РАН, доктор технических наук, профессор, заслуженный изобретатель РФ
Ныркov Анатолий Павлович	Заведующий кафедрой комплексного обеспечения информационной безопасности Государственного университета морского и речного флота имени адмирала С.О. Макарова, доктор технических наук, профессор
Овчинников Андрей Анатольевич	Доцент кафедры «Безопасность информационных систем» Санкт-Петербургского государственного университета аэрокосмического приборостроения, кандидат технических наук, доцент
Паращук Игорь Борисович	Начальник кафедры Военной академии связи им. С.М. Буденного, доктор технических наук, профессор
Попов Николай Николаевич	Аспирант кафедры морских информационных систем Российского государственного гидрометеорологического университета
Примакин Алексей Иванович	Полковник полиции, начальник кафедры специальных информационных технологий Санкт-Петербургского университета МВД России, доктор технических наук, профессор
Путилин Алексей Николаевич	Заместитель главного конструктора ОАО «Научно-производственное объединение «Импульс», доктор технических наук, профессор
Татарникова Татьяна Михайловна	Профессор Санкт-Петербургского государственного экономического университета, доктор технических наук, доцент
Трофимов Валерий Владимирович	Заведующий кафедрой информатики Санкт-Петербургского государственного экономического университета, заслуженный деятель науки РФ, доктор технических наук, профессор
Тулупьев Александр Львович	Заведующий лабораторией теоретических и междисциплинарных проблем информатики Санкт-Петербургского института информатики и автоматизации РАН, доктор физико-математических наук, доцент
Азаров Артур Александрович,	Младший научный сотрудник Санкт-Петербургского института информатики и автоматизации РАН
Устинов Игорь Анатольевич	Генеральный директор ОАО «Научно-производственное объединение «Импульс», кандидат технических наук
Цехановский Владислав Владимирович	Заведующий кафедрой «Автоматизированные системы обработки информации и управления» Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), кандидат технических наук, доцент
Цыулёв Сергей Валентинович	Главный специалист Отдела информационно-компьютерной безопасности Комитета по информатизации и связи
Шишкин Владимир Михайлович	Старший научный сотрудник лаборатории информационно-вычислительных систем Санкт-Петербургского института информатики и автоматизации РАН, кандидат технических наук, доцент
Шкирятов Олег Тимофеевич	Первый заместитель генерального директора по научной работе Открытого акционерного общества «Научно-производственное объединение «Импульс»
Яковлева Наталья Александровна	Полковник полиции, начальник кафедры математики и информатики Санкт-Петербургского университета МВД России, кандидат психологических наук

Ученый секретарь Конференции

Заболотский Вадим Петрович	Руководитель научно-исследовательской группы Санкт-петербургского института информатики и автоматизации РАН

Исполнительный директор Конференции

Касаткин Виктор Викторович	Ученый секретарь Научного совета по информатизации Санкт-Петербурга, декан ФПК Балтийского государственного технического университета «ВОЕНМЕХ» им. Д.Ф. Устинова

Информационное обеспечение Конференции

«Компьютер Информ»	Газета о передовых инфокоммуникационных технологиях, продуктах, решениях для руководителей предприятий и организаций, отделов АСУ, ведущих специалистов и служб ИКТ, www.ci.ru

ГОСУДАРСТВЕННАЯ ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕГИОНОВ РОССИИ

Балыбердин А.Л., Вус М.А.
Россия, Москва, Административный департамент аппарата Правительства РФ,
Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

К ДВАДЦАТИЛЕТИЮ РОССИЙСКОГО ЗАКОНА «О ГОСУДАРСТВЕННОЙ ТАЙНЕ»

Два десятилетия назад, с принятием в нашей стране Закона «О государственной тайне», начался процесс формирования правовых основ защиты сведений, составляющих государственную тайну. Впервые в истории России вопросы ограничения информационного обмена, связанные с необходимостью обеспечения безопасности государства, стали регулироваться открытым нормативно-правовым актом. При этом создавалось не только базовое законодательство, но и формировалось новое представление об ответственности за его нарушение. Первый постатейный комментарий к только что принятому Закону, подготовленный его разработчиками, вышел в Санкт-Петербурге.

Как и любая проблема, решение которой связано с функционированием и развитием институтов власти, становление и развитие института секретности носит политический характер. В новой России тема государственной тайны изначально оказалась сильно политизированной и в известный период даже инспирировалась правозащитниками в качестве объекта внимания для Конституционного Суда. Конституционный Суд Российской Федерации своим постановлением определил: «Обязанность соблюдать законодательство о государственной тайне вытекает из общеправовой обязанности органов государственной власти, местного самоуправления, должностных лиц, граждан и их объединений соблюдать Конституцию Российской Федерации и её законы». Постановление Конституционного Суда (от 27.03.96 г. №8-П) было опубликовано в «Российская газете».

Принятый Верховным Советом в 1993 году Закон Российской Федерации «О государственной тайне», претерпев в 1997 году новую редакцию, действует и по настоящее время. Этот закон решил многие проблемы, которые вывел из сферы ведомственных закрытых актов в сферу открытого законодательного регулирования. Уже в первые годы после его принятия была разработана в своей основе нормативно-правовая база, необходимая для функционирования механизмов реализации закона. Это позволило в определенной мере заполнить сложившийся в 1991-1993 гг., спровоцированный вследствие разрушения старой, действовавшей ранее в стране системы защиты государственной тайны, правовой вакуум и приостановить нанесение ощутимого урона интересам государства.

Свидетельства имевших место в конце прошлого века в России прецедентов разграбления государственной тайны и ухода значительных её массивов за границу можно найти в средствах массовой информации.

Приводились такие примеры и в газете «Петербургский дневник». Так, например, «только в 1992-2000 годах в США было зарегистрировано более 1000 патентов на технологии военного и двойного назначения, где авторами являются российские изобретатели, а обладателями патентов и, следовательно, исключительных прав – иностранные юридические и физические лица» [№45(104) от 20 ноября 2006].

Общественная палата Российской Федерации, обратившая внимание на состояние дел с защитой объектов интеллектуальной собственности, отмечала, что «зачастую руководители юридически не подготовлены в вопросах интеллектуальной собственности — как своей собственной, так и государства».

В 1998 г. в Санкт-Петербурге, в Смольном при поддержке администрации города была проведена научно-практическая конференция «Пять лет российскому Закону «О государственной тайне», с приветствием к участникам которой обратился В.В. Путин (на тот период директор ФСБ России). Отметив в своем приветствии, что сам факт проведения конференции с подобной тематикой свидетельствует о возросшем понимании учеными, практиками и общественностью страны важности стоящих перед государством задач по защите секретов, В.В. Путин подчеркнул: «Всем нам необходимо, чтобы принимаемые меры в деле укрепления режима секретности в стране были юридически обоснованы, взвешены и разумны, точно соответствовали динамично изменяющейся

обстановке и не создавали при этом ненужных трудностей в деятельности предприятий, коммерческих организаций, воинских частей, не ущемляли законных прав и интересов граждан».

Участники конференции в своих выступлениях отмечали, что органы государственной власти повысили внимание к поиску путей сохранности защищаемой государством информации, и высказались в пользу необходимости создания специальной общегосударственной программы, которая позволила бы расширить действие мер предупредительного, профилактического характера. В рекомендациях конференции указывалось, в частности, на необходимость постановки определенной пропагандистской работы в вузах, направленной на обеспечение знания законов и других нормативных актов высших органов государственной власти в сфере обеспечения безопасности государства.

К 15-летию принятия Закона Российской Федерации «О государственной тайне» были приурочены состоявшиеся в Государственной Думе парламентские слушания на тему «Актуальные проблемы совершенствования законодательства о государственной тайне», ставшие своеобразным подведением итогов развития законодательства о государственной тайне в условиях постсоветской России. Участники слушаний подчеркнули, что принятие в Российской Федерации Закона «О государственной тайне» явилось ответом на вызов времени, а действующие правовые нормы в области защиты государственной тайны в целом создают условия для поддержания необходимого уровня безопасности Российской Федерации. В прозвучавших выступлениях отмечалось, что необходимость дальнейшего совершенствования законодательства и правового режима государственной тайны не вызывает сомнений, но это процесс весьма тонкий и деликатный. В принятых Рекомендациях парламентских слушаний намечена целая система мер по совершенствованию законодательства, связанного с защитой государственной тайны, по разным направлениям. Опубликовав материалы состоявшихся в Государственной Думе слушаний, их организаторы призвали к продолжению начатого серьёзного разговора.

По сообщениям официального сайта ФСБ России, на состоявшемся в мае сего года заседании Общественного совета при Федеральной службе безопасности Российской Федерации в ходе дискуссии выступающие отметили важность ведения «образовательно-просветительской работы для формирования культуры информационной безопасности и соответствующих навыков поведения в информационной сфере у пользователей».

Вус М.А., Макаров О.С.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
Беларуссия, Минск, ГУО «Институт национальной безопасности Республики Беларусь»

О РАЗРАБОТКЕ СТРАТЕГИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВ – УЧАСТНИКОВ СНГ

В современных условиях возрастает опасность совершения преступлений, возникновения кризисных ситуаций и иных противоправных действий с применением современных информационных технологий. Вследствие этого особую актуальность приобретают вопросы формирования активной согласованной информационной политики государств – участников СНГ, развития общего информационного пространства, создания совместного потенциала по отражению информационных угроз, обеспечения информационной безопасности, защиты информационных ресурсов и коммуникаций, национальных органов власти и управления государств-членов.

Проектом подготовленной к принятию на 39-м пленарном заседании МПА СНГ Межгосударственной программы совместных мер борьбы с преступностью предусматривается разработка «Стратегии информационной безопасности государств – участников Содружества Независимых Государств». Целью такого документа должно стать правовое закрепление концептуальных подходов к определению согласованных приоритетов обеспечения безопасности общественных отношений, складывающихся в информационной сфере, определение актуальных направлений обеспечения информационной безопасности, форм и методов ее обеспечения. Исполнителями работы определены Санкт-Петербургский институт информатики и автоматизации РАН, Институт государства и права РАН и ГУО «Институт национальной безопасности Республики Беларусь».

Основной целью обеспечения информационной безопасности является создание таких условий, при которых субъекты информационных отношений могли бы реализовывать свои интересы без постороннего деструктивного вмешательства. Специфика информационной сферы такова, что негативные последствия реализации угроз информационной безопасности проявляются в других сферах жизнедеятельности личности, общества и государства и влияют на безопасность государств – участников СНГ в политической, экономической и иных сферах. Складывающаяся система отношений по обеспечению информационной безопасности требует стратегического планирования в связи с их важностью для обеспечения национальной безопасности государств – участников СНГ, региональной и международной безопасности.

В информационной сфере формируется две различные категории интересов личности, общества и государства. Это общечеловеческие интересы (закреплены в Конституциях государств − участников СНГ), которые реализуются в информационной среде, в том числе посредством применения информационных технологий. Это также и специальные интересы, являющиеся средством достижения базовых общечеловеческих интересов (характерны только для информационной сферы – это могут быть, например, интерес к участию в информационном обмене, обеспечению безопасности информационной инфраструктуры и др.). Особенность концептуальной архитектуры информационной безопасности (интересы – угрозы – меры) состоит в том, что основные угрозы не направлены непосредственно на общечеловеческие интересы, а воздействуют на способы их реализации (то есть на специальные интересы).

В концептуальную основу построения Стратегии разработчики закладывают принцип «безопасность через развитие» и характеристику состояния информационной безопасность личности, общества и государства статусными стандартами безопасности. В качестве таких стандартов безопасности будут выступать интегрированные показатели индикаторов достижения совокупности интересов отдельно для личности, отдельно для общества и для государства. Так как общей угрозой информационной безопасности может считаться не достижение сформированных интересов или отставание в темпах приближения к ним, то в качестве одного из показателей информационной безопасности можно рассматривать стабильную динамику развития информационных средств реализации базовых интересов личности, общества и государства.

В рамках работы над проектом Стратегии предполагаются: выработка и согласование понятийного аппарата; обоснование основных интересов; построение матрицы глобальных угроз (целесообразно при этом исходить из градации на угрозы базовым интересам и угрозы способам их реализации в информационной сфере); определение механизмов противодействия угрозам.

Иванов В.П.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

НЕКОТОРЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ

Информационно-психологическая безопасность личности, социальной группы, общества, государства является составной частью системы информационной безопасности страны. Если не принимать во внимание различные аспекты реализации информационно-психологической безопасности работниками отдельных профессий (в том числе спортсменами), включая мероприятия по завершении работ, то в целом, вопросам информационно-психологической безопасности населения у нас уделяется мало внимания.

Рассмотрим, например, пропаганду как один из методов обеспечения информационно-психологической безопасности населения.

Можно констатировать, что единая государственная политика пропаганды, пронизывающая всю страну, у нас отсутствует как в целом по СМИ, так и по их отдельным составным структурам. Возьмем, к примеру, временной отрезок с начала мая до начала июля сего года. Значимые исторические события – День Победы в Великой войне и парад Победы – в СМИ в основном нашли отражение в репортажах с Красной площади. Телевизионные каналы, за исключением, пожалуй, канала «Звезда», крайне мало представляли материалы, прославляющие подвиг народа в Великой войне. В позднее вечернее время демонстрировались американские документальные фильмы о Второй мировой войне, искажающие события и принижающие победы нашего народа. Плюрализм? Нет, скорее всего, антипропаганда, или осознанная идеологическая диверсия. Отметим, что проявляющиеся порой всплески активности деструктивных сект различных религиозных конфессий также свидетельствуют о необходимости пересмотра легковесного отношения к проблемам информационного обмена и пропаганды.

Отдельные издания наших СМИ напоминают классические западные образцы «желтой прессы». Через СМИ делаются попытки внедрить в общественное сознание чуждые нам идеологические штампы и социокультурные ценности.

Отсутствие единой государственной политики пропаганды сильно сказывается в критические моменты жизни государства, в том числе во время чрезвычайных ситуаций, выборов, и во время осложнения международной обстановки. Вспомним события во время конфликта с Грузией.

Представляется целесообразным организовать централизованную службу информационного обмена и пропаганды в виде государственного комитета, председатель которого должен входить в Совет безопасности Российской Федерации, и подчиненные ему региональные комитеты. Их задачами являются: 1) анализ информации, циркулирующей в федеральных и региональных СМИ, на предмет соответствия Конституции РФ и федерального законодательства; 2) проведение единой государственной политики в этой сфере; 3) предоставление СМИ для публикации соответствующих материалов; 4) организация формирования информационных пакетов, отражающих интересы государства и общества; 5) предоставление Прокуратуре фактов нарушения Конституции и федерального законодательства отдельными СМИ с требованиями о пересмотре их лицензирования;

6) направлять деятельность СМИ в русло служения интересам России; 7) ведение контрпропаганды как внутри страны, так и на международной арене.

При необходимости потребуется введение в федеральное законодательство дополнительных статей, регламентирующих деятельность комитетов информационного обмена и пропаганды.

Игнатьев М.Б., Липинский Я.А., Ненашев В.А., Никитин А.В., Шепета А.П.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

КАК ОБУСТРОИТЬ ОКОЛОЗЕМНОЕ ПРОСТРАНСТВО ДЛЯ БОРЬБЫ С КОСМИЧЕСКИМИ УГРОЗАМИ

Издревле на нашу планету падали метеориты и астероиды, вызывая катастрофы планетарного масштаба. В связи с освоением космоса возникла новая угроза, созданная людьми, – космический мусор. В настоящее время на орбите Земли находятся свыше 600 тысяч объектов размером от одного сантиметра и больше. Благодаря высокой скорости перемещения эти объекты представляют серьезную опасность для спутников и пилотируемых экспедиций. Развитие цивилизации на нашей планете позволяет поставить вопрос о предотвращении космических угроз. Реализация таких проектов возможна лишь при условии обеспечения информационной безопасности. Вклад России в решение этой проблемы может быть весомым. Для того, чтобы консолидировать научно-технические силы вузов, академий и предприятий различных государств, как государственных, так и частных, необходимо организовать специальный международный проект по обустройству околоземного космического пространства для предупреждения и отражения космических угроз. Основные разделы такого проекта представлены в докладе.

1. В настоящее время известно около четырех сотен астероидов (АСЗ), орбиты которых опасно сближаются с орбитой Земли, с диаметрами от 40 километров до нескольких метров. Общее же число неоткрытых АСЗ может достичь по некоторым оценкам ста тысяч и более. Встреча Земли с одним из таких АСЗ может иметь катастрофические последствия различной степени. Наиболее тяжелые, глобальные и региональные катастрофы ожидаются от столкновения с АСЗ крупных и средних размеров от 100 метров до десятков километров и более. Обсуждаемая в печати стратегия астероидной защиты Земли носит пока отвлеченный характер. Основной акцент ставится на сбор информации о характеристиках наиболее опасных АСЗ с диаметрами более одного километра путем организации мониторинга с целью их обнаружения, отождествления и прогнозирования движения. В рамках международной программы астероидной опасности (Spaceguard Foundation) более 40 астрономических телескопов ведут регулярные наблюдения по обнаружению и отождествлению малых тел Солнечной системы, в том числе и АСЗ. Малоразмерные астероиды, составляющие главную реальную угрозу при их падении на Землю более многочисленны и менее изучены. Здесь, учитывая большую вероятность их столкновения с Землей, наряду с мониторингом основное значение имеет предотвращение столкновения путем отклонения или уничтожения АСЗ. В ряде работ обсуждаются вопросы создания систем защиты от астероидной опасности различного назначения, структуры, местоположения. Лунная база рассматривается как интересное место для расположения службы астероидной безопасности. В настоящее время США, Китай, Европа и Россия развертывают работы по началу освоения Луны.

http://www.universetoday.com/2007/02/27/nasa-reveals-a-sample-lunar-base/?1365

2. Прежде чем осуществлять реальное освоение Луны и астероидов, необходимо осуществить полномасштабное компьютерное моделирование различных вариантов с целью выбора наилучших. Технология виртуальных миров обеспечивает погружение человека в определенную среду (например, искусственно созданный трехмерный мир с шестью степенями свободы) и взаимодействие (интерактивность) человека с объектами и персонажами этого мира в реальном времени с использованием физических, физиологических и других характеристик человека. Во-первых, необходимое создание Всемирной виртуальной астрономической обсерватории для полного мониторинга околоземного пространства на основе сетевого объединения как профессиональных обсерваторий, так и любителей астрономии, вооруженных телескопами. Если профессиональных астрономических обсерваторий на Земле около ста, то любителей астрономии свыше ста тысяч и их помощь в наблюдении за околоземным пространством очень важна. Технология виртуальных миров в настоящее время – это развитая отрасль компьютерной науки и в докладе приводится перечень основных аспектов этой технологии применительно к задачам обустройства околоземного космического пространства с целью разработки многофункциональной интерактивной 3D модели околоземного космического пространства, представляющее взаиморасположение и поведение Земли, Луны, астероидов и спутников для индивидуального и группового исследования и демонстрации. Рассматриваются вопросы информационной безопасности технологии виртуальных миров.

3. В целом, Луну можно считать идеальным местом для решения многих современных и будущих научных программ. Реализация этих программ связана с созданием на Луне

долговременной базы, обеспечивающей работу обсерватории, оснащенной астрономическими и другими инструментами. С общих позиций, Луна является закономерным, неизбежным этапом освоения человечеством космического пространства. Динамика этого процесса определяется уровнем развития земной цивилизации, ее научного и технологического уровня. Прогнозы показывают, что начальная стадия освоения Луны автоматическими устройствами-роботами может быть реализована в ближайшие 10–15 лет. Дальнейшее расширение работ на Луне и создание обитаемой лунной базы (или баз) по широкому диапазону исследования Луны, с Луны и на Луне просматривается в перспективе ближайших 10–20 лет. Луна сама по себе выполняет важные функции по защите Земли от астероидов, притягивая часть астероидов и метеоритов на себя. Но одной Луны мало для выполнения этой функции. Представляется целесообразным отбуксировать несколько астероидов на лунную орбиту, распределив их равномерно по лунной орбите и тем самым создав как бы экран для отражения космических угроз в плоскости эклиптики.

Санкт-Петербургский государственный университет аэрокосмического приборостроения предлагает создать систему интерактивного трехмерного моделирования лунной базы и других космических объектов на основе технологии виртуальных миров для выработки проектных решений по различным объектам и системе машин для освоения Луны и для обустройства околоземного космического пространства.

4. Существует множество проектов по борьбе с астероидной опасностью. Один из таких проектов – гравитационный тягач. Идея этого проекта заключается в том, чтобы изменить траекторию движения астероида путем длительного гравитационного воздействия космического корабля, который должен находиться рядом с астероидом и тем самым изменять характеристики движения астероида. Для иллюстрации идеи гравитационного тягача нами создан его макет. Макет состоит из системы взаимодействующих тел, лазерного дальномера, блока управления, двигателя и солнечной батареи. В макете гравитационные воздействия моделируются магнитными взаимодействиями стального шара (модель астероида) и сильных постоянных магнитов на подвижном основании. Шар перемещается по круговому желобу. Принцип действия макета заключается в том, что с помощью лазерного дальномера измеряется расстояние от подвижного основания, где установлены постоянные магниты, до шара. С помощью блока управления и двигателя это расстояние удерживается с точностью 1 мм в диапазоне 20–40 мм и тем самым имитируется перемещение астероида под воздействием дополнительной гравитационной силы космического аппарата. Макет служит для лучшего понимания действия гравитационного тягача и может быть использован в образовательных целях.

5. Как показывают исследования, с большим астероидом диаметром свыше 10 км человечество на данном уровне развития цивилизации справиться не сможет и тогда большой катастрофы планетарного масштаба не избежать. Поэтому важны теоретические исследования по разработке новой картины мира. В настоящее время успешно функционирует международная космическая станция и реализуются многие международные космические проекты, но налаживание широкого международного сотрудничества по борьбе с космическими угрозами требует нового уровня международного взаимодействия.

Карамышев В.Е., Сичкарук А.В., Черешкин Д.С.
Россия, Москва, Институт системного анализа РАН

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОБЪЕКТОВ ПУТЕМ УПРАВЛЕНИЯ РИСКАМИ НАРУШЕНИЯ ТРЕБОВАНИЙ

Рассматриваются возможности реализации новой методологии обеспечение безопасности различных типов – информационной, технико-технологической, экологической и т.д. – для сложных объектов, основанной на управлении рисками нарушения нормативных требований, выполнение которых обеспечивает безопасность. Описывается разработанный в ИСА РАН инструментарий – аппаратно-программный комплекс «РискДетектор» и подробный алгоритм его использования для расчета рисков вероятности возникновения чрезвычайной ситуации на объекте и выработки рекомендаций по ее предупреждению.

В настоящее время большинство объектов всех видов инфраструктуры, экономики, социальной сферы и системы управления характеризуются постоянным повышением уровня сложности. Это связано с рядом факторов – усложнением процессов их функционирования, появлением новых взаимосвязей, широкомасштабным использованием различного вида автоматизированных человеко-машинных систем, ориентированных на автоматизацию выполняемых объектами действий, необходимостью постоянного повышения производительности и эффективности деятельности. Одновременно с увеличением сложности повышается и уровень опасности возникновения различных аварийных ситуаций, часто с непредсказуемым исходом. Другими словами – существенно повышается значимость обеспечения безопасности такого рода объектов. При этом возникает необходимость обеспечения безопасности в широком смысле – от возможности реализации широкого спектра потенциальных угроз нарушения нормального функционирования объекта. Это могут быть

угрозы технико-технологического, организационного, информационного, террористического и криминального характера, ошибки человека в системе, возмущения внешней среды, неэффективности кадровой политики, характера и т.д.

Соответственно, проблемы обеспечения безопасности приобретают системную значимость и требуют комплексного решения. Определение решений этих проблем осложняется рядом факторов, к которым относятся:

– за счет высокой сложности объектов существенно возрастает сложность создания и эксплуатации систем управления безопасностью, создаваемых на традиционной основе (формирование моделей, нахождение точных решений);

– возможности реализации угроз, потенциально способных оказать воздействие на объект имеют вероятностный характер; следовательно, система управления безопасностью должна уметь работать с вероятностями и случайными величинами;

– в настоящее время превалирует тенденция создания систем управления безопасностью, ориентированных только на один какой либо один тип безопасности, например, – информационную, транспортную и т.д.;

– отсутствует общая методология (и даже единая терминология), направленная на создание системы управления безопасностью, универсальной для любых типов безопасности.

В целом можно утверждать, что создать систему обеспечения безопасности (СОБ), которая обеспечивает полную, сто процентную безопасность объекта практически невозможно, а если идти по такому пути, то СОБ будет очень сложной, предельно дорогой и неработоспособной. Это утверждение основывается на мировом и отечественном опыте.

Следовательно, необходимо искать новые, нетрадиционные пути решения проблем обеспечения безопасности сложных объектов. Такой путь существует – переход на управление рисками возникновения ЧС за счет невыполнения комплекса нормативных требований или критериев обеспечения безопасности. В этом случае СОБ, на основании разнообразной информации, отслеживает невыполненные (полностью или частично) требования, рассчитывает риски возникновения ЧС по этой причине и определяет набор возможных решений – состав мер, способных парировать возможность реализации угроз – в точке невыполнения требований. Очевидно, что здесь величина риска рассматривается как значение вероятности возникновения ЧС при невыполнении нормативного требования в течении определенного времени.

Лепёхин А.Н.
Беларуссия, Минск, Академия МВД Республики Беларусь

ОБ ОТДЕЛЬНЫХ НАПРАВЛЕНИЯХ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Законодательство многих государств предусматривает ответственность за совершение правонарушений в информационной сфере либо, так называемых cybercrime. Причем количество и содержание таких состав различны и зависят от типа правовой системы, сложившегося порядка регулирования отношений в информационной сфере, а также принципов и подходов в уголовной политике государства. Вместе с тем, анализ правоприменительной практики по выявлению и последующему расследованию киберпреступлений показывает, что практически каждое серьезное преступление (имеющее либо большой общественный резонанс, либо причинившее существенный экономический и иной вред) совершенное в информационной сфере, имеет международный характер.

Такая связь прослеживается как в международном характере преступной деятельности (совершение преступления в группе гражданами различных государств) так и в наступлении преступного результата на территории другого государства либо нескольких. Очевидно, что данные обстоятельства обуславливают необходимость осуществления международного сотрудничества по борьбе с cybercrime. Поскольку эффективность мер уголовного воздействия к правонарушителям лежит не сколько в плоскости наличия и жесткости тех или иных правовых норм, сколько в реальной возможности реализации мер уголовного воздействия к конкретным лицам (преступникам). Данные обстоятельства обуславливают необходимость выработки действенных механизмов международного сотрудничества с таким социально опасным явлением (причем в международном масштабе) как киберпреступность.

Сложившаяся практика взаимодействия правоохранительных органов свидетельствует, что наиболее часто используемыми механизмами такого сотрудничества является оказание различной помощи в борьбе с преступностью в рамках международного организации уголовной полиции INTERPOL, а также взаимодействие в рамках различных региональных объединений, например Содружества независимых государств. В принципе, механизмы, выработанные в рамках данных организаций, могут использоваться (и используются) в борьбе с преступлениями в информационной сфере. Вместе с тем, представляется актуальным вопрос, об эффективности и

оперативности такого сотрудничества, а также содержания конкретных мер, направленных на предупреждение, раскрытие и последующее расследование криминальных деяний в данной сфере.

Следует отметить, что в настоящее время, в рамках Содружества независимых государств проводиться работа по выработке согласованных подходов к борьбе с киберпреступностью. И как, предполагается существенным этапом проведения такой работы является подписание Конвенции о сотрудничестве государств-участников СНГ в борьбе с преступлениями, совершаемыми с использованием информационных технологий. Полагаем, что разработка и принятие такого документа, является более чем своевременной.

Кроме вышеназванных элементов международно-правового механизма сотрудничества в сфере борьбы с преступлениями в информационной сфере, следует выделить еще один такой достаточно серьезный резерв, как взаимодействие в рамках групп CERT (групп реагирования на компьютерные инциденты либо чрезвычайные ситуации (в некоторых государствах)).

В настоящее время такие группы созданы уже в порядке 50 государств и, в том числе, в ряде государств – участников СНГ. Причем спецификой такого процесса является то, что в ряде государств такие группы созданы в составе различных государственных организации, а в ряде - являются общественными формированиями, что, безусловно, предопределяет особенности их деятельности и круг решаемых задач.

В общем виде основными задачами таких групп является:

– оказание консультативных услуг по вопросам обеспечения информационной безопасности;

– разработка рекомендаций пользователям в информационной сфере;

– оказание организационной помощи в предотвращении и анализе инцидентов сфере компьютерной безопасности;

– обмен информацией и учебными материалами с CERT других государств, а также с иными организациями.

– принятие превентивных мер в отношении компьютерных инцидентов;

– анализ источников инцидента;

– сотрудничество с провайдерами и иными заинтересованными организациями;

– организация проведения обучения, научных исследований и разработок в информационной сфере.

Анализ содержания задач, заявляемых такими группами, показывает, что нет единого похода к их постановке и соответственно решению. Более того, как уже отмечалось, в ряде государств такие группы имеют государственный статус соответственно имеют больший круг полномочий по реагированию на компьютерные инциденты. Вместе с тем, как представляется, использование такого достаточно мощного резерва в борьбе с информационными преступлениями, как создание и взаимодействие в рамках CERT, является одним условий успешности такой борьбы. Следует отметить, что в Республике Беларусь в настоящее время вопрос о создании такой группы и ее статусе только прорабатывается.

Таким образом, современные условия борьбы с киберпреступлениями требуют выработки согласованных подходов к организации такой борьбы и международного сотрудничества, осуществляемого в рамках как международных, так и региональных организаций.

Подкидышева В.Е.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

О РОССИЙСКО-КАЗАХСТАНСКОМ СОТРУДНИЧЕСТВЕ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Развитие информационного общества и глобализация информационного пространства неизбежно приводит к возникновению проблем, с которыми довольно сложно справиться в рамках одного государства. Кроме того, скорость развития информационных технологий в целом и широкий спектр задач, решаемых областью, приводит к возникновению всё новых направлений исследований. В свете этого как никогда актуальным становится вопрос межгосударственного сотрудничества, в частности, в научной сфере.

В Казахстане формируется обширная информационная инфраструктура, однако собственные меры по её защите пока не очень развиты. Для обеспечения безопасной работы с данными используются преимущественно российские и американские программные и аппаратные комплексы. В целях решения возможных проблем информационной безопасности, развития отрасли в целом, создания собственных систем и средств защиты информации в Казахстан привлекаются специалисты и учёные иностранных государств.

В сентябре текущего года в Научно-исследовательском институте информационной безопасности и криптологии ЕНУ им. Л.Н. Гумилева прошла I Международная научно-практическая конференция «Информационная безопасность в свете Стратегии «Казахстан – 2050». В работе конференции приняли участие и российские ученые. В их числе представители Института проблем информационной безопасности МГУ им. М.В. Ломоносова, Всероссийского научно-

исследовательского института проблем вычислительной техники и информатизации – базовой организации по СНГ в области информационной безопасности, Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики. Были представлены доклады учеными вузов Европы и США – Боннского Университета (Германия), Университета Тарту (Эстония), Advanced Technical Concepts, Berkshire (NY, USA). В конференции также приняли участие представители крупнейших IT-компаний Казахстана. Среди участников государственных структур – Управление делами Президента, подразделения КНБ РК (Академия КНБ, НИИ), подразделения информационной безопасности Министерства обороны и Министерства внутренних дел Республики Казахстан, а также государственной технической службы МТК. Гостем конференции был вице-президент McAfee EMEA Ян ван Влиет, прибывший из Нидерландов.

В докладах, представленных на конференции, обсуждался широкий круг аспектов в области информационной безопасности: от общих тенденций и актуальных проблем национальной и международной безопасности до конкретных решений отдельно взятых задач в таких областях, как криптология, робототехника и т.д. Поднимались вопросы о необходимости объединения науки с IT-отраслью и формирования на этой основе системы защиты информационной безопасности. В связи с этим были выдвинуты предложения по открытию специальной лаборатории и созданию организации по разработке антивирусных программ.

Особое внимание было уделено межгосударственному сотрудничеству в вопросе подготовки специалистов по информационной безопасности. Казахстанские высшие учебные заведения активно участвуют в программах обмена студентов и аспирантов, участвуют в конкурсах грантов и предоставляют возможность иностранных стажировок. Одним из итогов конференции стало заключение соглашения о сотрудничестве между Национальным Исследовательским Университетом ИТМО (Санкт-Петербург) и Евразийским Национальным Университетом им. Л.Н. Гумилёва (Астана).

Пономаренко А.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННОГО ОБЩЕСТВА РОССИИ

Дальнейшее развитие России возможно только при адаптации всех государственных структур, приоритетов, ценностей, институтов в соответствии с требованиями информационного общества.

Информатизация считается прорывом в будущее. На это пошли все развитые страны, придав информатизации высшие приоритеты, подчинив этой цели основные ресурсы и усилия. Информатизация превратилась в критерий оценки могущества и фактор выживания той или иной страны в борьбе за экономическое и политическое превосходство, стала важнейшим ориентиром для выработки внутренней и внешней стратегии государства.

На данном этапе России необходимо создать собственное машинное производство и программное обеспечение к нему. Подготовить население к переходу в информационное общество, изменив образ жизни общества. Постоянно совершенствовать законодательство в данной сфере.

Данные проблемы необходимо решать через воспитание и обучение новых специалистов, а также создавая информационно-правовое поле жизнедеятельности общества.

К настоящему времени основные направления развития законодательства в информационной сфере определены, в основном соответствуют зарубежной практике правового регулирования информационных отношений и осуществляются в соответствии с международно-правовыми требованиями к обеспечению свободы слова и иных прав и законных интересов граждан в области производства, хранения и распространения информации.

В России интенсивное использование зарубежных технологий опережает реакцию законодателя, которому требуется время для адекватной регламентации в законах и иных нормативно-правовых актах отношений, возникающих в рассматриваемой сфере. Кроме того, очень важно разумно учитывать опыт других государств, которые, значительно раньше приступив к освоению информационного пространства и в частности в борьбе с преступлениями в сфере высоких технологий, выработали систему эффективных правовых средств этой борьбы.

На современном этапе законодательные инициативы должны затрагивать два основных направления регулирования в информационной деятельности общества: информационное экономическое право (регулирует порядок осуществления в информационной сети электронной экономической деятельности: электронной торговли, интернет-банкинга, электронного консалтинга, электронного рекламинга, интернет-страхования и т.д.); информационное гуманитарное право (регулирует порядок осуществления в информационной сети электронной гуманитарной деятельности по обеспечению государством реализации информационных прав физических лиц, в том числе путем создания и функционирования систем электронного администрирования). В России внедрена и совершенствуется так называемая система электронного правительства. В рамках этой системы реализация прав граждан на оказание им публичных услуг осуществляется

органами государства с помощью глобальных компьютерных сетей. Уже сейчас граждане получают возможность через специальные сайты государственных органов в сети Интернет получать доступ к соответствующей публичной информации о деятельности этих государственных органов, обращаться с жалобами и обращениями, направлять заявки на выдачу всевозможных справок, разрешений, оказание услуг социального характера.

Указанная система должна способствовать упрощению диалога между обществом и властью, повышать эффективность и адресность государственного и муниципального управления. Другим направлением выступает обеспечение государством информационных прав граждан, в том числе на свободный оборот незапрещенной (находящейся в открытом доступе) информации, ее сбор, обработку и распространение в электронной форме.

Необходимо также создание и совершенствование сетевого законодательства, регулирующего: сетевые безналичные расчеты для подготовки перехода к электронным деньгам, сетевое взаимодействие для дистанционного заключения договоров, сетевое разрешение споров в виртуальных процессах и многое другое.

Особо необходимо отметить, что приоритетным направлением развития законодательства Российской Федерации должна стать проблема охраны прав человека в условиях формирования информационного общества. Особое внимание необходимо уделять вопросам недостаточно разработанным в законодательстве РФ: реализации права на информацию; формированию эффективной системы информирования общества и совершенствованию функционирования СМИ; совершенствованию законодательства в области предпринимательства, прежде всего в части новых видов деятельности, таких, как электронная торговля, работа, обучение; дальнейшей либерализации рынков информационных продуктов, технологий и услуг, развитию конкуренции; защите персональной тайны; охране интеллектуальной собственности; улучшению сетевого доступа к информационным ресурсам и защите информации в сетях передачи данных.

И естественно, информация, превращаясь в основные ресурсы развития общества, должна защищаться государством. С этой целью законодательство обязано стоять на страже интересов граждан, обеспечивать правовую защиту на всех уровнях взаимодействия в новых условиях жизнедеятельности информационного общества.

Самойленко Е.А.
Россия, Санкт-Петербург, ЗАО «АСИС»

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИИ

Информационная безопасность в России только начинает формироваться, как новый государственно-общественный институт. Многое на пути его становления уже сделано, но и остается немало проблем, которые требуют оперативного решения.

Обеспечение информационной безопасности требует решения целого комплекса задач, доктрина перечисляет наиболее важные из них:

– разработка федеральных целевых программ обеспечения информационной безопасности;

– совершенствование нормативно-правовой базы обеспечения информационной безопасности;

– координация деятельности органов государственной власти, предприятий, учреждений и организаций независимо от то форм собственности в области обеспечения информационной безопасности;

– создание механизмов формирования и реализации государственной информационной политики России;

– разработка современных методов и средств защиты информации;

– развитие и совершенствование систем защиты информации и государственной тайны;

– создание системы подготовки кадров в области информационной безопасности и информационных технологий.

Выделяют четыре основные составляющие национальных интересов России в информационной сфере:

– соблюдение конституционных прав и свобод человека и гражданина в области получения и пользования информацией;

– информационное обеспечение государственной политики страны, связанное с доведением до российской и международной общественности достоверной информации;

– развитие современных информационных технологий;

– защита информационных ресурсов от несанкционированного доступа

Таким образом, можно сделать вывод, что состояние ИБ РФ существенно зависит от угроз ИБ, проявление которых может нанести непоправимый вред всей системе ИБ страны. Национальная безопасность РФ существенно зависит от обеспечения ИБ, влияющие на национальные интересы России в информационной сфере.

Синещук Ю.И., Филиппов А.Г.
Россия, Санкт-Петербург, Военно-морская академия им. Адмирала Флота Советского Союза Н.Г. Кузнецова, Санкт-Петербургский университет ГПС МЧС России

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, КАК ОСНОВА ОБЕСПЕЧЕНИЯ ЭФФЕКТИВНОСТИ СИСТЕМЫ УПРАВЛЕНИЯ МЧС

В России продолжается переход к постиндустриальной стадии развития в форме информационного общества, в котором производство и потребление информации являются важнейшим видом деятельности, информация признается наиболее значимым стратегическим ресурсом, новые информационно-коммуникационные технологии (ИКТ) становятся базовыми технологиями, а основу инфраструктуры общества формирует информационно-коммуникационная инфраструктура.

Эффективность и качество противодействия чрезвычайным ситуациям техногенного и природного характера напрямую зависят от механизма управления, оперативности и точности управляющих воздействий, качества навигационно-информационного обеспечения Единой государственной системы предупреждения и действий в чрезвычайных ситуациях (РСЧС), на всех уровнях (от федерального до местного).

Научные исследования в области управления социальными и экономическими системами неразрывно связаны с совершенствованием системы управления, информационной поддержки лица принимающего решение (ЛПР).

Достижение успехов в предотвращении и устранении последствий ЧС определяется, не столько потенциальными сколько реализуемыми возможностями подразделений МЧС, а степень реализации этих возможностей находится в непосредственной зависимости от эффективности процесса управления ими. В настоящее время состояние и перспективы развития системы управления являются важнейшим показателем готовности сил МЧС к реализации возложенных на них задач, уровня их организационного и технического совершенства. Систему управления силами РСЧС необходимо вывести на новый уровень информационной насыщенности и устойчивости. Должна быть сформирована кризисная информационно-управляющая система, обеспечивающая оперативное взаимодействие и реагирование сил и средств, что, в первую очередь. является важным для ликвидации крупномасштабных чрезвычайных ситуаций природного характера, крупных пожаров, реагирования на угрозы военного времени.

В целом РСЧС должна перейти от принципа оперативного реагирования, к принципу профилактики и предупреждения чрезвычайных ситуаций и комплексного взаимодействия всех органов управления, сил и средств. При этом следует обеспечить развитие инфраструктуры единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций с учётом создания системы обеспечения вызова экстренных оперативных служб с использованием ресурсов глобальной навигационной спутниковой системы ГЛОНАСС и других информационно-навигационных систем и технологий.

В рамках принятой в России Доктрины информационной безопасности сформулированы задачи и приоритеты в информационной сфере. Важнейшей из них определена задача создания ЕИП Российской Федерации, неотъемлемой частью которой является ЕИП МЧС. Такой подход является отражением всеобщей тенденции глобализации информационных систем, развитие которых сопровождается расширением перечня угроз, появлением дополнительных уязвимостей информационным ресурсов и, как следствие, совершенствованием способов реализации информационных атак. Решение комплексной задачи обеспечения безопасности ЕИП должно носить качественно новый характер, по отношению к традиционным методам и средствам информационной безопасности. Это требует создания новых интегральных технологий хранения и защиты информационных ресурсов, выработки дополнительных или совершенствования существующих организационных схем и процедур поддержания целостности информационных ресурсов, подготовки специализированных кадров для решения стоящих задач

В рамках предложенной концепции основными мероприятиями по развитию системы управления в кризисных ситуациях можно считать:

– внедрение интегральных оценок риска и комплексных систем реагирования в работу органов повседневного управления при установлении уровня реагирования на чрезвычайные ситуации;

– создание системы «112», интегрирующей деятельность ведомственных диспетчерских служб;

– внедрение в практику функционирования оперативных служб органов повседневного управления перспективных автоматизированных информационных и управляющих систем поддержки принятия решений (информационно-справочных, геоинформационных (включая ресурс ГЛОНАСС), аналитических, информационно-расчётных, а также моделирующих сценарии развития чрезвычайных ситуаций;

– обеспечение информационной безопасности процессов управления силами и средствами МЧС.

Советов Б.Я., Колбанёв М.О., Татарникова Т.М.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербургский государственный экономический университет

О РАЗВИТИИ ТЕХНОЛОГИИ ИНФОРМАЦИОННОГО ОБЩЕСТВА

Доклад посвящен анализу процессов развития технологий, обеспечивающих переход к информационному и интеллектуальному обществам.

Показано, что инновации последних десятилетий развития человечества направлены на удовлетворение потребностей людей в информационных продуктах и услугах, поддержку интеллектуального взаимодействия между людьми, обеспечение свободного доступа к мировым духовным ресурсам. Достижения в области построения информационных систем, предоставляющих соответствующие сервисы, определили в конце прошлого века переход к новому инновационному циклу развития человечества. Именно в 80-90 годы XX века были изобретены и получили широкое распространение такие системы как персональные компьютеры и сверхмощные компьютерные системы, новые типы систем сохранения информации, цифровые интеллектуальные и экспертные информационные системы, мультисервисные и мобильные сети связи, интернет и другие. Последовавшая далее конвергенция услуг систем хранения данных, телекоммуникаций и вычислительной техники породила новую технологию инфокоммуникации, которая стала доминирующей областью деятельности человека и может быть названа Великой технологией XXI века.

Переход от индустриального к информационному обществу обеспечен широким внедрением средств информатизации. Дальнейшее развитие информационных технологий должно привести к формированию интеллектуального общества.

Результатом такого движения по В.И. Вернадскому в текущем тысячелетии станет новая среда обитания человека – ноосфера, которая с информационно-технологической точки зрения может быть представлена на двух уровнях. Первый – материальный – обеспечивает накопление глобального информационного ресурса благодаря целенаправленной деятельности многих поколений людей.

Второй уровень нужно понимать как интеллектуальный. Он будет достигнут на базе накопленных информационных ресурсов при условии, что этот ресурс эффективно сохраняется во времени, распространяется в пространстве и обрабатывается при решении многообразных задач с применением качественно новых интеллектуальных технологий и систем во благо развития цивилизации. Переход от информационного к интеллектуальному обществу станет одним из результатов такого развития.

Технологическая основа информационного общества была создана благодаря революционным достижениям в области электроники, фотоники и радиотехники. Однако из проведенного анализа следует, что до сих пор технологии развивались по экстенсивному пути, совершенствовались в основном с точки зрения количественных характеристик, таких как объемы данных, хранящихся в системах хранения, объемы доставки данных системами распространения и объемы обрабатываемых данных. Сегодня технологические проблемы сохранения, распространения и обработки больших массивов информационного ресурса можно считать решенными благодаря достигнутым плотности записи при сохранении, пропускной способности при распространении и техпроцессу при обработке.

Для перехода к интеллектуальному обществу необходимо интенсивное развитие. Это означает, что должна появиться новая интеллектуальная, возможно не цифровая, технология работы с информацией, предоставляющая пользователю такие инструменты, которые позволят ему самостоятельно создавать новые средства для эффективного использования информационного ресурса.

Соколов С.С., Новоселов Р.Ю.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова

ГРИД-СИСТЕМЫ – БУДУЩЕЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ТРАНСПОРТНОЙ СФЕРЫ

Грид-система – форма «распределенных вычислений», в которой «виртуальный суперкомпьютер» представлен в виде кластеров, соединённых с помощью сети, слабосвязанных, гетерогенных компьютеров, работающих вместе для выполнения огромного количества заданий (операций, работ). Данная технология применяется при решение ресурсоемких задач, таких как сложные математические расчеты, прогнозирование. В чем разница между грид-системами и суперкомпьютерами? Каждая ячейка грид-системы представляет собой отдельный компьютер, соединенный через сеть с другими. Суперкомпьютер – это система из множества процессоров, подключенных к одной локальной шине, т.е. представляет собой одну большую машину. Таким образом, общая стоимость грид-системы дешевле, чем стоимость суперкомпьютера.

Выделяют три типа грид-систем:

– Добровольная. Система на основе добровольно предоставляемого ресурса компьютера. Владелец компьютера сам решает использовать или не использовать свой компьютер в качестве ячейки грид-системы.

– Научная. Приложения программируются специальным образом, чтобы максимально распараллелить вычисления.

– Коммерческий грид. По требованию заказчика обычные приложения работают на «виртуальном компьютере», который состоит из объединенных в грид-систему нескольких компьютеров.

Термин «грид-система» появился в начале 1990-х годов, когда вышел сборник под редакцией Яна Фостера и Карла Кессельмана «Грид: проект новой компьютерной инфраструктуры» («The Grid: Blueprint for a new computing infrastructure»). Добровольные грид-системы стали популярными в конце 1990-х годов, когда появились первые проекты добровольных вычислений GIMPS, distributed.net, SETI@home.

На данный момент грид-системы используются во многих сферах. Например, грид-система под названием GRID используется в работе Большого Адронного Коллайдера. Грид-системы также могут использоваться в сфере транспорта, например прокладывание сложных многопоточных параллельных маршрутов, организация сложной транспортной системы, с которой не справится простой компьютер (диспетчерский центр, прокладывание маршрутов, «умные» светофоры, анализ транспортного потока, параллельный анализ различных датчиков). Также данные системы могут успешно применяться в сфере водного и воздушного транспорта, ведь их использование сильно ускоряет расчеты, снижается риск аварий и катастроф.

Федоров Д.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

ПОДХОД К ФОРМАЛИЗАЦИИ ОПИСАНИЯ ДЕСТРУКТИВНОГО ИНФОРМАЦИОННОГО ВОЗДЕЙСТВИЯ НА ЛИЧНОСТЬ И ОБЩЕСТВО

В период становления информационного общества на передний план выступают гуманитарные аспекты информационной безопасности, т.е. методы нападения и защиты от деструктивного информационного воздействия (ДИВ) на личность и общество. Сдерживающим фактором развития гуманитарных аспектов информационной безопасности является недостаточно формализованный аппарат для описания угроз ДИВ. В работе предлагается подход к формализации описания ДИВ на личность и общество.

Познавая окружающую действительность, человек образует понятие о предметах и явлениях действительности. Система понятий, которая формируется у человека, отражает его мировоззрение и влияет в дальнейшем на его поведение. Информационное воздействие на структуру системы понятий приводит к перестроению картины мира человека. Базируясь на формализованном представлении знания (ФПЗ), предложенном проф. В.Я. Розенбергом, можно построить модель системы понятий человека и рассмотреть возможные типы атак на нее.

Суть ФПЗ заключается в автоматизированном построении многоуровневой сети знаний, вершинами которой являются элементы системы знаний – понятия, а дугами – связи между понятиями. Связь между понятиями осуществляется через определения. Таким образом, на основе ФПЗ можно автоматизировать построение системы понятий, на которую в повседневной жизни опирается человек. Построенная система выступает в качестве модели мировоззрения человека.

Рассмотрим варианты воздействия на сеть знаний человека. Наибольший интерес для субъектов ДИВ (манипуляторов) представляют системообразующие понятия, воздействие на которые приведет к максимальному перестроению структуры сети знаний. Выявить такие понятия можно автоматизировано по числу связей с другими понятиями.

Важно заметить, что механизмы получения новой информации и ДИВ принципиально не отличаются. Главное отличие – в цели, с которой информация передается человеку. Далее рассматриваются механизмы манипулятивного воздействия (скрытое психологическое воздействие), т.е. такого воздействия, которое побудило человека сделать поступок, из-за которого он оказался в проигрыше.

Приведем подход к классификации атак на сеть знаний.

Атакой 1-го рода будем называть вид информационного воздействия на сеть знаний, при котором в сети появляется новый элемент – новое понятие. Введение в мировоззрение человека нового понятия приведет к образованию новых связей и перестроению его внутреннего представления о мире.

Атакой 2-го рода будем называть вид информационного воздействия, при котором один из элементов сети знаний приобретает новое содержание, т.е. изменяется (замещается) его определение. Это приводит к перестроению связей между понятиями: появлению новых связей или изменению существующих. Предварительно, замещаемое понятие может быть актуализировано, т.е. на него направляется внимание объекта воздействия.

Например, частичное изменение взглядов на событие может потребовать от манипулятора провести подряд несколько видов информационных атак, используя при этом эмоциональную «завесу».

Предложенный подход к формализации описания атак на внутреннюю структуру знаний человека может быть спроецирован для описания ДИВ на уровне общества. Опасность общественного ДИВ заключается в неконтролируемости процесса воздействия, что может привести к отклонениям в психике людей (саморазрушению), поэтому каждому человеку необходимо развивать способность к рефлексии, внимательно относиться к поступающей информации и стараться выявлять цели, с которыми информация сообщается.

Шишкин В.М., Абросимов И.К.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ДИНАМИЧЕСКАЯ МОДЕЛЬ СИСТЕМЫ ВЗАИМОДЕЙСТВИЯ РАЗВИТИЯ ИКТ И ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Исключительная роль, которую приобрели в современном мире информационно-коммуникационные технологии (ИКТ) практически во всех областях деятельности человечества, стала очевидным фактом. Они инкорпорированы во все системы жизнеобеспечения и управления государства, регионов, производственные процессы, в большинство видов технических устройств и технологического оборудования, вошли в повседневный быт значительной части населения.

Очевидно также, что развитие и распространение ИКТ сопровождается нарастанием и усложнением плохо решаемых, как показывает практика, проблем информационной безопасности разного масштаба, от индивидуального до глобального. Информационная безопасность (ИБ) стала не просто структурной составляющей национальной безопасности, но неотъемлемо присутствует во всех её аспектах.

При этом существуют практически взаимоисключающие взгляды на стратегию развития ИКТ, а следовательно и на проблематику ИБ, в России. С одной стороны, прилагаются усилия по воссозданию импортозамещающего производства отечественной компонентной базы СВТ, коммуникационного оборудования, разработке ОС, без чего трудно говорить о поддержании приемлемого уровня ИБ, во всяком случае, в сфере государственного управления, обороны, функционирования критически важных систем и объектов, а с другой – утверждается неэффективность подобных мер при перенасыщенном глобальном рынке средств ИКТ. Достаточно, как пример, вспомнить подготовленную вскоре после утверждения «Доктрины информационной безопасности», видимо, как её контральтернатива, одиозную «Белую книгу информационных технологий» (2000 г.), в которой единственной областью ИКТ, достойной для развития в России был признан аутсорсинг ПО, а приоритет отдавался изучению английского языка. Или относительно недавние (2009 г.) намерения исключить из приоритетных направлений развития науки, технологий и техники в Российской Федерации направление «Информационно-телекоммуникационные системы», парадоксально мотивированные тем, что «Россия отстает от развитых стран по уровню научных исследований в области информационно-коммуникационных технологий». Причём все эти инициативы исходили от около правительственных структур.

В таком случае естественно попытаться применить инструмент, позволяющий в какой-то мере исключить субъективизм мнений, построив математическую модель, связывающую в систему динамического взаимодействия некоторый набор существенных в данном контексте факторов, и расчётным путём обеспечить возможность оценки развития ситуации при альтернативных сценариях. Опыт применения подобного рода динамических моделей в различных предметных областях, в том числе плохо формализуемых, имеет уже достаточно давнюю историю, показав их, по крайней мере, познавательную и прогностическую полезность.

Для нашей модели в качестве основы была использована структурная схема (Юсупов Р.М., Шишкин В.М. Информационно-коммуникационные технологии и национальная безопасность – противоречивая реальность // Информатизация и связь, №1, 2010. — С. 27–35.), иллюстрирующая взаимодействие развития ИКТ и обеспечения национальной безопасности через систему других разнонаправленно действующих факторов. Даже в образном виде она позволяет видеть, что при отсутствии сбалансированности составляющих процесса, недооценке угроз, учитывая опосредованные обратные связи, национальной безопасности и в целом социально-экономическому развитию может быть нанесен ущерб.

В текущей версии модель представлена системой восьми обыкновенных дифференциальных уравнений первого порядка. В качестве фазовых переменных выступают элементы указанной структурной схемы, в том числе, уровни развития ИКТ, состояния и угроз национальной безопасности, социально-экономического развития. В правых частях уравнений находятся суммы умноженных на некоторые коэффициенты переменных, знак которых определяется направленностью действия

факторов. Для упрощения поиска области устойчивости расчёты велись при различных значениях фиксированных коэффициентов, соответствующим разным сценариям развития ситуации, а для проверки устойчивости использовался критерий Гурвица. Решение системы полученных уравнений производилось при помощи системы компьютерной алгебры Wolfram Mathematica.

Тестовые расчёты показали правдоподобное поведение модели в автономном режиме, что позволяет исследовать её при различных сценариях управлений и более содержательном назначении коэффициентов. Полученные результаты, будут представлены в докладе.

Яковлева Н.В.
Россия, Санкт-Петербург, Санкт-петербургский филиал «Финансовый университет при Правительстве Российской Федерации»

СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ СИСТЕМЫ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОГО СОТРУДНИЧЕСТВА РЕГИОНОВ В ФОРМЕ ПАРАДИПЛОМАТИИ

Между административно-территориальными единицами субъектов двух стран, не граничащих друг с другом, сотрудничество осуществляется в форме парадипломатии. Каждый субъект использует свои сильные стороны для привлечения новых инвесторов и заинтересованных лиц, компаний и корпораций. Высокие экономические показатели района в субъекте Российской Федерации (РФ) зависят не только от производства товаров и услуг на внутренний рынок, но и от количества заключенных межгосударственных соглашений между органами местного самоуправления двух стран, которые дают дополнительные инвестиции для развития районов. Но недостаточное информационное обеспечение делает этот процесс общения тяжелее. В нашем понимании, информационное обеспечение – это информация, необходимая для управления экономическими процессами, содержащаяся в базах данных информационных систем; создание информационных условий функционирования системы, обеспечение необходимой информацией. Необходимо создавать такие информационные условия функционирования системы, которые могли бы обеспечивать необходимой информацией не только органы исполнительной власти субъектов РФ, но и государства соучастников. На сегодняшний момент отсутствует единая база поиска, получения, хранения, накопления, передачи, обработки информации, данных по каждому району.

На примере Немецкого национального района (ННР) в Алтайском крае и земли Саксонии Ангальт мы видим, что такое информирование реализовано частично в виде выпуска газеты на русском и немецком языках («Ihre Zeitung» и «Zeitung für Dich»); инвестиционного паспорта муниципального района немецкого национального района Алтайского края; дружественных отношений между представителями властей ННР и Германией.

В начале 2013г был изменен полностью сайт района. Теперь на сайте можно найти всю необходимую информацию по работе администрации; отсутствие мониторинга по межгосударственному сотрудничеству на уровне местного самоуправления; отсутствие электронного делопроизводства.

С другой стороны в Азовском ННР в Омской области на сегодняшний момент существует проблема идентификации в сети. У района хорошо развита система информационного обеспечения, но не достаточна ее защита.

Для того чтобы в полной мере осуществлялась информационное обеспечение, необходимо:

– со стороны ННР развивать виртуальную страницу сайта на английском языке; своевременно публиковать новости; проводить международные форумы с участием других государств; проводить экономический мониторинг; создание представительство по международному сотрудничеству.

– со стороны Алтайского края необходимо: во всех регионах создать единую базу сбора данных по экономическим показателям, на пример создание программу в которой будут отражаться экономические показатели, сильные и слабые стороны, создавать безопасность идентификации в сети при передачи данных;

– со стороны Омской области: создание хорошей базы защиты от вирусов и хакеров;

– со стороны земель ФРГ: создание консультативных бюро по Землям ФРГ; внесение новостей в новостную ленту НР, участие в выпусках газет на немецком языке, создание собственного радио в ННР.

ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Баушев С.В., Буторин Н.В., Гаценко О.Ю., Самонов А.В.
Россия, Санкт-Петербург, ЗАО «Центр научно-прикладных исследований «ИнформПро»

ПРОГРАММНЫЙ КОМПЛЕКС СОЗДАНИЯ И ПРОВЕРКИ ЮРИДИЧЕСКИ ЗНАЧИМЫХ ЦИФРОВЫХ ФОТОСНИМКОВ

Современные технологии и средства создания цифрового видео и фото контента активно внедряются в цифровые фотоаппараты, видеорегистраторы, смартфоны, планшеты и другие устройства. Однако их применение в ряде областей, где они могли бы быть исключительно полезны и востребованы, сдерживается тем обстоятельством, что их достаточно легко подправить и фальсифицировать. В настоящее время специальные технические способы надежного свидетельствования достоверности фотоснимка, сделанного цифровой фотокамерой, отсутствуют.

С целью устранения данного недостатка цифровых фотоматериалов сотрудниками ЗАО «ЦНПИ «ИнформПро» был разработан и предлагается к массовому использованию способ и средство создания защищенных от подделки и фальсификации цифровых фотоснимков. Опытные образцы данного программного средства в настоящее время реализованы для смартфонов и цифровых фотоаппаратов, функционирующих под управлением операционной системы Android (Samsung, LG и др.). Созданные с его помощью цифровые фотоматериалы обладают всеми признаками юридически значимых документов.

В предлагаемом инновационном решении достоверность цифровых фотографий подтверждается наличием у фотоматериалов электронной цифровой подписи (ЭЦП), удостоверяющей, во-первых, авторство, время и место получения фотоснимка и, во-вторых, отсутствие подделки изображения и служебных данных. Это достигается применением усиленной квалифицированной или неквалифицированной ЭЦП, создаваемой в соответствии с ГОСТ Р 34.11-2012 «Функция хэширования» и ГОСТ Р 34.10-2012 «Процессы формирования и проверки электронной цифровой подписи» согласно Федеральному Закону от 6.04.2011 г. №63-ФЗ «Об электронной подписи».

Реализующий этот способ программный модуль устанавливается в виде приложения в цифровом фотоаппарате или смартфоне. В момент съемки модуль создает в оперативной памяти буфер, в который создаваемый им асинхронный поток записывает данные съемки непосредственно с ПЗС-матрицы устройства, добавляя в них информацию о месте и времени съемки, получаемые с помощью встроенного в устройство приемника сигналов GPS/ГЛОНАСС, формирует для данного фотоматериала электронную цифровую подпись (ЭЦП) и сохраняет полученный фотодокумент в память устройства.

При создании ЭЦП задействуется механизм несимметричного шифрования, когда секретный ключ «зашит» в программный модуль и жестко привязан к устройству. Несекретный ключ может быть получен и использован любым пользователем, желающим удостовериться в достоверности как изображения, так и сопутствующих ему данных. Ключи ЭЦП для формирования юридически значимых документов должны быть получены от уполномоченных органов и аккредитованных удостоверяющих центров. Любое изменение в таком электронном документе со стопроцентной гарантией обнаруживается программой верификации ЭЦП.

Данное инновационное решение предлагается использовать в деятельности государственных органов и коммерческих предприятий, страховых и транспортных компаний, судебных и следственных органов, СМИ, специалистов и любителей в области фотоискусства, в интернет-сервисах и приложениях.

Бачило И.Л.
Россия, Москва, Институт государства и права РАН

О ПОДХОДАХ К СОВЕРШЕНСТВОВАНИЮ ИНФОРМАЦИОННОГО ЗАКОНОДАТЕЛЬСТВА

Глобальная информатизация жизни социума первого десятилетия XXI века действует как ускоритель движения во всех сферах жизни общества: экономической, социальной, политической, культурной. Распространение информации по сетям коммуникаций с большим снижением значения государственных границ, особенностей цивилизационных характеристик стран и континентов, этнических, национальных, религиозных и т.д. создает ситуацию усложнения условий для движения

общества по позитивной парадигме. Это усложняет гармонизацию правовых, политических, этических параметров отношений как внутри государств, так и в их сообществах.

Технологическому прогрессу сопутствуют факторы социального, культурного, экономического плана, питательной средой которых, среди прочих причин, является и информационное, цифровое неравенство, киберпреступность. Складывается ситуация напряжения в области правового регулирования всей сферы информационного взаимодействия, поворота к оздоровлению информационной среды, особенно Интернет-среды, обеспечения информационной безопасности. В таких условиях вопрос оценки адекватности и продуктивности уже принятых законов национальных и международных актов в обеспечении безопасности мира, каждого государства и общества в целом выходит на первый план.

За последние два десятилетия в России и в государствах-участниках СНГ сформирована законодательная база регулирования информационных отношений, действующая как для внутреннего развития информационных и технологических ресурсов, так и их использования во всех сферах жизни общества. Однако нарастающий разрыв в темпах и энергетике технологической структуры информатизации и усвоении потенциала ИКТ в управлении делами общества и государства, в реализации прав человека, его включенности в этот процесс правовой системой преодолевается с большим трудом и издержками. Многогранность процессов информатизации и обеспечения безопасности общества ведет к наращиванию числа законов и других нормативно-правовых актов. Их взаимодействие плохо обеспечивается, ибо каждый новый закон требует поправок и изменений в уже принятые. Так создается цепочка работы правовой системы и законодательства самой на себя с очень малым коэффициентов влияния на реальные отношения людей и их организаций.

В сложившейся ситуации возможны два подхода. Первый — продолжать «штопать» и обновлять действующие законы, и двигаться в уже сложившейся системе нормотворчества, о которой сказано выше. При таком подходе каждый закон выстраивает свой предмет регулирования, свои термины и их понятия, плохо взаимодействует с рядом стоящими законами, что тормозит включение практики в реально идущие процессы.

Так, например, практика применения российского закона «Об информации, информационных технологиях и о защите информации» (от 29.06.2006 г. №149-ФЗ) показывает, что только по идее этот закон является базовым. На сегодня ни этот закон, ни последовавшие за ним не создают юридической базы для продуктивного взаимодействия информационных технологий и информационных ресурсов. Производство и распространение информационных и коммуникационных технологий занимает положение одной из ведущих отраслей экономики и рынка, оценивается по признакам затрат, доходов, прибыли, а это мало влияет на состояние информационной культуры общества и его основных векторов развития. Ни один закон не смог решить вопросы наполнения Интернет-среды полезной информацией и снижения ее засорения вредной информацией.

Второй подход нацелен на уплотнение и координацию законодательного ресурса в целях повышения его действенности и эффективности. Он предусматривает переход от штучного, фрагментарного творчества по каждому нормативному акту «самого по себе» (результат отраслевой «самостоятельности» структур в системе управления) к комплексному решению назревших проблем.

Институт Государства и права РАН, анализируя создавшееся положение, разрабатывает концепцию Информационного кодекса. Эта работа ведется с учетом как российского опыта, так и опыта МПА СНГ в этом вопросе. Идея создания Кодекса предусматривает предварительную систематизацию уже накопленного нормативно-правового материала и вычленение базовых проблем, которые могут заложить основные принципы и требования, не подвергаемые при каждом заходе законодателя изменениям и требующие их обязательного соблюдения в дальнейшем нормотворчестве.

Бондуровский В.В.
Россия, Санкт-Петербург, Межпарламентская Ассамблея государств-участников СНГ

ОБ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПРАВ ЧЕЛОВЕКА В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

Межпарламентская Ассамблея государств – участников Содружества Независимых Государств (МПА СНГ) является межгосударственным органом, осуществляет сотрудничество высших законодательных органов государств-участников. Важнейшей составляющей этого сотрудничества является правотворческий процесс в интересах всех и каждого из ее участников.

Ассамблея в течение многих лет вносит лепту в сотрудничество государств-участников по обеспечению информационной безопасности и прав человека в информационном пространстве. В рамках деятельности Объединенной комиссии при МПА СНГ по гармонизации законодательства в сфере борьбы с терроризмом, преступностью и наркобизнесом, профильных постоянных комиссий МПА СНГ (по обороне и безопасности; по культуре, информации, туризму и спорту) в соответствии с

решениями высших уставных органов Содружества отрабатывались многие отдельные сегменты названной проблематики.

Предпринятый экспертами Объединенной комиссии анализ ситуации с целью определения системы мер по правовому обеспечению информационной безопасности показал, что именно в данной области назрела масса проблемных вопросов, которые должны быть успешно решены государствами СНГ в самые короткие сроки. В соответствии с Комплексным планом мероприятий по реализации Концепции сотрудничества государств – участников Содружества Независимых Государств в сфере обеспечения информационной безопасности, прежде всего, были подготовлены «Рекомендации по совершенствованию и гармонизации национального законодательства государств – участников СНГ в сфере обеспечения информационной безопасности», которые имеют концептуальный по своему значению характер. (Рекомендации приняты МПА СНГ 23 ноября 2012 г.) На основе этого документа государствам Содружества в наращивание усилий по обеспечению информационной безопасности предложен целый комплекс законодательных инициатив.

В соответствии с проектом Межгосударственной программы совместных мер борьбы с преступностью в 2014 г. предстоит разработать проекты Стратегии обеспечения информационной безопасности для государств – участников СНГ, модельный регламент административных процедур, осуществляемых уполномоченными органами в сфере обеспечения информационной безопасности государств – участников СНГ, модельный закон «О критически важных объектах информационно-коммуникационной инфраструктуры», проработать вопрос внесения изменений в модельный закон «Об информации, информатизации и защите информации», а к 2015 г. разработать и принять изменения и дополнения в модельный Уголовный кодекс для государств – участников Содружества Независимых Государств по вопросам борьбы с преступлениями в информационной сфере.

В соответствии с проектом Программы сотрудничества государств – участников СНГ в борьбе с терроризмом и иными насильственными проявлениями экстремизма предусмотрена разработка проекта Комментария к модельному закону «О государственных секретах» и проекта модельного закона «О критически важных объектах информатизации». Разработка названных документов и их реализация в национальных правовых системах государств-участников послужит добротным подспорьем в нормативно-правовом противодействии новым вызовам и угрозам информационной безопасности государств Содружества.

Прошедшая 11–12 июля 2013 г. в Минске международная научно-практическая конференция «Информационная безопасность как составляющая национальной безопасности государства» подтвердила актуальность проводимой работы и подкрепила её рядом новых и значимых инициатив.

К настоящему времени полностью завершена работа над еще одним проектом специального в данной области документа – «Рекомендациями по правовому регулированию эксплуатации открытых телекоммуникационных сетей для предупреждения их использования в террористических и иных противоправных целях», который внесен для принятия на тридцать девятое пленарное заседание Ассамблеи в текущем году. При принятии Ассамблеей этих Рекомендаций, перечень мер по совершенствованию правового обеспечения информационной безопасности и гармонизации законодательства государств-участников в данной области будет расширен.

Вус М.А., Кучерявый М.М.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН, Управление ФСТЭК России

ВОПРОСЫ ПРЕДУПРЕЖДЕНИЯ ИСПОЛЬЗОВАНИЯ ОТКРЫТЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ В ТЕРРОРИСТИЧЕСКИХ И ИНЫХ ПРОТИВОПРАВНЫХ ЦЕЛЯХ

В информационном пространстве сегодня в той или иной форме нашли воплощение большинство видов деятельности (политическая, финансово-экономическая, коммерческая, образовательная, культурная и т.д.). В современных глобальных социальных сетях представлены практически все социальные слои и возрастные группы населения. Вместе с тем, процесс становления социальных отношений и форм собственности в новой информационной среде, не подкрепленный в достаточной мере ни соответствующими законодательными, ни нравственными установками, оказывает существенное влияние на структуру преступности, порождает неизвестные ранее формы негативного девиантного поведения.

Расширяющиеся возможности глобальных компьютерных информационных и телекоммуникационных сетей обусловили повышенный интерес к ним со стороны организованной преступности, в том числе экстремистских и террористических организаций. Особенностью современного терроризма является активное использование как информационно-психологического воздействия, являющегося важным элементом манипулирования сознанием и поведением людей, так и информационно-технического воздействия на отдельные элементы информационно-телекоммуникационной инфраструктуры государств в целях нанесения им ущерба, а также для их подавления и/или уничтожения. Новейшие информационные технологии и открытые телекоммуникационные сети всё чаще используются террористами, террористическими группами или организациями для пропаганды, обмена информацией, привлечения финансовых ресурсов,

планирования и осуществления актов терроризма. Количество атак на информационные ресурсы с каждым годом увеличивается, а сами угрозы становятся все более изощренными. С террористическими угрозами тесно переплетаются криминальные угрозы экономической безопасности.

Расширение масштабов террористических угроз и экстремистских проявлений требует укрепления антитеррористического потенциала, совершенствования законодательного обеспечения противодействия этим угрозам. Важную роль, в частности, призвана сыграть выработка и использование в законодательстве и юридической практике стран Содружества общих правовых подходов, применяемых в области правового регулирования использования открытых телекоммуникационных сетей (ОТКС). В комиссиях Межпарламентской Ассамблеи СНГ (МПА СНГ) прошел обсуждение проект «Рекомендации по правовому регулированию эксплуатации открытых телекоммуникационных сетей (ОТКС)». Этот документ был подготовлен российскими и белорусскими специалистами с учётом положений международных правовых актов и рекомендаций международных организаций по вопросам совершенствования правового регулирования в области эксплуатации ОТКС для предупреждения их использования в террористических и иных противоправных целях на территории Содружества.

В качестве первоочередных задач развития национальных правовых механизмов регулирования эксплуатации ОТКС в государствах Содружества разработчиками Рекомендаций предложено рассматривать создание и обеспечение функционирования общегосударственной системы мер по предупреждению возможного использования таких систем в террористических и иных противоправных целях и координацию деятельности компетентных государственных органов и иных организаций в области предупреждения деструктивного использования ОТКС. Необходимы целенаправленные совместные усилия всех ветвей власти, следует задействовать широкий спектр сил, средств и методов воздействия со стороны государства и общества. Последнее, в свою очередь, требует сближения (гармонизации) законодательства государств – участников СНГ в области правового регулирования эксплуатации ОТКС.

Совершенствование правового регулирования предупреждения использования информационных сетей в террористических и иных противоправных целях может осуществляться государствами – участниками СНГ посредством комплекса мер, разрабатываемых и принимаемых как каждым государством самостоятельно, так и в рамках Содружества в целом. При этом необходимо принимать во внимание разнообразие форм и характер возможного использования ОТКС в террористических и иных противоправных целях на территориях государств – участников СНГ. Принципиально важно соразмерять временно вводимые ограничения прав и свобод человека (применяемые в связи с ограничением его права на получение и распространение информации) характеру и уровню связанных с ними угроз и реализовывать приоритет мер по профилактике и предупреждению возможного использования ОТКС в террористических и иных противоправных целях.

В вышеназванных Рекомендациях особо подчеркнута актуальность развития понятийного аппарата в рассматриваемой предметной области, отмечена необходимость обеспечения терминологической ясности и единообразного понимания (трактовок) законодательными органами государств – участников СНГ ряда широкоупотребительных сегодня понятий, таких как: «автоматизированная обработка данных», «информационная сеть (сети)», «защита информации» и др. Важно единообразное понимание и легальное закрепление в правовом поле государств – участников СНГ базовых общетехнических категорий информационной сферы, таких, например, как: «компьютерная информация» и «компьютерные данные», «информационные ресурсы» и «государственные информационные ресурсы», «информационная система» и «компьютерная система», «информационная инфраструктура» и «критически важная информационная инфраструктура», «критически важный объект информационно-телекоммуникационной инфраструктуры» и др.

Применительно к реалиям инфокоммуникационной среды необходимо уточнение и расширение содержательного наполнения таких, в известной мере хрестоматийных юридических понятий, как: «противоправная деятельность» и «террористическая деятельность», «террористическая организация» и «террористические материалы».

В контексте упомянутых Рекомендаций требуют своего легального определения такие правовые категории, как: «открытые телекоммуникационные сети», «информационные ресурсы ОТКС», «технологическое использование ОТКС» и др. Необходимо достичь определенности в трактовках таких понятий как «информационно-психологический терроризм» и «информационно-технический терроризм». Определяя понятия необходимо дать четкое разграничение и выделить классифицирующие признаки, позволяющие отграничивать такие понятия как, например: «компьютерный инцидент» и «компьютерная атака»; «неправомерное использование ОТКС», «правонарушения в области использования ОТКС» и «акт терроризма в области эксплуатации ОТКС».

В целях повышения эффективности межгосударственного сотрудничества важно обеспечить ориентацию всех участников на использование единого понятийного аппарата при разработке конкретных международных и национальных нормативных правовых актов.

Клишков В.Б., Пасынков В.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

НЕКОТОРЫЕ ПРОБЛЕМЫ ПРЕСТУПНОСТИ В СФЕРЕ КОМПЬЮТЕРНЫХ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Одной из тенденций современного времени является активное использование новых информационных технологий преступными группами и сообществами для совершения все более дерзких и изощренных преступлений, наносящих огромный материальный вред стабильности экономики, безопасности граждан, обороноспособности страны. Развитие информационных технологий, компьютеризация населения привели не только к появлению нового вида преступных посягательств, но и необходимости совершенствования уголовно-правовой политики Российского государства, направленной на борьбу с таким явлением, как компьютерная преступность.

Изучение данных уголовно-правовой статистики свидетельствует об актуализации данных видов преступлений с каждым годом во всем мире. В развитых странах с высоким экономическим развитием и компьютеризацией компьютерная преступность имеет более долгую историю, и борьба с ней давно признана одной из первостепенных задач государства. Одной из причин являются огромные ущербы, которые наносятся экономике страны при совершении указанных правонарушений. Так, по данным некоторых исследователей, только США в год несут ущерб, оцениваемый более 6 млрд. долларов, Франция более 2,3 млрд. евро, Германия около 6,6 млрд. евро, Англия 5,2 млрд. фунтов.

Не лучшим образом обстоят дела и в России. С учетом сложившейся к началу 2013 года ситуации можно свидетельствовать, что в ближайшем будущем можно ожидать продолжения повышения криминогенных факторов, влияющих на состояние и динамику преступлений в сфере компьютерной информации в стране.

Среди основных причин быстрого роста данного вида преступлений в первую очередь вступает их высокий уровень латентности, а также сверхвысокий уровень обогащения в течение короткого срока времени. Также этому способствуют и объективные трудности, связанные не только с выявлением и документированием рассматриваемых правонарушений, но и с их доказыванием, что делает преступления в сфере компьютерной информации привлекательней год от года для все большего числа лиц разного возраста.

Как свидетельствуют данные ГИЦ МВД России, доля компьютерных преступлений у нас в стране ежегодно не превышает 0,02–0,03%. Однако если обратиться к материальной стороне вопроса, то можно отметить, что размер ущерба от совершения данных преступлений исчисляется в десятки миллиардов рублей. Развитие же технического прогресса, более глубокое вхождение информационных технологий в нашу жизнь делает еще больше неотвратимость новой угрозы, которая увеличивается с каждым годом по всему миру. При этом необходимо отметить и тот факт, что в настоящее время все больше преступлений совершается с использованием всемирной компьютерной сети Интернет, которая имеет тенденцию к росту криминальных проявлений.

Как уже отмечалось ранее, компьютерные преступления не только являются сравнительно новыми для уголовно-правовых наук, но и обладают высокой латентностью. Данное обстоятельство напрямую связано с недостаточным изучением личности компьютерного преступника.

Как свидетельствуют выборочные исследования, абсолютное большинство компьютерных преступников составляют лица мужского пола (80%). Причиной тому служит, как правило, специфика работы данных лиц, а так же более легкое освоение вычислительной техникой мужчинами в сравнении с женщинами.

Особенностью компьютерных преступников является сравнительно молодой возраст, а также высокий уровень знаний новых компьютерных технологий, которые молодым поколением усваиваются значительно легче. Наличие специального образования для компьютерного преступника не является обязательным атрибутом. Тем не менее, абсолютное большинство преступников имеют высшее и среднее специальное образование. При этом более чем у 50% лиц, совершивших преступление в сфере компьютерной информации, имеется специальная подготовка в области автоматизированной обработки информации.

Возраст лиц, совершающих правонарушения в области компьютерной информации, как правило, составляет от 15 до 45 лет, при этом все чаще правонарушителями становятся молодые люди, а иногда и лица, не являющиеся субъектами преступления. Данные статистики свидетельствуют, что возраст 33% преступников не превышает 20 лет.

В последнее время отмечается устойчивый рост числа компьютерных преступлений. Это связано как с криминализацией отдельных составов в новом Уголовном кодексе РФ, так и с распространением компьютерной техники, ее доступностью, простотой и удобством в использовании. С появлением глобальных компьютерных сетей, например, сети открытого доступа интернет, с помощью которой

компьютерные преступления могут совершаться в одном государстве, а преступный результат наступит в другом, причем следы преступлений могут оказаться в ряде третьих государств. Обращается внимание на важность определения в данной ситуации юрисдикции государства, то есть о компетенции судебных и административных органов государства по рассмотрению и разрешению компьютерных преступлений.

Одной из причин, способствующей развитию компьютерной преступности, является поведение жертвы преступления, а именно принятие решения потерпевшей стороны об обращении в правоохранительные органы по факту совершения компьютерного преступления, которое зачастую делается неохотно в связи с различными обстоятельствами.

Таким образом, можно заключить, что одной из основных причин роста числа совершаемых компьютерных преступлений является их высокая латентность, и, как следствие, безнаказанность. Кроме этого, зачастую, средства массовой информации создают у граждан, и в первую очередь у молодёжи, неправильное представление об ответственности за совершение компьютерных преступлений, об институте интеллектуальной собственности, создают неадекватный образ компьютерного преступника.

Кононов О.А., Кононова О.В., Попенко Н.В.
Россия, Санкт-Петербург, Смольный институт РАО,
Санкт-Петербургский государственный университет аэрокосмического приборостроения,
Москва, Президиум РАН

ПРАВОВЫЕ ВОПРОСЫ ЭЛЕКТРОННОЙ БИБЛИОТЕКИ

В условиях современного информационного общества цели и задачи, стоящие перед библиотеками организаций, институтов, университетов существенно расширяются. Благодаря развитию информационных технологий и средств телекоммуникаций повышается мобильность обновления и доставки информации, и, прежде всего, технической, библиографической, учебной, научной и т.п. к субъектам профессиональной деятельности. Библиотека постепенно превращается из хранилища знаний в информационный центр, способный не только предоставлять потенциальным пользователям и читателям целесообразно организованную информацию из книг, учебников, монографий и периодических изданий, но и обеспечивать доступ к гипертекстовым обучающим и контролирующим системам, полнотекстовым документам, видео- и аудиодокументам, а также к оперативной информации внутри организации или учебного заведения.

Можно выделить следующие основные уровни электронных библиотек:

– внутриучрежденческие (библиотеки, научные организации, учебные заведения и др.);
– региональные, объединяющие электронные библиотеки различных библиотек региона;
– межрегиональные электронные библиотеки, включающие библиотеки разных регионов.

Автоматизированные библиотечно-информационные системы имеют следующие особенности: построение системы на открытых технологиях; использование Интернет-архитектуры, а также трехуровневой архитектуры при наличии на клиентских местах только программы просмотра Web; полная интеграция с Интернетом; обеспечение поиска и обработки полнотекстовых документов; эргономичный графический интерфейс пользователя; масштабируемость; поддержка российских и международных стандартов передачи и хранения информации; реализация штрих-кодовых технологий обслуживания клиентов в читальных залах.

Электронная библиотека должна:

– иметь единую базу данных (фонд), содержащую электронные документы с единым пользовательским интерфейсом доступа из одной точки ко всем коллекциям;
– иметь систему метаданных, в первую очередь – электронный каталог;
– использовать технологию надежного накопления, сохранения и использования электронных документов.

Развитие информационных ресурсов в библиотеках, музеях, архивах, способствующих созданию и использованию электронных документов, автоматизированных информационных центров, электронных библиотек, служб электронной доставки документов, доступных через электронную почту, через глобальные телекоммуникационные системы и сеть Интернет происходит в условиях, когда правовое обеспечение не соответствует потребностям общества. В этой ситуации библиотеки, музеи, архивы, с одной стороны, обязаны соблюдать права авторов произведений, с другой, обеспечить широкое использование их произведений в целях образования, просвещения и научной деятельности пользователей (читателей, посетителей). Эти вопросы постоянно возникают в повседневной деятельности этих учреждений и имеют юридический и практический характер.

В этой ситуации особую актуальность приобретают вопросы организационно-правового обеспечения конкретных направлений функционирования электронных библиотек, освоение специалистами библиотечно-информационных служб обширного массива законодательных и иных нормативных актов, регулирующих оптимальные формы взаимоотношений и взаимодействия с пользователями и партнерами.

Кононов О.А., Кононова О.В., Попенко Н.В.
Россия, Санкт-Петербург, Смольный институт РАО,
Санкт-Петербургский государственный университет аэрокосмического приборостроения,
Москва, Президиум РАН

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ЭЛЕКТРОННОЙ ПОЧТЫ

Сегодня в условиях преобразования индустриального общества в информационное с его возможностями связи «каждого с каждым» и доступа к мировому информационному фонду изменяется и поднимается на более высокую ступень характер, стиль и интенсивность общения между людьми, появляется возможность значительно повысить уровень информированности каждого члена общества. Это, несомненно, влияет на социальную природу человека, социальную организацию общества, на его социальные коммуникации.

Следствием этого является изменение и значительный рост роли социально-экономических отношений между субъектами инфокоммуникационного взаимодействия таких областей социологии как социальный контроль, социальные нормы и санкции, агенты формального и неформального контроля, номенклатура, мафия и закрытая группа и ряд других областей.

Сказанное связано с информационной безопасностью личности, общества и государства, что обусловлено все большей «прозрачностью» и уязвимостью различных сторон жизни и деятельности людей для внешнего воздействия. На решение этих проблем нацелены социальные институты информационной безопасности, определяющие систему «правил игры» в обществе и активно формирующиеся в настоящее время.

В докладе рассматриваются правовые аспекты информационного взаимодействия на примере правового обеспечения электронного письма и средств его передачи.

Одним из наиболее распространенных способов передачи электронных писем является электронная почта – первый и наиболее распространенный из сервисов Интернета. Электронная почта – типичный сервис отложенного чтения. Сообщение, как правило, посылается в виде обычного текста, адресат получает его на свой компьютер и читает сообщение тогда, когда ему будет удобно.

Изобретателем электронной почты считается Рэй Томлинсон, соединивший в 1971 году с помощью специальной почтовой программы пользователей удаленных компьютеров электронной сети «Arpanet». Для этого была разработана система организации почтовых адресов на удаленных ЭВМ. При работе с программой каждому пользователю локальной машины присваивался адрес, состоящий из его имени и сетевого имени его компьютера, разделенных знаком «@». Этот знак использовался Р. Томлинсоном вместо предлога «at» (на), т.е. выражение user@machine означает: пользователь такой-то на компьютере таком-то. Местонахождение «почтового ящика» каждого пользователя «Arpanet» становилось однозначно определенным, что дало возможность осуществлять обмен сообщениями между ними.

Таким образом, уже в 70-е годы прошлого века были заложены основные возможности и механизмы работы электронной почты, которые усовершенствуются и используются в современных почтовых программах и серверах.

В то же время за прошедшие десятилетия накоплен богатый опыт борьбы с различными видами мошенничества при использовании электронной почты.

В докладе показано, что при правовой квалификации преступлений в области использования электронной почты можно использовать существующее законодательство, опираясь, прежде всего, на Уголовный кодекс Российской Федерации, а также отмечаются возможные уголовные наказания за преступления в области ее использования.

Кучерявый М.М.
Россия, Санкт-Петербург, Управление ФСТЭК России

К ВОПРОСУ ПРАВОВОГО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ПРОИЗВОДСТВЕННЫМИ И ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФРАСТУКТУРЫ

Модельный закон Межпарламентской Ассамблеи СНГ «Об информации, информатизации и защите информации», принятый в 2005 г., полностью скопировал структуру и содержание принятого десятилетие назад первого российского закона с аналогичным названием. В свое время этот российский закон положил начало формированию общей системы нормативно-правовых актов, регулирующих процессы информатизации общества, В названном законе дано общее понятие информации как сведений о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. Предметом закона законодатель сделал документированную информацию – такую, которая зафиксирована на материальном носителе с реквизитами, позволяющими её идентифицировать. При таком определении информация рассматривалась как информационный ресурс, выступающий в форме отдельных документов, их массивов в информационных системах. Закрепление в законодательной форме условий правового режима для

информационного ресурса определенного субъекта создавало реальную почву для обеспечения всех форм права на информацию.

Быстро развивающиеся процессы информатизации влекут необходимость расширения границ правового поля информационных отношений и опережают их нормативно-правовое опосредование. Вовлечение информационной продукции в экономический оборот актуализирует проблему реализации имущественных прав на информацию. Проблема осложняется необходимостью законодательного обеспечения широкого доступа к информации – с одной стороны, и определения границ такого доступа с учетом интересов государства, юридических и физических лиц – с другой. Создание и использование глобальных общедоступных информационных систем и сетей передачи данных сопровождалось появлением новых видов преступлений – компьютерных, что вызвало необходимость в создании правовых мер борьбы с ними. Все сказанное требует развития, совершенствования и гармонизации информационного законодательства, касается и базового закона, каковым по своему статусу призван быть закон об информации.

В Российской Федерации в 2006 г. на смену закону об информации 1995 г. пришел новый базовый закон «Об информации, информационных технологиях и о защите информации», который регулирует отношения при осуществлении права на поиск, получение, передачу, производство и распространение информации, при применении информационных технологий, а также при обеспечении защиты информации. Разработка этого закона была обусловлена необходимостью унификации, как с понятийной, так и с содержательной точки зрения принципов и правил взаимодействия в данной сфере, устранения в ней ряда пробелов и приближения к международной практике регулирования общественных отношений.

В последующие годы в российский закон «Об информации, информационных технологиях и о защите информации» предлагались и вносились изменения, касавшиеся как понятийного аппарата, так и содержательных аспектов. Представляется, что аналогичные вопросы актуальны и в плане совершенствования и гармонизации информационного законодательства в Содружестве Независимых Государств. Однако Модельный закон МПА СНГ «Об информации, информатизации и защите информации» с момента его принятия остается в первозданном виде.

Обострившиеся сегодня проблемы обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры требуют своего правового опосредования. В связи с этим представляется, что заслуживает внимания рассмотрение вопроса о внесении в законы об информации дополнений, нацеленных на повышение эффективности защиты информации в государственных информационных системах и информационных системах критически важных объектов. Такое предложение основывается на опыте проведения ФСТЭК России работ в области защиты информации с применением национальных и международных стандартов.

Мазнев В.Б.
Россия, Санкт-Петербург, Межрегиональный институт экономики и права при МПА ЕврАзЭС

ПРОБЛЕМЫ КИБЕРПРЕСТУПНОСТИ И КИБЕРБЕЗОПАСНОСТИ: АКТУАЛЬНЫЕ РИСКИ И ВОЗМОЖНОСТИ ПРОТИВОДЕЙСТВИЯ (ПРАВОВОЙ АСПЕКТ)

Рассматриваются проблемы киберпреступности, дано определения таким явлениям, как виртуальность и виртуальная реальность, киберпреступность, компьютерные преступления, чтобы отграничить их друг от друга и от смежных понятий. Киберпреступление — это признаваемые уголовно-наказуемыми противоправные действия (или бездействие) в киберпространстве, т.е. в глобальной компьютерной сети (вычислительной сети, сети передачи данных, включая систему связи компьютеров или компьютерного оборудования, где для передачи информации используются различные физические явления, такие как электрические и световые сигналы или радиомагнитное излучение), с использованием компьютера (ноутбука, смартфонов, информационных носителей) и (или) и программных продуктов для них, с использованием или применением информационно – коммуникационных технологий.

Киберпреступность носит в значительной степени транснациональный характер. Первоначально Интернет был задуман как сеть военного назначения с рассредоточенной архитектурой. Такая сетевая архитектура и возможность глобального доступа к соответствующим услугам часто придают киберпреступлениям международный аспект. Электронные письма с запрещенными материалами без труда пересылаются по адресам в целом ряде государств, даже когда их исходный отправитель и конечный получатель находятся в одной и той же стране, например, если отправитель либо получатель пользуются услугами зарубежного провайдера электронной почты. Тот факт, что клиентами некоторых популярных провайдеров, предоставляющих почтовые услуги бесплатно, являются миллионы людей на всей планете, дополнительно подчеркивает транснациональные масштабы киберпреступности.

В Европейской Конвенции о преступности в сфере компьютерной информации, (межд. регистрационный номер ETS №185) вместо понятия «компьютерная сеть» используется понятие «компьютерная система» под которым понимается любое устройство или совокупность соединенных

между собой или связанных устройств, одно либо более из которых осуществляет автоматическую обработку данных в соответствии с программой.

Еще одно общее принятое определение описывает киберпреступность (в широком смысле) как любое деяние, в котором инструментом, целью или местом совершения преступных действий являются компьютеры или сети Недостатком такого определения является то, что сюда можно отнести традиционное определении преступности (убийство), например, можно ударить жертву ноутбуком по голове и убить. В проекте Международной Конвенции по улучшению защиты от киберпреступности и терроризма («Стенфордский проект») сказано, что киберпреступностью называются действия в отношении кибернетических систем В других источниках киберпреступность определяется как «действия, осуществляемые посредством компьютеров, которые являются незаконными, либо считаются противоправными некоторыми сторонами и которые могут быть совершены с помощью глобальных электронных сетей».

Одним из возможных подходов к противодействию киберпреступности в ее транснациональном аспекте и развитию международного сотрудничества являются выработка и стандартизация соответствующего законодательства. В последние годы в разных регионах был применен ряд подходов к решению этой задачи.

Говоря о России, характеризуя институциональный компонент обеспечения кибербезопасности, можно отметить, что, в отличие от Европейского Союза и некоторых государств-членов (например, ФРГ), в РФ отсутствует специальное ведомство, ответственное за кибербезопасность. Основные функции в данной сфере рассредоточены между органами исполнительной власти: Федеральной службой безопасности, Службой внешней разведки, Федеральной службой охраны, Министерством внутренних дел, Министерством обороны, Федеральной службой по техническому и экспортному контролю, Федеральной службой по надзору в сфере связи, информационных технологий и массовым коммуникациям, Национальным антитеррористическим комитетом, Государственным антинаркотическим комитетом и др.

Учитывая глобальный характер вопроса обеспечения кибербезопасности считаем целесообразным создать в РФ орган для координации работы по обеспечению кибербезопасности между выше перечисленными органами исполнительной власти, например: «Агентство информационной безопасности».

Макаров О.С.
Беларуссия, Минск, ГУО Институт национальной безопасности

О НЕКОТОРЫХ АСПЕКТАХ ХАРАКТЕРИСТИКИ ПРАВОВЫХ МЕР ЗАЩИТЫ ГОСУДАРСТВЕННЫХ СЕКРЕТОВ ГОСУДАРСТВ-УЧАСТНИКОВ СНГ

Характеристика подсистемы правовых мер защиты государственных секретов является важной научной задачей, поскольку её совершенствование является необходимым условием обеспечения безопасности государственных секретов (и, как следствие, национальной безопасности) и соблюдения баланса прав и интересов субъектов данных отношений. Принципиально важным является то, что правовое регулирование защиты государственных секретов имеет конституционно-правовую основу. Хотя сравнительно-правовое исследование законодательства государств-участников СНГ в сфере защиты государственных секретов показывает, что не во всех Конституциях государств Содружества непосредственного закреплен такой вид государственной деятельности, как защита государственных секретов, – все государства-участники СНГ в качестве правовой основы института защиты государственных секретов определяют национальные Конституции.

Представляется, что правовой основой деятельности государства по защите государственных секретов является установленное в национальных Конституциях право самостоятельно защищать свою независимость и территориальную целостность, конституционный строй, обеспечивать законность и правопорядок. Защита указанных атрибутов государственности осуществляется в рамках обеспечения национальной безопасности. Кроме этого, осуществляя регулирование оборота государственных секретов, государство реализует установленные в Конституции исключительные права на обладание отдельными объектами и на осуществление отдельных видов деятельности. Необходимо отметить, что в соответствии с законодательством большинства государств-участников СНГ, государственные секреты являются категорией объектов исключительной собственности государства. Также конституционный характер деятельности по защите государственных секретов обусловлен тем, что защита государственных секретов влечет законодательное ограничение отдельных закрепленных в Конституции прав граждан. Правомерность подобных ограничений возможна только при их конституционном закреплении и в условиях необходимости достижения конкретных общественно-значимых целей (в данном случае – обеспечения национальной безопасности). Таким образом, государство, основываясь на конституционных нормах и принципах, соблюдая баланс между частными и публичными интересами, устанавливает особый режим защиты сведений, составляющих государственные секреты.

Наиболее ярким проявлением публично-правового характера отношений в сфере государственных секретов является неравенство сторон рассматриваемых отношений, проявляющееся в наложении государством ряда ограничений на иных субъектов отношений. Сравнительно-правовой анализ национального и зарубежного законодательства в сфере оборота государственных секретов позволяет выделить типичные ограничения:

– ограничение права на выезд лиц, осведомленных о сведениях, составляющих государственные секреты,

– ограничение права на распространение сведений, составляющих государственные секреты,

– ограничение права на неприкосновенность частной жизни лиц, допускаемых к государственным секретам,

– ограничение права на использование открытий и изобретений, содержащих государственные секреты.

Указанные ограничения касаются конституционных прав: права на свободу выбора места жительства, права на свободу передвижения, права на свободный поиск, получение информации, право на свободу слова, право на обладание собственностью, право на неприкосновенность личной жизни.

Субъектами ограничения являются граждане (в ряде стран под гражданами понимаются граждане страны, лица без гражданства и иностранцы, но в большинстве стран – только граждане данной страны). Для иностранцев, как правило, существуют отдельные ограничения (например, особый порядок доступа), либо вообще запрет на приобретение прав, связанных с государственными секретами.

Ограничения закрепляются законодательно.

Ограничения носят срочный характер.

Ограничения носят возмездный характер (подлежат компенсации).

Ограничения носят добровольный характер (за исключением запрета в отдельных странах на распространение сведений лицами, отказавшимися от заключения договорных отношений по поводу засекречивания находящихся у них в собственности сведений).

Ограничения носят договорной характер. Как правило, ограничения не распространяются на лиц, не находящихся в договорных отношениях по поводу защиты государственных секретов.

Ограничения обеспечиваются системой государственного контроля их соблюдения.

Ограничения обеспечиваются ответственностью за их нарушение.

Макаров О.С.
Беларуссия, Минск, ГУО «Институт национальной безопасности Республики Беларусь»

К ВОПРОСУ О СУЩНОСТНОЙ ХАРАКТЕРИСТИКЕ ГОСУДАРСТВЕННЫХ СЕКРЕТОВ КАК ИСТОЧНИКА ПОВЫШЕННОЙ ОПАСНОСТИ

Актуальной научной проблемой в сфере государственных секретов, как представляется, является недостаточная теоретическая разработанность самого феномена государственных секретов, что порождает и недостаточную эффективность возникающих правоотношений.

Сравнительный анализ законодательства государств-участников СНГ, регламентирующего сферу государственных секретов, позволяет выделить два подхода к определению сущности данного феномена. В соответствии с первым подходом, который иллюстрируется законодательством Республики Казахстан и модельным законодательством Межпарламентской Ассамблеи СНГ, в качестве предназначения государственных секретов определяется обеспечение эффективной деятельности государства. Второй, в известной мере традиционный подход, который представлен в законодательных актах Республики Беларусь, Российской Федерации и ряда других государств, исходит из того, что основной характеристикой государственных секретов является возможность причинения вреда национальной безопасности в случае их разглашения.

Сегодня второй из обозначенных подходов является доминирующим. Вместе с тем следует заметить, что определение в качестве характеризующего феномен государственных секретов критерия «эффективность государственной политики» видится прогрессивным подходом, больше отвечающим сущности государственных секретов. Ведь, если в качестве критерия определить ущерб национальной безопасности, – какой смысл генерировать секреты, вероятно, лучшим выходом было бы отказаться от данного института.

Наличие государственных секретов является благом для государства, способствует повышению обороноспособности, экономической мощи страны. Государство создает государственные секреты в целях получения преимуществ в геополитической конкуренции, а их способность причинить ущерб безопасности собственника представляется «побочным эффектом».

Как известно, в праве существует механизм трансформации качественной характеристики интереса, в случае его не достижения, в качественную характеристику ущерба через институт упущенной выгоды. Однако, по нашему мнению, необходимо дифференцировать позитивную цель

секретов и их деструктивное свойство, так как объединение процессов прогресса и безопасности в одну категорию порождает методологическую сложность их защиты.

Наличие у государственных секретов, как объекта правового регулирования, ярко выраженных позитивного «целевого» и деструктивного «побочного» свойств обуславливает его схожесть с источником повышенной опасности. Научная проблема распространения на информацию юридической конструкции источника повышенной опасности уже рассматривалась ведущими учеными в сфере информационного права.

Традиционным признаком источника повышенной опасности является его характеристика как объекта материального мира, либо деятельности, связанной с таким объектом. Государственные секреты также не существуют без материального носителя (свойство неотчуждаемости). В пользу сходства государственных секретов с категориями источника повышенной опасности свидетельствует и такое специфическое их (секретов) свойство как источника повышенной опасности, как необратимость возможных деструктивных процессов. Действительно, процесс разглашения сведений, составляющих государственные секреты, на определенном этапе его протекания не подлежит стабилизации, восстановление конфиденциальности разглашенных неопределенному кругу лиц сведений становится не возможным.

Определенное сходство источника повышенной опасности и государственных секретов дает основание попытаться обосновать применение в отношении последних механизма правового регулирования, разработанного для источника повышенной опасности, как личная безвиновная ответственность.

Максимова Е.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

РАЗВИТИЕ СИСТЕМЫ НОРМАТИВНОГО ПРАВОВОГО РЕГУЛИРОВАНИЯ ОТНОШЕНИЙ В ОБЛАСТИ СОЗДАНИЯ И ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Развитые страны переживают новый этап научно-технической революции, связанный с возрастанием роли информации в обществе. Правовые проблемы регулирования информационных отношений при построении информационного общества в настоящее время нуждаются в тщательном исследовании, поскольку резко ускоряющиеся информационно-коммуникативные процессы эволюционируют в качественно новое состояние – режим реального времени. Вследствие «проникновения» информатизации в повседневную жизнь граждан проблемы информационной безопасности прямо или косвенно стали касаться интересов практически каждого человека. Возникающие в связи с этим новые общественные отношения нуждаются в адекватном правовом регулировании.

Одним из необходимых условий развития информационного общества является развитие системы нормативного правового регулирования отношений в области создания и использования информационно-телекоммуникационных технологий. Обеспечение информационной безопасности должно быть направлено на защиту конституционных прав и свобод личности, информационное обеспечение государственной политики, обеспечение безопасности информационных ресурсов России и надежное функционирование информационных и телекоммуникационных систем. Таким образом, создание эффективной системы информационной безопасности России – это комплексная проблема, успешное решение которой возможно при целенаправленной совместной работе государственных, коммерческих и общественных институтов страны.

Правовая защита информации предполагает наличие регламентации прав на информацию; реализации их; контроля за процедурами реализации данных прав. Современный этап развития полностью зависит от информационных ресурсов и технологий, их качества и безопасности и характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информационных ресурсов, информационной инфраструктуры, систем формирования, распространения, использования информации и регулирования возникающих при этом отношений. При этом существенно возрастает общественная значимость информационных отношений. В самом общем виде «правовой режим информации» следует понимать как совокупность нормативно установленных правил, определяющих:

– права собственности, владения и распоряжения информацией;

– степень открытости информации (необходимость или возможность ее отнесения к категории ограниченного доступа);

– порядок отнесения информации к категории ограниченного доступа и перечень уполномоченных на это лиц;

– порядок документирования, доступа, хранения, контроля и распространения информации;

– нормы, регулирующие применение различных средств и методов обеспечения информационной безопасности;

– порядок привлечения к ответственности и меры наказания за нарушение установленных норм и правил в области информационных отношений.

Комплексное изучение установленных норм и правил в конкретной прикладной области всегда является обязательным элементом культуры работающего в этой области специалиста.

Правовое обеспечение информационной безопасности охватывает (или должно охватывать) все многообразие юридических вопросов, возникающих в этой области и, следовательно, находит свое отражение в целом комплексе законодательных актов.

Законодательный уровень является важнейшим для обеспечения информационной безопасности. Правовые вопросы защиты информации достаточно разнообразны, как разнообразны и способы использования информации. Самое важное на законодательном уровне создать механизм, позволяющий согласовать процесс разработки с реалиями и потребностями, прогрессом развития современного общества, в частности развития в сфере информационных технологий. Законы не могут опережать жизнь, но важно, чтобы они шли в ногу со временем, так как на практике это может приводить к снижению информационной безопасности. В информационном обществе нормативно-правовая база в области информационной безопасности должна быть согласована с международной практикой. Подводя итог можно отметить следующие действия на законодательном уровне: разработка законов с учетом категорий субъектов всех информационных отношений, обеспечение баланса конструктивных и ограничительных законов, интеграция в мировое правовое пространство, учет современного развития информационных технологий.

Нигметов Н.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

СОДЕРЖАНИЕ ОПЕРАТИВНО-РОЗЫСКНЫХ МЕРОПРИЯТИЙ В СЕТИ ИНТЕРНЕТ

Основным мероприятием, реализуемым в Интернете оперативно-техническими подразделениями, является снятие информации с технических каналов связи.

Следует учитывать, что в каждый конкретный момент времени информация может находиться в одной из двух форм: а) храниться на машинном носителе; б) передаваться по каналу связи. СИТКС осуществляется в отношении передаваемых данных: их сбор производится в реальном масштабе времени путем перехвата за счет использования программного обеспечения и специальной аппаратуры, подключенной к каналу связи.

Перехват данных при СИТКС может осуществляться в двух формах. Пассивный перехват предполагает слежение за передаваемыми по каналу связи сообщениями без вмешательства в их поток (с данных снимается копия, а сами они направляются по назначению), что обеспечивает конспирацию (отправитель и получатель не наблюдают признаков перехвата). При активном перехвате над сообщениями выполняются определенные действия: сообщения могут быть изменены, уничтожены, задержаны, переупорядочены и т.п.

Особое содержание в сетевом пространстве приобретает ОРМ «отождествление личности». Как правило, такое ОРМ основывается на сопоставлении полученных из оперативных источников данных о личности фигуранта, причастного к преступной деятельности, со сведениями о субъекте, сетевая активность которого изучается.

К специфическим формам отождествления личности можно отнести опознание по фотографиям, размещаемым на персональных страницах социальных сетей («Одноклассники», «ВКонтакте» и др.), по указанным там же автобиографическим данным, по используемым псевдонимам («никам»), адресам электронной почты, номерам ICQ, IP-адресам и т.п.

Функционирование в Интернете мощных справочно-информационных систем создает условия для наведения справок путем непосредственного изучения размещенных в них документов, а также направления по электронной почте запросов в организации, обладающие интересующими сведениями.

Одним из наиболее сложных ОРМ при реализации в сетевом пространстве представляется оперативный эксперимент. Международной практике известны примеры осуществления оперативного эксперимента, связанные с созданием в сетевом пространстве негласно контролируемых объектов, которые представляли интерес для преступников (например, хакерских сайтов).

Интересен пример проведения ФБР подобных действий в отношении российских хакеров, осуществлявших взломы сайтов на территории США. Для разоблачения преступников была создана фиктивная интернет-компания «Invita». После «успешного» взлома ее системы защиты хакерам была предложена работа в компании в качестве консультантов по проблемам безопасности. Изображавшие руководителей компании агенты ФБР попросили прибывших в США хакеров продемонстрировать свои навыки. Все действия регистрировались специальным программным обеспечением, велась скрытая видеозапись. После завершения «собеседования» хакеры были задержаны, им было предъявлено обвинение.

Увеличение количества торговых операций, реализуемых через Интернет, заставляет расширять практику использования и ОРМ «проверочная закупка и контролируемая поставка» с

целью выявления преступлений в сфере торговли (например, фактов обмана покупателей интернет-магазинов, интернет-аукционов) и в сфере распространения запрещенных к обороту объектов (наркотических средств, материалов, содержащих детскую порнографию, и др.). Так, практике известны примеры успешного применения проверочной закупки и использования возможностей сети Интернет в ходе реализации контролируемых поставок наркотических средств.

Пожалуй, в наше время трудно найти человека, который не был бы знаком с сетью Интернет. Его можно назвать одним из феноменов нашего века. Интернет прочно вошел в нашу жизнь, регулируя многочисленные вопросы повседневности. Благодаря «всемирной паутине» любому из нас ничего не стоит получить доступ к нелегально добытым данным, фильмам, аудиофайлам, даже не подозревая, что в это время он, например, нарушает, многочисленные авторские права. Уникальность сети Интернет состоит в том, что она не находится во владении какого-либо одного физического или юридического лица, государственного ведомства или отдельной страны. В результате практически во всех сегментах паутины отсутствует государственное регулирование, цензура и другие формы контроля над информацией, циркулирующей в ней. Это открывает неограниченные возможности для доступа к любым файлам, которые все шире используются в преступной деятельности, и распространение которых пока что практически невозможно контролировать.

Таким образом, исходя из вышеуказанных в данной статье факторов о преступности в глобальной сети Интернет, можно сделать вывод о том, что необходимо определенное вмешательство со стороны государства в регулирование данной сферы, так как Интернет занимает не просто часть жизни современного человека, но и затрагивает его права и обязанности. Именно в этом случае как никогда возрастает роль ОВД, в частности сотрудников оперативного аппарата по выявлению, пресечению и расследованию преступлений в сети Интернет посредством проведения тактически грамотных и спланированных оперативно-розыскных мероприятий.

Однако на данном этапе несовершенство норм не позволяет в должной степени обеспечить свободу и контроль одновременно. Тем не менее, ключевым и позитивным моментом является создание первой судебной практики и определенная заинтересованность отечественных юристов к данной теме.

Перевалов Д.В., Вус М.А.
Беларуссия, Минск, ГУО «Институт национальной безопасности Республики Беларусь»,
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

О ПРОЕКТЕ МОДЕЛЬНОГО ЗАКОНА МПА СНГ «О КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТАХ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ»

Совершенствование безопасности функционирования информационных и телекоммуникационных систем критически важных объектов инфраструктуры и объектов повышенной опасности предусмотрено Стратегиями национальной безопасности государств – участников СНГ. Государственная политика в области обеспечения безопасности систем управления производственными и технологическими процессами имеет целью снижение до минимального уровня рисков неконтролируемого вмешательства в процессы функционирования информационных и телекоммуникационных систем и автоматизированных систем управления на таких объектах.

Проектом подготовленной к принятию на 39-м пленарном заседании МПА СНГ Межгосударственной программы совместных мер борьбы с преступностью предусматривается разработка в 2014 г. модельного закона «О критически важных объектах информационно-коммуникационной инфраструктуры» (КВО ИКИ). Предметом правового регулирования такого закона должны выступать общественные отношения, складывающиеся в сфере охраны и защиты национальных интересов государств Содружества при эксплуатации КВО ИКИ. Данные общественные отношения возникают, развиваются и прекращаются: в процессе осуществления государственными органами властной деятельности по реализации мер обеспечения безопасности КВО ИКИ; при осуществлении собственниками КВО ИКИ данной деятельности; при создании условий для обеспечения эффективности деятельности по реализации мер обеспечения безопасности КВО ИКИ.

В докладе обсуждается примерная структура предлагаемого проекта модельного закона МПА СНГ «О критически важных объектах информационно-коммуникационной инфраструктуры»:

Глава 1. Общие положения, понятийный аппарат.

Глава 2. Государственное управление в области обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры.

Глава 3. Отнесение объектов информационно-коммуникационной инфраструктуры к критически важным.

Глава 4. Организация функционирования критически важных объектов информационно-коммуникационной инфраструктуры.

Глава 5. Обеспечение безопасности критически важных объектов информационно-коммуникационной инфраструктуры.

Глава 6. Ответственность за нарушение законодательства в области обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры.

Глава 7. Исключение объектов информационно-коммуникационной инфраструктуры из числа критически важных.

Глава 8. Государственный контроль за обеспечением безопасности критически важных объектов информационно-коммуникационной инфраструктуры.

Глава 9. Порядок вступления закона в силу.

Представляется, что эффективное решение задач по охране и защите национальных интересов государств Содружества при эксплуатации КВО ИКИ возможно только при скоординированной деятельности всех заинтересованных компетентных государственных органов стран СНГ и вовлечении собственников КВО ИКИ в данный процесс. При этом определяющее значение имеют не столько действия уполномоченных государственных органов и других организаций по локализации и ликвидации последствий нарушения функционирования КВО ИКИ, сколько превентивные действия по выявлению угроз безопасности КВО ИКИ и их нейтрализации на стадии зарождения и насыщения.

Сагайдак А.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ПРОФИЛАКТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Современный период развития общества характеризуется ростом преступности и ее качественными изменениями. Развитие высоких технологий создает условия для появления новых форм и видов злоупотреблений техническими средствами, в том числе и в преступных целях.

Компьютеры представляют сегодня огромный потенциал всевозможной информации, имеющий в некоторых случаях и конфиденциальный характер. Люди беспокоятся о безопасности таких сведений и наличии рисков по предоставлению открытого доступа к персональным данным. В этом случае информация представляет собой ресурс, который необходимо защищать.

Преступления в сфере компьютерной информации имеют высокую латентность. Сегодня на государственном уровне принят ряд базовых нормативно-правовых актов в области информационных отношений, регулирующих данные вопросы.

Возрастает и значение мер профилактики, направленных на исключение возможности противоправного использования компьютерных технологий. Воздействие на преступность основывается на ряде принципов: во-первых, оно должно носить системный характер; во-вторых, деятельность общества в этом направлении должна быть в достаточной мере обеспечена материально и технически; в-третьих, система воздействия должна претерпевать изменения в соответствии с изменениями, происходящими в обществе и в структуре преступности.

Необходимо также отметить, что в процессе воздействия на преступность должны принимать участие все граждане государства, только при их полной поддержке общество может иметь достаточно ресурсов для действенных мер, направленных на противодействие компьютерной преступности. Важным принципом является и то, что воздействие на преступность должно носить стабильный, поступательный и системный характер.

В современных условиях меры компьютерной информационной безопасности направлены на обеспечение трех основных свойств: конфиденциальность, целостность, готовность информации и средств ее обработки.

В зависимости от детерминирующих факторов, преступлений в сфере защиты компьютерной информации выделяют общесоциальный, специально-криминологический и индивидуальный уровни профилактики данной преступности.

Общесоциальный уровень профилактики включает, деятельность государства и общества, их институтов, направленную на разрешение противоречий, возникающих в различных областях общественной жизни. На этом уровне с учетом специфики компьютерных преступлений необходима продуманная государственная политика в области борьбы с данного рода преступностью.

Специально-криминологический уровень выражен в профилактической деятельности отдельных групп компетентных органов, направленных на предупреждение преступлений в сфере компьютерной информации.

На индивидуальном уровне проводится воздействие на конкретного субъекта – правонарушителя.

Основными направлениями профилактики и борьбы с компьютерной преступностью сегодня являются:

а) введение соответствующих изменений в уголовное законодательство по вопросам защиты информации;

б) усиление мер безопасности против возможных злоупотреблений пользователей электронных ресурсов и поиска более совершенных средств защиты компьютерной техники и информационных сетей;

г) использование новых форм и методов предупреждения компьютерной преступности, основанных на учете ее особенностей: введение обязательного страхования некоторых видов деятельности, связанной с обработкой персональных конфиденциальных сведений о гражданах; выявление латентных жертв с целью выявления латентных преступлений; изучение их характеристик с целью выявления характера преступника, выбравшего данную жертву; переориентации компьютерных преступников с целью привлечения их навыков и умений для борьбы с компьютерной преступностью; профессиональная экспертиза степени защищенности компьютерных систем; анализ риска существования угрозы и возможных последствий несанкционированного доступа к компьютерным системам.

Современные компьютерные технологии активно внедряются во все сферы жизни общества. Национальная безопасность начинает напрямую зависеть от обеспечения информационной защиты – главного гаранта стабильности в обществе.

Смирнова О.Г.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

СРАВНИТЕЛЬНЫЙ АНАЛИЗ КЛАССИФИКАЦИЙ КИБЕРПРЕСТУПЛЕНИЙ И ИХ СВЯЗЬ С УГОЛОВНЫМ ЗАКОНОДАТЕЛЬСТВОМ РФ

Современные компьютерные технологии в настоящее время охватывают практически все сферы социальной жизни общества. Внедрение современных компьютерных технологий привело к новым видам преступлений, связанных с электронно-вычислительными машинами. Данный вид преступлений получил у общества распространенное название – киберпреступления.

Киберпреступления приобретают сегодня все более изощренный (кибертерроризм) и иногда трудноопределимый (компьютерное мошенничество) характер. Сегодня киберпреступления можно смело сравнивать с оружием массового поражения. Киберпреступность – это нарастающая угроза безопасности общества и государства, а в целом и мирового сообщества.

Безопасность в сфере информационных технологий – основная проблема государств всего мира. Конвенция Совета Европы о киберпреступности была открыта для подписания в 2001 году, а вступила в силу 1 июля 2004 года. Сегодня Конвенцию подписали 46 государств-членов Совета, а также Канада, Япония, ЮАР и США. Конвенция стала первым документом, в котором содержится классификация киберпреступлений. Конвенция Совета Европы о киберпреступности называет четыре вида компьютерных преступлений, определяя их как преступления против конфиденциальности, целостности и доступности компьютерных данных и систем:

1. Незаконный доступ – ст. 2 (противоправный умышленный доступ к компьютерной системе либо ее части).
2. Незаконный перехват – ст. 3 (противоправный умышленный перехват не предназначенных для общественности передач компьютерных данных на компьютерную систему, с нее либо в ее пределах).
3. Вмешательство в данные – ст. 4 (противоправное повреждение, удаление, нарушение, изменение либо пресечение компьютерных данных).
4. Вмешательство в систему – ст. 5 (серьезное противоправное препятствование функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, нарушения, изменения либо пресечения компьютерных данных).

Трудно с этим не согласиться, так как именно эти преступления являются компьютерными. Именно на свойства конфиденциальности, целостности и доступности данных направлена защита компьютерной информации в целом. Но есть и другая группа преступлений, которые непосредственно связаны с компьютером или совершаются с его помощью. К этим видам преступлений можно отнести: электронные кражи, мошенничество, нарушение авторских прав, распространение призывов в сети Интернет к межнациональной розни и т.д.

И сегодня, наиболее приемлемой классификацией компьютерных преступлений с учетом развития научно-технического прогресса представляется классификация, которая выделяет следующие виды киберпреступлений:

1. Насильственные или иные потенциально опасные киберпреступления, посягающие на физическую безопасность, жизнь и здоровье человека.
2. Преступления, посягающие на конфиденциальность информации – незаконный доступ к компьютерам или компьютерным системам без причинения ущерба информации.
3. Деструктивные киберпреступления, заключающиеся в повреждении данных и посягающие на целостность данных и безопасность функционирования компьютерных систем. Такие преступления также могут причинить имущественный ущерб, но они не связаны с хищением информации, данных, денежных средств.

4. Преступления, посягающие на имущество, имущественные права, а также на право собственности на информацию и авторские права.

5. Преступления, посягающие на общественную нравственность.

6. Преступления, посягающие на общественную безопасность.

7. Иные киберпреступления, совершаемые посредством компьютерных сетей, и посягающие на различные охраняемые законом объекты.

В Российском законодательстве такой вид, как компьютерные преступления был криминализирован лишь в 1996 году, когда в Уголовный кодекс Российской Федерации была введена глава 28 «Преступления в сфере компьютерной информации». Она состоит всего лишь из трех статей: неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК РФ), нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК РФ). Глобализация информационных процессов в обществе привела к открытию новых глобальных угроз безопасности, перед которыми все мировое сообщество оказалось бессильно. Приведенная выше классификация киберпреступлений требует качественного пересмотра уголовного законодательства в этой сфере, а так же создает предпосылки для новой качественной подготовки сотрудников органов внутренних дел по борьбе с данными видами преступлений.

Сорокина Е.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

СОВРЕМЕННОЕ СОСТОЯНИЕ НОРМАТИВНО-ПРАВОВОЙ БАЗЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРЕДИТНО-ФИНАНСОВОГО УЧРЕЖДЕНИЯ

В Доктрине информационной безопасности Российской Федерации, утвержденной указом президента РФ 9 сентября 2000 года говорится, что воздействию угроз информационной безопасности РФ в сфере экономики, в том числе, наиболее подвержена кредитно-финансовая система. Серьезную угрозу для нормального функционирования экономики в целом представляют преступления, связанные с получением несанкционированного доступа к данным банков и иных кредитных учреждений. Под информационной безопасностью РФ, согласно вышеупомянутой Доктрине, подразумевается «состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства». Экономическая безопасность всецело зависит от обеспечения, в том числе, информационной безопасности кредитно-финансового сектора, регламентируемой нормативно-правовыми актами, имеющими ряд пробелов и противоречий. С учетом этого анализ современного состояния нормативно-правовой базы обеспечения информационной безопасности кредитно-финансового сектора представляется весьма актуальным.

Деятельность кредитно-финансовых учреждений жестко регламентируется Законодательством РФ, стандартами Банка России, внутренней документацией. При осуществлении деятельности кредитно-финансовые учреждения руководствуются строго определенной нормативно-правовой базой. Всю совокупность оговоренной выше нормативно-правовой базы условно можно разделить на четыре группы, отдельно выделив Конституцию РФ.

В первую группу входят следующие Федеральные законы РФ: «О Центральном Банке РФ», «О банках и банковской деятельности», «О государственной тайне» (ряд положений данного документа используется, в том числе, и для создания нормативных документов по работе с информацией, составляющей коммерческую тайну), «Об информации, информатизации и защите информации» (является основой, базовым документам для осуществления деятельности службы безопасности любой организации, в том числе и кредитно-финансовых учреждений), «Об электронной цифровой подписи», «О банках и банковской деятельности», «О правовой охране программ для электронных вычислительных машин и баз данных».

Вторую группу составляют Указы Президента РФ: «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации», «О защите информационно-телекоммуникационных систем и баз данных от утечки конфиденциальной информации по техническим каналам», «О мерах по упорядочению разработки, производства, реализации, приобретения в целях продажи, ввоза в РФ и вывоза за ее пределы, а также использования специальных технических средств, предназначенных для негласного получения информации», «Об утверждении перечня сведений конфиденциального характера». Отдельно выделим Постановления Правительства: «О перечне сведений, которые не могут составлять коммерческую тайну» и «О сертификации средств защиты информации».

Четвертая группа – комплекс БР ИББС: СТО БР ИББС-1.0-2010. «Общие положения (4 редакция)», СТО БР ИББС-1.1-2007. «Аудит информационной безопасности», СТО БР ИББС-1.2-2010. «Методика оценки соответствия информационной безопасности организаций банковской

системы РФ требованиям СТО БР ИББС-1.0-20xx (3 редакция)», РС БР ИББС-2.0-2007. «Методические рекомендации по документации в области обеспечения информационной безопасности в соответствие с требованиями СТО БР ИББС-1.0», РС БР ИББС-2.1-2007. «Руководство по самооценке соответствия информационной безопасности организаций банковской системы РФ требованиям СТО БР ИББС-1.0», РС БР ИББС-2.2-2009. «Методика оценки рисков нарушения информационной безопасности», РС БР ИББС-2.3-2010. «Требования по обеспечению безопасности персональных данных в информационных системах персональных данных организаций банковской системы РФ», РС БР ИББС-2.4-2010. «Отраслевая частная модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных организаций банковской системы РФ».

Указанная нормативно-правовая база обеспечивает регламентацию комплексной защиты информации в кредитно-финансовом учреждении, но в текстах данных документов обычно берется за основу то, что в банковском секторе имеет место жесткое противопоставление друг другу интересов собственника информации и злоумышленника. Так же слабый момент перечисленных документов – это открытое заявление, что собственник информации практически никогда не обладает информацией о готовящейся информационной атаке.

Ярмоленко Н.В.
Россия, Санкт-Петербург, Санкт-Петербургский военный институт внутренних войск МВД России

ПРОБЛЕМЫ ПРАВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Статья посвящена проблеме правого обеспечения информационной безопасности. В разных контекстах словосочетание «информационная безопасность» может иметь различный смысл. Под информационной безопасностью понимают защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений. Информационная безопасность включает в себя меры не только по защите процессов создания данных, их ввода, а так же обработки и вывода данных. Таким образом, информационной безопасностью называют меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе. Исходя из этого, информационная безопасность дает гарантию того, что достигаются следующие цели: конфиденциальность критической информации; целостность информации и связанных с ней процессов (создания, ввода, обработки и вывода); доступность информации, когда она нужна; учет всех процессов, связанных с информацией.

Защита информации (данных) является одним из элементов системы безопасности информации и характеризуется комплексом мероприятий, направленных на обеспечение информационной безопасности. Ежегодно 30 ноября отмечается Международный день защиты информации. Его целью является напоминание пользователям о необходимости защиты компьютеров и всей хранимой в них информации. 2 ноября 1988 года была зафиксирована первая массовая эпидемия «червя» Морриса, получившего название по имени своего создателя - Роберта Морриса, аспиранта факультета Вычислительной техники Корнельского университета.

В 2000 г. Президентом РФ была утверждена Доктрина информационной безопасности Российской Федерации. Она определила политику нашего государства в информационной сфере на ближайшую перспективу, а именно, закрепила понятие информационной безопасности, обозначила основные виды угроз информационной безопасности и методы ее обеспечения, определила основные положения государственной политики обеспечения информационной безопасности и организационную основу системы обеспечения информационной безопасности.

Среди российских законов, которые посвящены вопросам информационной безопасности, является Федеральный закон «Об информации, информационных технологиях и о защите информации». Закон действует с 27 июля 2006 года за номером 149-ФЗ. В нем даются не только основные определения, но и намечаются направления развития законодательства в данной области. Согласно второй статье информационные технологии – это процессы, методы поиска, сбора, хранения, обработки, предоставления информации и способы осуществления таких процессов и методов, но нет упоминания о программных и аппаратных средствах. В статье 2 дается определение информационной системы, представляющей собой совокупность содержащейся в базах данных информацию и обеспечивающих ее обработку информационных технологий и технических средств. Таким образом, технология является частью системы, в которую еще входят информация баз данных и технические средства, отсутствует упоминание о программных и аппаратных средствах.

Но в законопроекте только упоминаются модификация, подмена и уничтожение, осуществляемые неправомочным способом, но не дается определение свойств, квалифицирующих данные действия. Информационные процессы являются основным понятием в информационных технологиях. К сожалению и здесь правила формулирования определений нарушены. Фактически определение информационных процессов представляет собой не полный список действий или

операций без разъяснения или ссылок на другие законы. В законопроекте используется широко известный термин «доступ», однако его нет в перечне операций, входящих в информационные процессы.

В соответствие со статьей 16 Федерального закона защита информации представляет собой принятие правовых, организационных и технических мер, направленных на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации. Тогда должны быть определены действия, совершенные «неправомочным способом». Но если субъект получил возможность получения информации, но не воспользовался данной возможностью, т. е. не получил информацию, или получил информацию, но не использовал ее, то как квалифицировать эти действия? Таким образом, регламентация нормами информационных законов реальных процессов информационной сферы осуществляется недостаточно полно.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Аполлонский А.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД

ИДЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ ИНТЕРНЕТА И КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Существуют ситуации, в которых участие лиц в сетевых процессах должно с позиции безопасности этих лиц оставаться анонимным. Например, имеют место случаи использования государством выражения пользователями своего мнения по различным вопросам для их административного и уголовного преследования.

Однако доказывание принадлежности, например, текстов конкретному автору не всегда является простым. Например, в социальной сети «ВКонтакте» в сентябре 2013 года 5045 пользователей с именем Владимир Путин и с узнаваемой фотографией на странице. Но это не означает, что все написанные на этих страницах тексты можно приписать одному человеку. И не означает, что пользователи обеспечили себе анонимность.

Класс задач, связанных с идентификацией пользователя в Интернете, решается компьютерной экспертизой. В основе этих задач доказывание идентичности субъектов сетевых процессов.

Многими считается, что однозначно компьютер может быть идентифицирован по использованию им IP-адресу [w: IP-адрес]. И, напротив, обеспечить анонимность действий в сети возможно, скрывая свой IP-адрес. Оба утверждения не соответствуют действительности.

По IP-адресу или доменному имени сайта, действительно, можно из баз данных регистраторов адресов и имен получить много информации. Используя любой Whois Server (например, http://2ip.ru/), можно узнать самые разнообразные сведения о своем провайдере: адреса, описание компании, контактные телефоны и телефоны технических служб, имена и фамилии инженеров [w:WHOIS]. Желающие там же свободно по имени сайта vk.com могут получить пару номеров мобильных телефонов Павла Дурова, основателя ВКонтакте.

Однако это все та информация, которую субъекты добровольно предоставляют регистраторам для публичного использования.

Эксперименты с сервисом *Whois* могут показать, что сервер видит у вас один и тот же *IP*-адрес, даже когда вы выходите в Интернет одновременно с нескольких компьютеров, подключенных к общему роутеру. Действительно, один *IP*-адрес может назначаться сотням и тысячам пользователям или сайтам. Для различения пользователей роутер (или сервер) использует внутренние *IP*-адреса, преобразования адресов происходит роутером или сервером по технологии *NAT* [*w:NAT*]. Эти внутренние адреса для внешнего сетевого субъекта недоступны. Известны случаи, когда Роскомнадзор выдавал требования операторам связи блокировать по *IP*-адресам ресурсы, на которых имелись признаки нарушения законодательства, и при этом страдали другие субъекты, которые использовали те же адреса. Текущая политика Роскомнадзора связана с блокировкой по *URL*. Предполагается, что каждая информационная единица имеет свой логический адрес. Однако это не так для некоторых технологий, когда страница не адресуется однозначно, а данные вычисляются или запрашиваются на сервере по технологии *Ajax*, Так ведет себя, например, социальная сеть ВКонтакте.

Некоторые сайты в настройках (httpd.conf/.htaccess) включают:

- Order Allow, Deny
- Allow from All
- Deny from 109.207.0.0/20

Whois дает для указанного диапазона 4096 IP-адресов принадлежность к Роскомнадзору, желание владельцев сайта ограничить его посещение сотрудниками Роскомнадзора понятно.

Заинтересованные в информации о пользователе имеют широкие возможности его идентификации по другим признакам. Например, сохраняя у него на компьютере куки – небольшие фрагменты данных, отправленные сервером. Эти данные при открытии соответствующего сайта пересылаются веб-серверу.

К другим распространенным методам идентификации можно отнести использование уникальных характеристик компьютера пользователя (устройств, настроек ОС и браузера и т.д.). Распространенный в Интернете пример http://panopticlick.eff.org/ показывает, какую уникальную информацию можно получить от браузера, используя Javascript: характеристики экрана и системных шрифтов, версию браузера и подключенные к нему программные модули, часовой пояс и другое. Все эти характеристики будут отправлены серверу, даже если пользователь применяет технологии анонимности IP-адреса

(VPN, proxy [w: Прокси-сервер], TOR и другие), например, для обхода ограничений Интернет – цензуры [w: Интернет-цензура].

В http://javascript.ru/unsorted/id приведен обзор разнообразных программных методов идентификации. Для целей идентификации при компьютерной экспертизе могут быть использованы и имеющиеся тексты. Речевые, грамматические и словарные особенности их написания говорят об индивидуальности автора, вполне могут быть сопоставлены, и мера расхождения может быть оценена количественно. Такую же возможность могут предоставить программы-кейлоггеры [*w:* Кейлогер], которые регистрируют действия пользователя с клавиатурой и мышью. Опыт, навыки, темп действий, ошибки и исправления – все это так же может характеризовать пользователя и быть использовано для задач идентификации. Не случайно современные программы *Internet security* включают в себя виртуальные клавиатуры, которые позволяют обезопасить исследования вводимых на клавиатурах данных, например, при работе с банком.

Атисков А.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ИСПОЛЬЗОВАНИЕ ОНТОЛОГИЧЕСКОГО ПРОЕКТИРОВАНИЯ ДЛЯ АВТОМАТИЗИРОВАННОГО АНАЛИЗА ДОКУМЕНТОВ ПОЛИТИКИ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ

На сегодняшний день развитие компьютерных технологий идет стремительными темпами. Информационные технологии активно внедряются во все сферы деятельности, они управляют работой кассовых аппаратов, следят за работой автомобильных систем зажигания, ведут учёт семейного бюджета, или просто используются в качестве развлекательного комплекса.

Для того чтобы сохранить в целостности и сохранности данные предприятий необходимо провести анализ структуры организации и определить права доступа каждого сотрудника к ценной информации. На сегодняшний день доступ сотрудников к корпоративной информации осуществляется путем распределения должностных обязанностей руководством компании. Для того чтобы исключить ошибки в распределении доступа к информации, большинство организаций составляют специальный документ «политику безопасности». Для того чтобы исключить ошибки в распределении доступа, необходимо провести анализ политики безопасности.

Политика безопасности может быть разработана и описана с использованием как формального, так и неформального метода. Для неформальных способов описания политик при разработке информационно-безопасных технологий разграничения доступа широкое распространение получило описание правил доступа субъектов к объектам в виде таблиц, наглядно представляющих правила доступа. Обычно такие таблицы подразумевают, что субъекты, объекты и типы доступа для данной системы заранее определены.

Существующие недостатки использования формальных методов заключаются в неразрешимости некоторых проблем безопасности с использованием формальных методов, использование формальных методов при разработке систем может привести к появлению систем, практическое использование которых весьма неудобно; использование формальных методов при разработке систем приводит к дорогостоящим проектам; многие нарушения безопасности происходят вследствие некорректного использования пользователями компьютерных систем, модели безопасности часто не обеспечивают безопасности реальной системы; безопасность обеспечивается только в рамках формальной модели, которая часто бывает упрощенной; любой выход за пределы модели влечет нарушение безопасности.

В настоящий момент еще не создан универсальный метод создания онтологии политики безопасности. Процесс создания онтологий включает в себя создание чернового варианта, определение деталей разработки, уточнение онтологии, пока она не будет отражать концепцию предметной области с определенной степенью.

Для того чтобы разработать онтологическую модель политики безопасности необходимо определить классы онтологии организации, то есть определить термины предметной области. Разрабатываемая система должна проанализировать политику безопасности и выявить наиболее критичные места в модели. Для этого выбирается предварительный список терминов в онтологии, далее на основе анализа структуры предприятия и видов деятельности выбираются конкретные классы.

В инструменте онтологического проектирования Protégé существует закладка запросов, при помощи которой получают нужные сведения из созданного проекта по всем экземплярам классов. Анализ онтологической модели политики безопасности может выявлять ошибки в распределении прав доступа сотрудников к корпоративной информации. Позволяет прослеживать всю структуру организации, следить за распределением прав доступа сотрудников к корпоративной информации, и отслеживать, как сотрудники могут воздействовать на компоненты организации.

Данный подход будет полезен тем компаниям, которые имеют большой штат сотрудников. Главным преимуществом онтологической модели является то, что при необходимости можно расширить структуру путем добавления сотрудников и их обязанностей, сделав процесс поиска ошибок автоматизированным.

Афанасьев С.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ОНТОЛОГИЧЕСКИЙ ПОДХОД К ОПРЕДЕЛЕНИЮ ОБЛАЧНЫХ СЕРВИСОВ

Облачные вычисления – интернет базируемое развитие и использование компьютерной технологии, посредством чего динамически масштабируемые и часто виртуализируемые ресурсы обеспечиваются как обслуживание через интернет. По мнению ведущих специалистов провайдеров облако больше не раскладывается на четко определенные слои. В будущем многие приложения будут собирать разные сервисы и большие данные из разных мест и совмещать их воедино. Здесь необходимо мета описание (семантическое или онтологический подход) данных и сервисов в различных облаках необходимо для выбора релевантных сервисов (таких как инфраструктура, платформы, объемы памяти и т.д.) и различных разрозненных источников данных.

Научные инструменты и компьютерное имитационное моделирование порождают громадные объемы данных, для анализа и организации которых требуются новые научные методы. Каждый год объемы данных почти удваиваются. Поскольку новые научные инструменты обладают исключительной точностью, так же быстро улучается качество данных. Для анализа этих данных с целью нахождения тонких эффектов, упущенных в предыдущих исследованиях, требуются алгоритмы, которые одновременно могут работать с огромными наборами данных и обнаруживать при этом очень тонкие эффекты.

Онтологическое описание позволит автоматически строить структуру и таксономию данных и сервисов в вычислительных облаках. Для больших данных из различных источников в различных форматах интегрировать данные на основе онтологий. Использование языка онтологий (Web Ontology Language, OWL) и языка запросов SPARQL позволит освободить пользователя от необходимости отбирать источники данных, в которых находится интересующая информация и осуществлять интеграцию данных на основе онтологий.

Белоусов А.С.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ ПЕРЕДАЧИ ДАННЫХ В БЕЗОПАСНЫХ БЕСПРОВОДНЫХ ТРАНСПОРТНЫХ СЕТЯХ

Беспроводные сети являются наиболее востребованными на сегодняшний день во всех областях, а особенно в транспортной сфере. Территориальная удаленность, а так же динамическое изменение местоположения для доступа в сеть, ставит упор именно на беспроводные сети. Основными параметрами, характеризующие беспроводной сети, являются дальность действия и возможная скорость передачи данных. Обеспечение высоких показателей для этих параметров является ключевой задачей для обеспечения хорошего качества обслуживания.

На сегодняшний день существует большое количество различных технологий для повышения качества беспроводных сетей. С недавних пор активное развитие получила технология MIMO (MultipleInput – MultipleOutput, Множественный вход – множественный выход). Технология MIMO основывается на создании антенных массивов, как на приемной, так и на передающей стороне беспроводного канала передачи данных. Сигнал передается с массива антенн в соответствии с выбранным алгоритмом. В зависимости от поставленных задач это может быть как одновременная передача одинаковых сигналов, так и передача сложного комбинированного или кодированного пространственно-временным кодом сигнала с разных антенн. На приемной стороне так же возможно использование различных алгоритмов обработки сигналов с массива антенн. Применение определенного алгоритма передачи и приема сигнала позволяет повысить помехоустойчивость канала, что приводит к увеличению возможной скорости передачи данных.

Наличие антенных массивов так же повышает зону действия беспроводной сети передачи данных. Сигналы распространяются различными путями с различных передающих антенн, а так же принимаются различными приемными антеннами. Тем самым получается пространственная избыточность, когда при использовании различных пар приемной и передающей антенны, возможен выбор наилучшей пары для передачи данных на большее расстояние.

Наличие антенных массивов на передающей стороне так же может быть использовано для формирования адаптивной диаграммы направленности (beamforming). Технология состоит в том, что сигналы, передающиеся с массива антенн, испытывают усиливающую интерференцию в области нахождения массива антенн приемной стороны. Сигналы, которые посылает приемная сторона, помогают определить местоположение и сформировать узконаправленную диаграмму. Так как в беспроводных сетях часто используется технология мультиплексирования с разделением по времени, то технология сможет работать с множеством пользователей, изменяя диаграмму направленности для каждого пользователя индивидуально.

Существует несколько видов формирования адаптивной диаграммы направленности. Условно их можно разделить на 2 типа: с всенаправленными антеннами и узконаправленными антеннами.

В системе с всенаправленными антеннами на передающей стороне вычисляется местоположение приемника. Производятся сдвиг фазы на массиве антенн для того, чтобы в точке местоположения приемника происходила усиливающаяся интерференция сигналов. При этом, одна антенна задает «базовую» фазу, а все остальные антенны сдвигают фазу сигнала относительно нее. Недостаток такой реализации является в том, что в системе с всенаправленными антеннами нельзя полностью контролировать направление лучей усиливающей интерференции. Большое количество лучей направлены не в сторону приемника и часть энергии передатчика не используется в полезном действии. Более того, лучи усиливающей интерференции, направленные не в сторону приемника, могут оказывать побочное действие и вносить помехи в канал передачи данных, тем самым ухудшать его характеристики.

В системе с узконаправленными антеннами используется несколько антенн, каждая из которых обрабатывает свой сектор общей диаграммы направленности. При передаче данных по беспроводному каналу, сигнал идущей с каждой передающей антенны обрабатывается, вычисляется наилучшая комбинация антенн, которая создает оптимальный луч усиливающей интерференции, причем количество антенн и мощность сигнала с каждой из них может быть различна для каждого пользователя. Таким образом, луч усиливающей интерференции будет сформирован строго по направлению к приемнику, а все остальные области будут ослаблены.

В обоих видах систем формирования адаптивной диаграммы направленности возможно динамичное изменение параметров массива передающих антенн, что позволит обслуживать с хорошим качеством пользователей находящихся в движении или пользователей находящихся в условиях изменения среды распространения сигнала.

Применение новых технологий сможет существенно улучшить характеристики беспроводной сети передачи данных, что в свою очередь повысит качество сети в целом.

Белоусов А.С., Воеводский К.С.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова

ШИФРОВАНИЕ КАК СПОСОБ ЗАЩИТЫ ПЕРЕДАВАЕМЫХ ДАННЫХ В МОБИЛЬНЫХ СЕТЯХ

Голосовые вызовы, мгновенные сообщения и электронная почта являются одними из основных способов общения не только для личных целей, но и выполнения служебных задач. При организации обмена таким трафиком через частные локально-вычислительные сети, в том числе и беспроводные, он может быть надежно защищен при использовании алгоритмов шифрования передаваемых данных, серверов криптозащиты и других средств, но при выполнении некоторых задач не каждый пользователь может быть постоянно коммутирован в частную сеть. Некоторая часть рабочих мест вынуждена быть территориально удаленной и, возможно, подвижной. В таких случаях удобно организовать доступ через публичные мобильные сети, такие как сотовые сети стандарта GSM.

Широко распространенные на сегодняшний день сотовые сети стандарта GSM используют несколько методов защиты, а именно начальное установление подлинности по средствам алгоритма A3, шифрования передаваемых данных по средствам алгоритма A5 и вычисление персональных ключей шифрования Кс по средствам алгоритма A8. Для работы этих алгоритмов используется некоторое количество ключей шифрования и переменных, которые хранятся в SIM-карте или вычисляются в ходе работы алгоритмов.

На практике сотовые операторы вместо алгоритма A3 и A8 используют один алгоритм COMP128, представляющий хэш-функцию. Безопасность сетей GSM изначально базировалась на принципе «безопасность за счет неизвестности», закрытые алгоритмы A3, A8 и COMP128 подвергались массовым анализам и атакам. Необходимо было получить ключ Ki, который храниться в недоступной для чтения памяти SIM-карты. Система была взломана в 1998 году группой исследователей. Итог этих исследований очевиден, повсеместный отказ от алгоритма COMP128 и замена на более надежные модификации COMP128-2 и COMP128-3, технические детали которых, как и раньше держатся в секрете.

Передаваемые данные шифруются секретным алгоритмом A5, который имеет 3 модификации. Для работы алгоритма так же используются ключи и переменные, которые либо хранятся в SIM-карте, либо вычисляются в ходе работы алгоритмов. Сам алгоритм опирается на систему регистров сдвига с обратной связью, сдвиги в регистрах происходят только при выполнении определенных условий. На сегодняшний день большинство успешных атак происходило при получении шифрованной и не шифрованной информации. Такая ситуация кажется невозможной, однако из-за специфики стандарта GSM, при передаче шифрованных данных система передает нешифрованные системные сообщения, которые дублируются в шифрованном потоке данных. Используя эти данные, возможно получить сессионный ключ шифрования.

Исправить ситуацию с защитой информации передаваемой в сотовых сетях решила канадская компания RIM (ResearchinMotion), которая предложила линейку беспроводных мобильных устройств под торговой маркой BlackBerry. Изначально устройство позиционировалось только для работы с

электронной почтой. На сегодняшний день устройства расширили свой функционал и могут так же осуществлять голосовые вызовы и передачу мгновенных сообщений.

Помимо ряда удобных пользовательских функций, таких как мгновенное получение электронной почты и снижение пользовательского трафика за счет кодирования передаваемой информации, данные устройства обладают расширенными настройками безопасности пользовательских данных, а так же используют технологию шифрования данных с применением алгоритмов 3DES(128) и AES(256). Алгоритм шифрования AES (AdvancedEncryptionStandard) является одним из самых криптостойких и принят в качестве стандарта правительством США. Более того в системе используется несколько ключей шифрования для защиты различных типов данных.

MasterKey (симметричный) – основной ключ шифрования, применяемый для взаимодействия устройства с сервером, генерируется каждые 30 дней. MessageKey (симметричный) – ключ, используемый для шифрования передаваемых мгновенных сообщений и сообщений электронной почты, генерируется через каждые 2 КБ переданных данных. ContentProtectionKey (асимметричный) применяется для шифрования информации в защищенном хранилище устройства. GrandMasterKey (симметричный) используется для защиты хранилища ключей шифрования и сертификатов.

Современные мобильные устройства обладают достаточно высокими показателями безопасности и могут быть использованы как альтернатива частным локально-вычислительным сетям, хотя они и имеют ряд уязвимостей. Так же следует заметить, что большинство современных устройств имеют дополнительные возможности защиты информации, такие как криптографические протоколы SSL и TLS, поддерживаемые на уровне устройства, что позволяет достичь еще большей защиты информации.

Биричевский А.Р.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ПОДХОД К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ВЗАИМОДЕЙСТВИЯ ПРОЦЕССОВ ПРИ РАЗРАБОТКЕ ОПЕРАЦИОННЫХ СИСТЕМ

В основе архитектуры классической операционной системы лежит процесс. Процесс это абстракция, описывающая выполняющуюся программу. Крайне редко процесс функционирует без взаимодействия с «внешней средой» (процессами ядра операционной системы, служебными процессами, другими прикладными процессами). Такое взаимодействие называется межпроцессное. Безопасность взаимодействия процессов является одним из важнейших частей комплексной системы защиты операционной системы.

Суть подхода к обеспечению безопасности взаимодействия между процессами заключается в следующем:

– в качестве «пользователя» принимается процесс (процесс рассматривается как «клиент» который пользуется услугами операционной системы);

– обеспечение безопасности взаимодействия процессов является прямой задачей операционной системы (операционная система обязана обеспечить безопасность взаимодействия своих «клиентов»);

– для обеспечения требований безопасности операционная система может требовать от процесса выполнения некоторых требований.

Ключевая составляющая подхода состоит в том, что операционная система принимает на себя все обязанности по защите данных процесса. В связи с этим «внешняя среда» для процесса рассматривается как абсолютно безопасная.

Для реализации данного подхода предлагается реализовать в операционной системе некое количество классических мер защиты, которые будут предоставляться процессу (аналогично «услугам» клиенту):

– средства усиленной аутентификации (например, идентификация устройства, на котором выполняется программа);

– средства защиты приложений (в том числе защиты от отладки);

– средства защищенного хранения данных (защищенная память, контейнеры для постоянного хранения ключей);

– средства выполнения криптографических операций (криптопровайдер).

Согласно основной идее подхода данные методы могут быть доступны процессу двумя путями:

– по запросу процесса (вызов функций из приложения);

– независимо (прозрачно) от алгоритма процесса (например, при создании процесса будет указано, что процессу необходима защита от отладки и аутентификация устройства, и операционная система будет обязана выполнить это требование).

Стоит заметить, что кроме вышеуказанных методов обеспечения безопасности в операционной системе, возможна реализация и других методов, таких как разграничения доступа к ресурсам, контроль процессов и так далее.

Рассмотренный подход к обеспечению безопасности взаимодействия процессов может сделать защищенную операционную систему не только более безопасной для пользователя, но и более привлекательной для разработчиков коммерческих приложений.

Большаков В.И., Большакова Л.В., Яковлева Н.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

МЕТОДЫ МНОГОМЕРНОГО СТАТИСТИЧЕСКОГО АНАЛИЗА В РЕШЕНИИ ПРОБЛЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В последнее время при исследовании различных проблем, связанных с информационной безопасностью, все чаще стали применяться математико-статистические методы многомерного анализа. Первоначальная информация в таких исследованиях, как правило, представлена в виде набора объектов, каждый из которых характеризуется определенным числом признаков, характеристик или показателей. Например, в качестве объектов исследования могут быть рассмотрены предприятия, регионы, страны, а в качестве признаков – факторы, определяющие уровень информационной безопасности объекта. Как показывает опыт число объектов и число факторов может быть очень большим. Кроме этого, чаще всего, факторы бывают взаимосвязаны и по-разному влияют на безопасность объекта.

При решении задач определения структуры взаимосвязи факторов, степени влияния их друг на друга и в целом на информационную безопасность объекта, возникают трудности, обусловленные неполнотой информации и сложностью получения статистических данных. Методы многомерного анализа позволяют выбрать ту вероятностно-статистическую модель, которая наилучшим образом соответствует исходным статистическим данным, характеризующим реальную ситуацию. По построенной модели можно оценить надежность и точность выводов, сделанных на основании ограниченного статистического материала.

Многомерный математико-статистический анализ опирается на широкий спектр методов: множественный корреляционно-регрессионный, факторный, кластерный, дискриминантный и т.д. Наиболее распространенными в практической работе в настоящее время являются методы множественного корреляционно-регрессионного анализа. Они позволяют оценить тесноту между системами показателей (факторов) и дать представление о стохастических связях между отдельной зависимой переменной и группой влияющих на нее факторов. Исследование зависимостей и взаимосвязей между существующими явлениями или процессами дает возможность глубже понять сложный механизм причинно-следственных отношений между явлениями. Корреляционно-регрессионный анализ находит широкое применение при прогнозировании, при решении задач планирования, при выявлении факторов, воздействуя на которые можно вмешиваться в исследуемый процесс с целью получения нужных результатов.

Однако корреляционно-регрессионные методы не всегда дают результаты адекватные действительности или результаты, по которым можно сделать важные выводы. Происходит это чаще всего тогда, когда исследуется неоднородная совокупность объектов, т.е. совокупность объектов, которые имеют существенные различия. В таких случаях актуальным является применение перед корреляционно-регрессионным исследованием процедуры классификации объектов. Методы кластерного и дискриминантного анализа предназначены для разделения рассматриваемых совокупностей объектов, на некоторые однородные в определенном смысле группы.

Наличие множества исходных признаков, характеризующих процесс функционирования объектов, заставляет отбирать из них наиболее существенные и изучать затем меньший набор показателей. Метод главных компонент и факторный анализ позволяют с минимальной потерей «сжать» информацию за счет некоторого преобразования исходных признаков, приводящего к уменьшению их числа. Новые факторы или главные компоненты позволяют лаконично и более просто объяснять многомерные структуры.

Одним из недостатков методов многомерного анализа является громоздкость статистических вычислений, однако после появления различных пакетов программ обработки статистической информации, практически снявших эту проблему, эти методы стали получать все более и более широкое применение.

Виноградов А.Б., Щиголева М.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОПАСНЫХ РЕЖИМОВ РАБОТЫ В НАУЧНЫХ ИССЛЕДОВАНИЯХ

Особенностью и тенденцией развития научных исследований в современный момент является ориентация на инновационные преобразования всех этапов наукоёмких разработок. Наука и производство стали взаимопроницаемы новыми знаниями и наукоемкими интеллектуальными преобразованиями. Технические средства производства и парк оборудования науки, сближаясь,

переходят на уникальную высокотехнологичную аппаратуру. Слияние науки и производства с целью высокой инновационной отдачи помимо первой, очевидной особенности – неотъемлемое научно-производственное проникновение в технологические процессы и индустрию оборудования (1); организовало новую сферу научного сервиса (2) одновременно в интересах как науки, так и массового производства; формирование новых категорий высокотребовательных производителей (3) и потребителей (4), ориентированных на перспективный уровень достижений всех составляющих научно-производственного цикла. Все эти компоненты представлены в инновационной инфраструктуре, сущностью которой является наукоёмкий конечный продукт производства, сервиса и реализации, потребляемый с использованием высокотехнологического ресурса требовательными образованными кадрами. Подобная постановка позволяет обозначить точки опасностей и рисков, разрушительных для человека, объектов и средств производства, среды обитания, что накладывает высокую ответственность на специалистов каждого звена производства, потребления и оказания услуг. Ценностное отношение к природной, производственной и среде обитания, выстраивает обязательную стратегию безопасной жизнедеятельности, охватывающей теорию и практику защиты человека от всевозможных опасных факторов во всех сферах его существования. Для конкретной подконтрольной профессиональной среды необходимо, как минимум, обеспечить информирование о точках угрозы безопасности жизнедеятельности и материальных потерь. Выполнение научных исследований в новых условиях обязательных инновационных преобразований в новых структурах ИТЦ, ИКТ, ЦИТ, технопарков, инжиниринговых центров и т.п., специалистами перечней специальностей, присущих новым тенденциям развития наукоёмкого производства. Из выявленных точек опасностей и рисков выстраивается программа снижения профессионального риска, обеспечивающая минимизацию значений вредных производственных и профессиональных факторов, установления участков гарантированной безопасности, совокупных зон отсутствия профессиональных рисков при многофакторных связанных воздействиях, остаточных и накапливаемых рисков. Помимо обозначения точек опасностей и рисков, их констатации и содержательной информационной поддержки, предусматривается экспертиза и реальная оценка опасностей и рисков, выработка предупреждающих и профилактических мероприятий, формирование универсальных и узкоспециальных шкал оценки условий труда, режимов работы, как результатов мониторинга потенциально опасных процессов проведения научных исследований. И построение, в перспективе, модели безопасного выполнения научного исследования.

Демьянчук А.А., Новикова Е.С., Молдовян Д.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербургский институт информатики и автоматизации РАН

СПОСОБ ПОВЫШЕНИЯ УРОВНЯ БЕЗОПАСНОСТИ ПРОТОКОЛОВ АУТЕНТИФИКАЦИИ С НУЛЕВЫМ РАЗГЛАШЕНИЕМ СЕКРЕТА

В арсенале средств обеспечения информационной безопасности особое место занимают протоколы аутентификации с нулевым разглашением секрета, используемые для проверки подлинности личности удаленных пользователей. Достоинством протоколов аутентификации данного типа является то, что в ходе их выполнения никакой утечки информации о секретном ключе в определенном смысле не происходит. Протоколы без разглашения секрета (с нулевым разглашением секрета) относятся к криптосистемам с открытым ключом, стойкость которых основана на вычислительной трудности некоторой математической задачи, положенной в их основу. Понятие стойкости характеризует важнейшее свойство криптографических схем – способность выдерживать всевозможные атаки. Основной проблемой оценки стойкости криптосхем является то, что трудно доказать, что в ближайшем будущем не будут найдены прорывные алгоритмы взлома данной криптосистемы. Можно утверждать, что стойкость отражает только одну из двух сторон понятия безопасности криптосхем. Второй стороной последнего понятия является низкая вероятность того, что в обозримом будущем будут получены прорывные результаты по разработке алгоритмов решения используемых трудных задач. Таким образом, безопасность криптосхем с открытым ключом связана со следующими двумя моментами: 1) со сложностью лучшего из известных методов решения трудной задачи, положенной в основу алгоритма (текущая стойкость алгоритма) и 2) с вероятностью появления принципиально новых методов и алгоритмов решения базовой вычислительно трудной задачи, имеющих сравнительно низкую трудоемкость (вероятность непредвиденного взлома). В целом уровень безопасности определяется как вычислительной сложностью решения базовой трудной задачи, так и вероятность нахождения прорывных решений базовой трудной задачи в обозримом будущем является достаточно малой.

В настоящем сообщении предлагаются способы повышения уровня безопасности протоколов с нулевым разглашением секрета путем такого их построения, при котором их взлом требует одновременного решения задачи факторизации (ЗФ) и задачи дискретного логарифмирования (ЗДЛ)

в простом конечном поле. Для построения протоколов такого типа используется комбинирование двух подходов, предложенных ранее авторами.

Первый подход относится к построению двухшаговых протоколов с нулевым разглашением, основанный на применении схем открытого согласования ключа и механизма генерации (проверяющим) разовых открытых ключей и разового общего секрета. При этом проверка, выполняемая доказывающим (пользователем, подлинность которого проверяется), того факта, что проверяющий знает разовый общий секрет, выполняется по значению хэш-функции или криптограмме, вычисляемой путем шифрования заранее специфицированного сообщения. Для упрощения протоколов (устранение использования алгоритмов хэширования и шифрования) предлагается реализация протоколов с использованием ЗДЛ в конечном поле двоичных многочленов, порядок мультипликативной группы которых равен достаточно большому простому числу Мерсенна, или с применением идеальных эллиптических кривых. Такой вариант построения протоколов обеспечивает существенное упрощение аппаратной реализации, особенно в последнем случае.

Второй подход связан с использованием вычислительной трудности ЗДЛ по трудно разложимому модулю. Рассматриваются следующие два варианта реализации предлагаемого подхода к повышению безопасности криптосхем. В первом варианте составной модуль n и связанные с ним параметры криптосхем вырабатываются некоторым доверительным центром, который уничтожает делители q и r после выработки значения n и параметров криптосхемы. В этом случае может быть построен более широкий ряд криптосхем различного типа, основанных на трудности одновременного решения ЗФ и ЗДЛ по простому модулю. Второй вариант состоит в использовании значения модуля n в качестве одного из элементов открытого ключа и представляется предпочтительным, поскольку в нем достаточно использования услуг удостоверяющего центра. Оба варианта обеспечивают возможность реализации протоколов с нулевым разглашением. Некоторые типы криптосхем (протоколы коллективной и слепой коллективной подписи) требуют использования первого подхода.

Работа поддержана грантом РФФИ (проект № 12-07-31164 мол_а).

Дормидонтов А.А., Зубакин В.В.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного

АНАЛИЗ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОГО ОБМЕНА ПРИ ПРИМЕНЕНИИ ДИНАМИЧЕСКИХ АЛГОРИТМОВ МАРШРУТИЗАЦИИ

В настоящее время наиболее широкое развитие получают мультисервисные сети, по которым возможна передача любых видов информации, преобразованных в цифровую форму. Одним из способов обеспечения требований безопасности в сетях с коммутацией пакетов на сетевом уровне ЭМВОС является взаимодействие только с разрешёнными устройствами. Таким требованиям в полной мере удовлетворяет статическая маршрутизация, как правило, с несколькими обходными маршрутами. При применении статической маршрутизации выполнение требований по доставке сообщений напрямую зависит от знания техническим персоналом структуры всей сети и пропускных способностей линий связи, так как задание маршрутов и составление таблиц маршрутизации производится вручную. При этом, пользователю важно, чтобы информационный обмен выполнялся по всем заданным ВВХ. Основным недостатком статической маршрутизации является невысокая скорость адаптации к изменяющимся условиям функционирования сети, таким как увеличение нагрузки, выход из строя коммутационных центров, каналов передачи и т.п.

Исходя из вышесказанного, статическую маршрутизацию целесообразно применять, когда заранее известен объём информации, передаваемый от органов управления. В настоящее время, в связи с возрастающими требованиями к объёму и типу передаваемой информации, количеством сетевых устройств, расширением объёма сетей, затруднительно произвести точные расчёты передаваемого трафика. В этом случае алгоритмы фиксированной маршрутизации могут не в полном объёме выполнять заданные требования по ВВХ информационного обмена.

Адаптивные алгоритмы маршрутизации являются наиболее предпочтительными с точки зрения производительности сети. Они позволяют не только выбирать маршрут в зависимости от складывающейся ситуации на сети, но и балансировать нагрузку по различным маршрутам. Адаптивные алгоритмы поиска оптимальных маршрутов способны обеспечить требуемую пропускную способность, практически в режиме он-лайн. В случае применения таких алгоритмов при расчёте оптимальных маршрутов могут быть задействованы все имеющиеся в сети устройства. При этом не исключается возможность деструктивных воздействий путём нахождения в сети стороннего устройства.

Для выполнения безопасного обмена необходимо обязательно применять идентификацию устройств, участвующих в обмене. Таким средством могут быть служебные пакеты со специальным полем идентификатора. В этом случае сетевые устройства, поддерживающие такой протокол, смогут взаимодействовать друг с другом, при этом, пакеты, не содержащие такого идентификатора, будут игнорироваться.

Таким образом, применение адаптивных алгоритмов маршрутизации позволяет существенно увеличить производительность сети передачи данных в целом, а для обеспечения требуемого уровня безопасности информационного обмена необходимо применение специальных идентификационных протоколов.

Дулатов И.Н.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова

ОРГАНИЗАЦИОННЫЕ И ПРАВОВЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

С 1 июля 2011 года полностью вступил в силу Федеральный закон от 27.07.2006 года номер 152-ФЗ «О персональных данных». Основная цель закона - защитить права и свободы человека при обработке его личной информации, в том числе право на неприкосновенность частной жизни, личную и семейную тайну. Защита конфиденциальной информации является одной из приоритетных задач современного законодательства. Защита персональных данных — комплекс мероприятий технического, организационного и организационно-технического характера, направленных на защиту сведений, относящихся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).

Обычно выделяют следующие этапы создания режима защиты персональных данных:

– Создание внутренней документации по работе с персональными данными.
– Создание организационной системы защиты персональных данных.
– Внедрение технических мер защиты.
– Получение лицензий регулирующих органов (ФСБ, ФСТЭК). Лицензия ФСТЭК России на Техническая защита конфиденциальной информации нужна только в случае, если организация оказывает услуги по созданию системы защиты персональных данных для других лиц. При создании системы защиты персональных данных силами организации, как техническими средствами, так и организационными — данная лицензия не нужна.
– Получение сертификатов регулирующих органов (ФСБ, ФСТЭК) на средства защиты информации.

Технологические системы обработки и хранения конфиденциальных документов могут быть традиционными, автоматизированными и смешанными.

Традиционная (делопроизводственная) система основывается на ручных методах работы человека с документами и является универсальной. Она надежно, долговременно обеспечивает защиту документированной информации, как в обычных, так и в экстремальных ситуациях. В связи с этим стадии защищенного документооборота в большинстве случаев технологически реализуются методами и средствами именно традиционной системы обработки и хранения конфиденциальных документов, а не автоматизированной. Вместе с тем система характеризуется низкой степенью оперативности доставки документов потребителям информации, невысокой эффективностью справочной, поисковой и контрольной работы по документам, потребностью в значительном количестве персонала, обслуживающего систему.

В автоматизированной технологической системе обработки и хранения конфиденциальных документов рассмотрение и исполнение электронных конфиденциальных документов и электронных аналогов бумажных документов разрешается только при наличии сертифицированной системы защиты компьютеров и локальной сети, включающей комплекс программно-аппаратных, криптографических и технических мер защиты базы данных, компьютеров и линий связи. Помещения, в которых конфиденциальная информация обрабатывается на ЭВМ, должны иметь защиту от технических средств промышленного шпионажа, надежную круглосуточную охрану и пропускной режим. Кроме того, следует учитывать, что при автоматизированной обработке объективно резко увеличивается количество носителей (источников), содержащих конфиденциальные данные. Недостатком обработки информации на ЭВМ также является необходимость постоянного дублирования информации на нескольких носителях с целью исключения опасности ее утраты или искажения по техническим причинам.

В настоящее время наиболее широко используется смешанная технологическая система обработки и хранения конфиденциальных документов, совмещающая традиционную и автоматизированную технологии. Выборочно автоматизируются: справочная и поисковая работа по бумажным документам, процедура составления и изготовления документов и учетных форм, контроль исполнения, сервисные задачи. Остальные стадии и процедуры выполняются в русле традиционной, делопроизводственной технологии (распределение бумажных документов, их рассмотрение, исполнение, оперативное и архивное хранение документов). Недостаток смешанной технологии состоит в неполном использовании преимуществ и функциональных возможностей компьютерной технологии, отчего сохраняются рутинные делопроизводственные операции, которые мешают совершенствовать документооборот.

Ежгуров В.Н., Соколов С.С.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова

УЯЗВИМОСТИ В СИСТЕМАХ УПРАВЛЕНИЯ МУЛЬТИМОДАЛЬНЫМИ ПЕРЕВОЗКАМИ НА ПРИМЕРЕ СУБД ERP-КЛАССА

Реализация систем управления мультимодальными перевозками в рамках международных транспортных коридоров требует разработки, и развертки не просто автоматизированной системы управления (АСУ), а системы управления базами данных (СУБД) ERP – класса. Такая система должна непрерывно отслеживать ресурсы организации, в роли которых выступают транспортные средства; персонал, задействованные в обработке транспортных операций; а так же договоры и взаимные обязательства.

Такая реализация потребует усложнения и без того сложной структуры СУБД, что в свою очередь будет приводить к возникновению уязвимостей в безопасности СУБД.

Классы уязвимостей СУБД в большинстве своем возникают из-за человеческого фактора, но огромный пласт уязвимостей возникает также в результате конфликтов и проблем в программной части СУБД.

В связи со сложностью настройки прав доступа могут возникать уязвимости в безопасности СУБД, что в конечном итоге может привести к несанкционированному доступу к данным и механизму работы СУБД. Если система продолжает развитие, в нее постоянно вносятся корректировки и доработки, то специалисты не всегда сразу смогут указать необходимые и достаточные прав для той или иной группы пользователей.

Закрытость и специфичность системы закладывает уязвимость в саму основу системы. СУБД из-за своей объемности и сложности требует больших денежных и временных затрат на тестирование и устранение недостатков и уязвимостей. И чем более специфична СУБД, тем больше затрат на ее тестирование и отладку требуется, в виду крайне медленного процесса выявления неисправностей в системе, из-за малого количества реальных пользователей системы, которые не сразу выявят те или иные ошибки системы. Для таких систем обновления выходят крайне медленно, так как большинство ресурсов организация бросает на более прибыльные и массовые проекты, обновления к которым выходят на порядок быстрее и включают в себя больше исправлений.

В специфичности СУБД скрывается опасность наличия ошибок нулевого дня, которые могут критически воздействовать на всю СУБД в целом и известную злоумышленниками, но не выявленная разработчиком.

Недостаточная квалификация сотрудников службы безопасности организации в обращении с СУБД возникает в связи с задачей организации-подрядчика «развернуть систему в срок и уложится в бюджет». В основном организации подрядчики занимающиеся развертыванием СУБД проводят программы по обучению и подготовке только для конечных пользователей СУБД в самой организации, которые в дальнейшем будут сопровождать СУБД и обучать остальных сотрудников организации.

Зачастую подрядчик ограничивается развертыванием СУБД на серверах заказчика, подразумевая под этим установку СУБД и внесением доработок под требования заказчика.

Подрядчик не предоставляет заказчику программных средств (ПС) по тестированию; сценариев тестирования, разработанных за время разработки СУБД, по которым проводилось тестирование на работоспособность СУБД и наличие в ней уязвимостей.

Служба безопасности, если не вникает в СУБД, затрачивая время, усилия и другие ресурсы как организации заказчика, так и организации подрядчика не может гарантировать отсутствие наличия уязвимостей. Даже наличие у СУБД сертификатов безопасности не гарантирует защищенность СУБД и отсутствие уязвимостей, так как зачастую в процессе развертывания СУБД в ее структуру вносятся значительные изменения, влияющие на безопасность в целом. Наличие у специалистов службы безопасности понимания структуры СУБД и сценариев тестирования, которые отработаны у подрядчика во время разработки, крайне важны для полноценного развертывания СУБД.

Конфликт ПО часто возникает из-за того, что СУБД не тестировалась на одновременную работу с какой-либо сторонней программой. Так же стоит упомянуть ПО изначально созданное с целью создать или эксплуатировать уязвимость СУБД. Зачастую такое ПО ставит перед собой одну из целей: получить доступ к СУБД с максимально возможными правами и/ил нанесение максимального вреда базам данных (БД) СУБД в частности и полным нарушением работоспособности СУБД в целом.

Опасность для функционирования СУБД может так же исходить и от ОС любого семейства. Большинство современных СУБД проходят длительный период тестирования и исправления ошибок, но зачастую сам стиль разработки ОС накладывает некоторые ограничения, которые в конечном итоге приводят к возникновению уязвимостей в ОС, через которые злоумышленник может нанести удар.

Известны основные пути воздействия на ОС, которые в конечном итоге могут создать брешь в безопасности СУБД - доступ к СУБД посредством получения доступа к ОС:

1. Подбор паролей к аккаунтам с административными или близким набором прав.
2. Получение широкого круга прав на доступ к файлам СУБД.

Кислов Р.И., Юрин И.В.
Россия, Санкт-Петербург, ООО Центр защиты информации «Актив»,
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

К ВОПРОСУ ОБ ИЗМЕРЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Современные методы управления информационной безопасностью (ИБ) способны обеспечить решение любых корректно поставленных задач в области ИБ, а уровень безопасности любой технологии может быть сколь угодно высок. Наиболее развитый подход к построению системы управления информационной безопасностью предприятия изложен в национальном стандарте ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности». Управление осуществляется в соответствии с процессной моделью, а основными процессами являются оценка и обработка информационного риска. Но если взглянуть на проблему широко, то мы увидим, что она не сводится только к этим процессам. Жизнеспособная система управления информационной безопасностью должна включать в себя целый ряд процессов, обеспечивающих непрерывный контроль и совершенствование этой системы. Нахождение разумного компромисса, выбор приемлемого уровня безопасности при допустимых затратах является обязательным условием постановки задачи обеспечения ИБ.

Для того чтобы выбрать оптимальную систему необходимо правильно оценить необходимый уровень безопасности и приемлемый объем затрат. Необходимый уровень безопасности можно определить при наличии:

– системы показателей для оценки эффективности подсистемы безопасности и методики их измерения;

– должностных лиц, уполномоченных принимать решение о допустимости определенного уровня остаточного риска;

– системы мониторинга, позволяющей отслеживать текущие параметры подсистемы безопасности.

Нами выделены следующие составляющие затрат на информационную безопасность:

– затраты на формирование и поддержание звена управления информационной безопасностью (организационные затраты);

– затраты на контроль, т.е. затраты на определение и подтверждение достигнутого уровня защищенности информационных активов предприятия;

– внутренние затраты на ликвидацию последствий нарушения политики информационной безопасности – затраты, понесенные предприятием, в результате того, что требуемый уровень защищенности не был достигнут;

– внешние затраты на ликвидацию последствий нарушения политики информационной безопасности – компенсация потерь при нарушениях политики безопасности в случаях, связанных с утечкой информации, потерей имиджа компании, утратой доверия партнеров и потребителей и т.п.;

– затраты на техническое обслуживание системы защиты информации и мероприятия по предотвращению нарушений политики безопасности предприятия (затраты на предупредительные мероприятия).

Исследованию подвергалась каждая составляющая затрат на информационную безопасность. Получены функциональные зависимости затрат от уровня защищенности информационно-телекоммуникационной системы предприятия для каждой составляющей в отдельности. Сумма этих функций дает общие затраты на информационную безопасность предприятия.

С помощью полученного графика легко определить точку экономического равновесия. Оказывается, что непрерывно увеличивая затраты на информационную безопасность, мы добиваемся лишь незначительного снижения уровня риска. И наоборот, небольшой начальный вклад дает существенное увеличение защищенности системы. График отражает только общий случай, так как построен с учетом некоторых допущений, которые не всегда соответствуют реальным ситуациям.

Первое допущение заключается в том, что предупредительная деятельность по техническому обслуживанию комплекса программно-технических средств защиты информации и предупреждению нарушений политики безопасности предприятия, соответствует правилу Парето: то есть в первую очередь рассматриваются те проблемы, решение которых дает наибольший эффект по снижению информационного риска. Если не следовать этой модели, то вид графика станет совсем иным.

Второе допущение заключается в том, что так называемое экономическое равновесие не изменяется во времени.

На практике график функции «затраты/защищенность» конечно не будет гладким. Но тщательный систематический анализ составляющих затрат на информационную безопасность на предприятии поможет ответственному за информационную безопасность сделать своевременный вывод о том, где наиболее эффективно начинать предупредительные мероприятия. Другими словами, определить те области, которые дадут наибольшую отдачу в ответ на затраченные усилия.

Зорин К.М.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет» ЛЭТИ» им. В.И. Ульянова (Ленина)

ПРОГНОЗИРОВАНИЕ СЕТЕВЫХ АТАК С ПОМОЩЬЮ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ И DATA MINING

Большинство средств защиты информации предназначены для устранения последствий и минимизации ущерба от событий нарушения безопасности. Для выявления и предотвращения атак (или утечек конфиденциальной информации) используют системы обнаружения и предотвращения вторжений. Система обнаружения вторжений выявляет факты неавторизованного доступа в защищаемую систему либо несанкционированного её управления. Система предотвращения вторжений предназначена для обнаружения вторжений или нарушений безопасности, она позволяет отслеживать активность в реальном времени и быстро реализовывать действия по предотвращению атак. Но эти системы защиты в основном только обнаруживает и регистрирует атаки, которые уже происходят. Но даже обнаруженная атака не исключает причинения вреда. Специалистам по безопасности очень полезным было бы заранее знать о предполагаемых атаках. Информацией для анализа и прогнозирования служат логгирование и журналирование пользовательских сессий, данные аудита и прочие средства, позволяющие проанализировать действия пользователей, запрашиваемые ресурсы, вводимые данные, интенсивность и периодичность этих действий. Для прогнозирования также необходимо определить, какие из последовательностей пользовательских действий (или совокупности действий нескольких пользователей) приводят к нанесению ущерба. Для получения этих данных используются записи пользовательских сессий тестировщиками системы, а также специально нанятыми внешними аудиторами системы. На основе полученных шаблонных данных строится математическая модель прогнозирования атак. В качестве алгоритмов могут использоваться различные методы машинного обучения и интеллектуального анализа данных (data mining).

К методам машинного обучения относят классификацию (например, на основе меры близости в многомерном пространстве, деревьев решений, нейронных сетей), кластеризацию, регрессию и др. Для использования алгоритмов классификации и кластеризации каждый атрибут пользовательской сессии представляется измерением в многомерном пространстве, значение атрибута — координата в этом измерении. Таким образом, каждая пользовательская сессия — точка в многомерном пространстве. По мере схожести (или близости) можно отнести ту или иную сессию к представляющим опасность или нет. Но методы классификации и кластеризации не могут учесть тот факт, что злоумышленник для поиска, анализа и реализации атаки может делает использовать разные пользовательские сессии, ресурсы, инструменты и прочее. Поэтому необходимы способы анализа цепочек событий. Для этого используются методы анализа временных рядов (например, поиск ассоциативных правил и секвенциального анализа). Прогнозирование (с определённым уровнем вероятности) атак позволяет специалистам по безопасности успеть подготовиться к возможной атаке или предотвратить эту атаку, минимизировать или вообще исключить ущерб.

Ковальногова Н.М.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЭКОНОМИЧЕСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ

Информация, отображающая и обслуживающая процессы производства, обмена и потребления материальных благ и услуг определяется как экономическая. Широкое распространение автоматизированных информационных систем (АИС) сбора, обработки, передачи и хранения экономической информации актуализирует проблемы, связанные с ее защитой.

Экономические информационные системы (ЭИС) – совокупность внутренних и внешних потоков прямой и обратной информационной связи экономического объекта, методов, средств и специалистов, участвующих в процессе обработки информации и выработки управленческих решений.

Существенные для обеспечения безопасности особенности экономической информации:

- большой объем;
- многоразовые повторы циклов ее получения и обработки;
- разнообразие и рассредоточение источников и потребителей;

– большой удельный вес логических операций в общем объеме обработки.

Под угрозой безопасности информации понимаются события или действия, которые могут привести к хищению, искажению информации, несанкционированному использованию и разрушению информационных ресурсов управляющей системы, а также программно-аппаратных средств.

Угрозы информационной безопасности могут быть обусловлены естественными и антропогенными факторами. Наибольший интерес и сложность представляют последние, которые, в свою очередь, могут быть разделены на пассивные и активные.

Пассивные направлены в основном на несанкционированное получение/использование информационных ресурсов, не оказывая влияния на их функционирование. К ним относятся, например несанкционированный доступ (НСД) к базам данных (БД), прослушивание каналов связи и др.

Несмотря на то, что пассивные угрозы не разрушают информационные ресурсы, они могут иметь не менее пагубные последствия, чем активные. Например, НСД и последующий выброс инсайдерской информации (информация о тендерах, проекты новых разработок, клиентские базы, внутренняя финансовая отчетность, планы развития компании), которая в случае её раскрытия способна повлиять на рыночную стоимость ценных бумаг компании.

Активные угрозы нарушают нормальное функционирование АИС путем целенаправленного воздействия на ее компоненты. К активным угрозам относятся, например, разрушение или подавление линий связи, вывод из строя сетевого оборудования, программного или аппаратного обеспечения, искажение сведений в базах данных либо в системной информации и т.д.

К основным угрозам безопасности и нормального функционирования ЭИС относятся:

– утечка конфиденциальной информации;
– компрометация информации;
– несанкционированное использование информационных ресурсов;
– несанкционированный обмен информацией между абонентами;
– незаконное использование привилегий;
– нарушение информационного обслуживания.

Колесникова С.И.
Россия, Томск, Национальный исследовательский Томский государственный университет

ОСОБЕННОСТИ ПРИМЕНЕНИЯ ХАОТИЧЕСКИХ МОДЕЛЕЙ В ШИФРОВАНИИ ИНФОРМАЦИИ

Введение. Постановка проблем. Известно, что существует абсолютно криптостойкий алгоритм шифрования (К. Шеннон), со статистически надёжным ключом, длина которого равна или больше длины сообщения. Практическое применение систем, удовлетворяющих таким требованиям, ограничено соображениями стоимости и удобства пользования, так как хранение и передача ключей, размерами сопоставимыми с размерами исходных данных, а так же создания статистически надежных ключей (случайных последовательностей) является на данный момент непреодолимой проблемой. Известны работы (напр., Liu S., Sun J., Xu Zh., L. Kosarev, и др.), где предлагается использовать хаотические модели (обладающих сложной динамикой и большим периодом-орбитой), при этом в качестве ключевой последовательности берется траектория модели, а в качестве ключа системы шифрования - параметры модели.

Основными нерешенными проблемами при этом являются следующие: 1) нежелательный эффект (см. напр., работу Н. Птицына), связанный с влиянием математики с плавающей запятой на характер хаотичности, приводящий к возможному его исчезновению (покидание аттрактора исходной системы и вхождение в стационарный режим фактически уже в системе с другим, неизвестным, вообще говоря, функциональным описанием); 2) атака на шифр должна встретить практически непреодолимые вычислительные сложности.

Подход к решению проблем. Для решения первой проблемы предлагается использовать в качестве гамма-последовательности с ключом в виде значений параметров хаотической модели синергетически управляемую модель, где управляющими воздействиями служат параметры модели. Как известно, именно параметры модели определяют характер хаотичности динамического объекта. Так, аналог хаотического генератора случайных величин в модели Фейгенбаума возникает только при значениях параметра от 3-х до 4-х; «странные аттракторы» в системе Лоренца возникают при значениях параметров $r > 25$, $b = 8/3$, $\sigma = 10$ и принципиально не возникают при $b > 2\sigma$.

В докладе изложен подход к поддержанию хаотического поведения объекта с целью применения этого необходимого свойства в процедуре шифрования/дешифрования. Подход использует идеологию управления на многообразиях, а именно, классический метод аналитического конструирования агрегированных регуляторов (А.А. Колесников, ТТИ ЮФУ).

Исследование сравнительных свойств рядов данных двух моделей (управляемой и неуправляемой) проводилось в принятии за меру их хаотичности функции энтропии (неопределенности выбора состояния в конкретный момент времени), позволяющей судить об относительной степени упорядоченности состояний двух систем.

Решение частных задач. Поставлены и решены следующие частные задачи, свидетельствующие о плодотворности предложенного подхода: 1) разработка модификации поточного и блочного шифров AES (Advanced Encryption Standard) на базе хаотических моделей Эно и Фейгенбаума и демонстрация его качеств; 2) проведение криптографического анализа свойств алгоритма модифицированного шифрования; 3) проведение апробации модифицированных методик шифрования на ряде примеров шифрования/дешифрования изображений.

Выводы. Криптографический анализ алгоритмов AES и AES+Eno показал, что AES+Eno является более стойким к атакам, основанным на статистических данных, но крайне чувствителен к изменениям ключа. Качество шифрования AES+Eno выше качества шифрования AES. Теоретическая длина ключа в AES+Eno зависит от числа раундов и практически может быть сколь угодно большой за счет управления параметром модели, тогда как максимально возможная длина ключа в классическом алгоритме шифрования AES ограничена. В силу детерминированности рядов данных, порожденных хаотическими моделями, выводы по результатам численного исследования энтропийных свойств указанных моделей достаточны для вынесения положительных решений в практических задачах.

Заключение. Исследован вопрос об особенностях применения хаотических систем в криптографии. Предложен подход к поддержанию хаотического поведения объекта на базе нелинейного управления на многообразиях с целью формирования статистически надежных ключей (случайных последовательностей). Осуществлена апробация алгоритма шифрования AES с применением двух хаотических моделей Эно и Фейгенбаума. Проведен криптографический анализ свойств алгоритма модифицированного шифрования. Исследования показали, что энтропия управляемого ряда данных не меньше энтропии ряда данных, полученного итеративно с накоплением ошибки (связанной с недостатками арифметики с плавающей запятой).

Автор благодарит А.В. Коноваленкова, магистранта Томского университета систем управления и радиоэлектроники, за разработку программного комплекса, реализующего модификацию AES+Eno (на базе модели Эно), и проведение численного моделирования.

Колодин М.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБРАЗОВАТЕЛЬНЫХ СИСТЕМ

В настоящее время значительная часть действий в образовательной области (школы, вузы), как то — собственно обучение, учёт, управление, организация учебной среды, взаимодействие между администрацией, учителями, учениками, студентами, родителями) реализуется с помощью компьютеров, прежде всего — посредством компьютерных сетей. Это небезопасно, особенно если в сетевой обмен информацией включаются персональные данные.

Нарушение безопасности карается законом, который, несмотря на благие намерения, в нём заложенные, вводит жёсткие санкции против нарушителей, каковыми становятся почти все. Важна не абсолютная защита всего, а адекватная, т. е. в соответствии с потенциальным вредом, который произойдёт в случае нарушения защиты и получения посторонним доступа к защищаемым данным или их повреждения.

Важна и возможность нарушения авторских и смежных прав, в т.ч. по отношению к авторским разработкам (учебники, методички); но и здесь всё не так однозначно: интеллектуальная собственность ценна, но более ценным являются обмен опытом и распространение знаний, передовых подходов в быстро меняющемся мире, поэтому тотальные запреты, ограничения и блокировки здесь приносят больше вреда, чем пользы.

Представляется, что нужно действовать одновременно в нескольких направлениях: совершенствовать законодательство, повышать информационную и правовую культуру населения, вводить адекватные (но не чрезмерные) средства защиты информации.

Большинство технических средств давно и хорошо известны: надёжные и сменяемые пароли, защищённые каналы, проверка уровня доступа при каждом обращении к ресурсу (даже в рамках установленной сессии), авторизация, в т.ч. посредством открытых асимметричных схем и регистрации на проверяемых защищённых ресурсах, защита от ошибок и преднамеренных враждебных действий пользователя, от ошибок программного обеспечения в самой системе, управление резервными копиями, шифрование и анонимизация данных, выборки данных в соответствии с правами пользователя, ограничение доступа, сокрытие наличия функциональности вне прав пользователя, использование надёжных операционных систем (в нашем случае это ОС семейства Linux Debian, последняя стабильная версия) с правильными настройками в части безопасности, проверенного профессиональным сообществом инструментария, разделение справочной, информирующей и редактирующей частей системы, и прочее.

Вместе с тем нужно применять и организационные меры: обучать сотрудников и клиентов, не хранить и не передавать избыточную личную информацию, выделять данные, которые действительно нуждаются в защите, в отдельные массивы и охранять их в соответствии с

получившимся классом безопасности, а для остальных данных достаточно обычных баз данных, сетевых каналов и представления через веб-браузер: их разглашение не влечёт неприятностей для их владельцев и связанных с ними лиц. Образовательные информационные системы имеют свою специфику: они чаще подвергаются попыткам взлома изнутри.

В наших разработках (сайты «Всеумно» www.vseumno.ru и «Международный Академический Центр Вектор» www.vector-education.ru, сайты СПИИРАН www.spiiras.nw.ru и ИГИТО www.computer.edu.ru и другие) мы применяем относительно простые, удобные в программировании и использовании, достаточно надёжные средства защиты, но изучаем и будем применять и более новые, более совершенные средства.

Полезным при разработке систем (программы, сайты) оказывается мета-подход, позволяющий гибко разрабатывать и обновлять элементы систем с применением более совершенных средств защиты информации.

В целом надо отметить, что развитие образовательных систем в отношении информационной безопасности идёт в правильном направлении, его результаты вполне применимы в ежедневной работе.

Култышев Е.И., Полонский А.М., Козлов А.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В БЮРО ПРОПУСКОВ БИЗНЕС-ЦЕНТРА

Промышленные предприятия, научно-исследовательские института сдают в аренду неиспользуемые для основной производственной деятельности помещения. В отличии от традиционных бизнес-центров, которые изначально ориентированы на прием большого числа посетителей, бизнес-центры, созданные на базе промышленных предприятий и научно-исследовательских институтов, имеют режимные ограничения в свободном проходе посетителей, что связано с профильной деятельностью предприятий. Такие предприятия обязаны иметь бюро пропусков и систему контроля входа-выхода посетителей.

Бюро пропусков такого бизнес-центра обрабатывает персональные данные посетителей и, следовательно, на предприятии должны исполняться требования федерального закона 152-ФЗ от 27.06.2006 г. «О персональных данных». В связи с этим оператор персональных данных (собственно предприятие) должен утвердить мотивированную цель для получения, обработки и хранения персональных данных.

Такими целями могут являться: идентификация посетителей для предотвращения несанкционированного доступа к конфиденциальной информации предприятия, идентификация посетителей для защиты собственности предприятия, идентификация посетителей на предприятии, имеющем статус режимного объекта, для предотвращения проноса опасных веществ и взрывчатки, для ограничения доступа в производственные помещения и т.п.

Обработка персональных данных в бюро пропусков может быть автоматизированной и неавтоматизированной. Для обоих типов обработки оператору персональных данных необходимо закрепить документально (разработать и утвердить): способ фиксации и обработки полученной информации, перечень лиц имеющих доступ к журналам с занесенной в них персональной информацией, сроки обработки и порядок уничтожения персональной информации, а также инструкцию на случай отказа посетителя в предоставлении своих персональных данных. В дополнение ко всему, при автоматизированной обработке требуется: проведение классификации информационной системы персональных данных, утверждение модели угроз и принятие мер по нейтрализации выявленных угроз. Каждый посетитель организации должен быть уведомлен (под роспись) о сборе, хранении и обработке своей персональной информации.

При отказе в предоставлении персональной информации посетителем коммерческого объекта, на котором не установлен режим коммерческой тайны или иные режимы, бюро пропусков (отдел охраны) не может воспрепятствовать в проходе на территорию, иначе будут нарушены конституционные права и свободы гражданина Российской федерации. В качестве организационных мер безопасности, отказавшегося предоставить свои персональные данные посетителя рекомендуется сопроводить сотрудником охраны или принимающей стороны до места назначения. Если же предприятие имеет статус режимного объекта, возможен вариант полного ограничения доступа такого посетителя на территорию охраняемого объекта.

Возможен вариант предоставления своей персональной информации посетителем без подтверждения. Такой вариант оптимален, например, для прохода на территорию бизнес-центра с минимальными требованиями по безопасности.

В бюро пропусков организаций, где практикуется принудительное сканирование паспортов посетителей, необходимо либо отменить данное мероприятие, либо ввести дополнительный журнал учета под роспись согласия посетителей на обработку биометрических данных. Копии паспортов

желательно удалять сразу после того, как посетитель покинет территорию организации. Удаление данных должно осуществляться сертифицированными программными средствами.

Один из важнейших этапов обеспечения безопасности информационной системы персональных данных бюро пропусков – обучение и информирование сотрудников предприятия. На данном этапе необходимо четко и ясно описать цели сбора, обработки персональных данных, разъяснить должностные инструкции работникам бюро пропусков.

Макшаков В.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

МЕТОД ИДЕНТИФИКАЦИИ ИСТОЧНИКОВ ИМПУЛЬСНОГО РАДИОИЗЛУЧЕНИЯ

Неотъемлемой частью идентификации сигналов является их обработка. Цифровая обработка сигналов (ЦОС) – это динамично развивающаяся область вычислительной техники, которая охватывает как технические, так и программные средства. Родственными областями для цифровой обработки сигналов являются теория информации, в частности, теория оптимального приема сигналов и теория распознавания образов - классификация и идентификация сигнала.

В широком смысле под системами ЦОС понимают комплекс алгоритмических, аппаратных и программных средств. Как правило, системы содержат специализированные технические средства предварительной (или первичной) обработки сигналов и специальные технические средства для вторичной обработки сигналов. Средства предварительной обработки предназначены для обработки исходных сигналов, наблюдаемых в общем случае на фоне случайных шумов и помех различной физической природы и представленных в виде дискретных цифровых отсчетов, с целью обнаружения и выделения (селекции) полезного сигнала, его пеленгования и оценки характеристик обнаруженного сигнала. Полученная в результате предварительной обработки полезная информация поступает в систему вторичной обработки для классификации, архивирования, структурного анализа и т.д.

Распознавание по виду и параметрам модуляции является необходимым этапом при решении задач идентификации сигналов.

При радиомониторинге одной из основных задач является восстановление структуры принятого сигнала. По структуре затем можно определить тип источника радиоизлучения (ИРИ), или использовать ее в качестве эталонного описания ИРИ. График мгновенной частоты содержит практически всю информацию о сигнале, необходимую для выявления его структуры. Оценку мгновенной частоты предлагается находить по модели, используемой в модифицированном методе Прони. Для повышения точности оценивания при наличии шумов необходимо увеличивать количество отсчетов на интервале измерения. Метод дает приемлемые результаты при отношении сигнал/шум 10 и более dB, при этом количество отсчетов, используемых для получения одного значения частоты, не превышает пяти.

В системах радиомониторинга определение типа ИРИ по принятому сигналу осуществляют на основе описаний эталонов, которые тем или иным образом собирают в библиотеку. Предлагается строить эти описания в виде грамматик, алфавиты которых – это элементарные фрагменты сигнала, характеризуемые начальной и конечной частотой, длительностью и изменением фазы. Паузы так же являются частью алфавита. Тогда конкретный эталон сигнала может быть представлен грамматикой над этим алфавитом, а конкретный сигнал после восстановления его структуры – словом. Отождествление сигнала (слова) с некоторым эталоном состоит в выводе этого слова из грамматики – эталона типа ИРИ.

Построение эталонной грамматики сигналов некоторого типа ИРИ может быть выполнено в обратном направлении, а именно, имея набор реальных записей сигналов, относящихся определенно к некоторому типу ИРИ, можно, построив слова, описывающие структуры этих сигналов, методами восстановления грамматик получить требуемые описания.

Существуют разные языки описания грамматик. Ввиду того, что нам потребуется не только по грамматике строить контрольные сигналы, но и по реальному сигналу восстанавливать его структурное описание, удобно за основу языка взять отношение соседства между подфрагментами.

Михайлов Н.С.
Россия, Санкт-Петербург, ОАО «Равенство»

РАЗГРАНИЧЕНИЕ ПРАВ ДОСТУПА В ИНТЕГРИРОВАННОЙ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ

При построении интегрированной корпоративной информационной системы (КИС) возникает ряд проблем, связанных с обеспечением защиты информации. Одна из них - необходимость обеспечения требуемого уровня защиты информации при организации доступа к данным смежных подсистем КИС. При этом подсистемы интегрированной КИС могут иметь собственные системы разграничения прав доступа.

Для решения данной проблемы достаточно реализовать механизм синхронизации пользователей и контроля смежных прав доступа на уровне промежуточного программного

обеспечения. За основу необходимо взять данные из ИС, содержащей актуальную информацию о штатном расписании и организационной структуре предприятия. Такой подход даёт «побочный» положительный эффект. Учетные данные пользователей уволенных или принятых на работу сотрудников будут находиться в актуальном состоянии. Для новых сотрудников будет обеспечен оперативный доступ к нужным ИС, а учетные данные уволенных сотрудников будут вовремя заблокированы.

Лавренов В.В.
Беларуссия, Минск, Академия МВД Республики Беларусь

ОЦЕНКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ РЕСПУБЛИКИ БЕЛАРУСЬ

Информационная сфера превращается в системообразующий фактор жизни людей, обществ и государств. Информационные технологии нашли широкое применение в управлении важнейшими объектами жизнеобеспечения, которые становятся более уязвимыми перед случайными и преднамеренными воздействиями. Происходит эволюция информационного противоборства как новой самостоятельной стратегической формы глобальной конкуренции. В связи с этим информационная безопасность играет важную роль в существовании и развитии любого государства. Мировые эксперты считают наиболее опасными угрозами информационной безопасности рост киберпреступности, компьютерного терроризма и использование информационно-коммуникационных технологий в межгосударственных конфликтах.

В рамках государственной системы информационной безопасности проблема обеспечения безопасности современных автоматизированных систем органов внутренних дел стоит в ряду первых и самых важных. Сложность этих систем, разветвленность составляющих их основу компьютерных сетей еще больше усугубляют ситуацию. Как показывает анализ, в органах внутренних дел большинство автоматизированных систем обработки информации в общем случае представляет собой территориально распределенные системы взаимодействующих между собой по данным и управлению локальных вычислительных сетей и отдельных ЭВМ. В результате чего в распределенных автоматизированных системах возможны все "традиционные" для локально расположенных вычислительных систем способы несанкционированного вмешательства в их работу и доступа к информации. Кроме того, для них характерны и новые специфические каналы проникновения в систему и несанкционированного доступа к информации.

Для успешного выполнения задач по обеспечению информационной безопасности автоматизированных систем органов внутренних дел должна быть выработана действенная система ее оценки. Начать надо с выбора методики, по которой будет проводиться оценка информационной безопасности. Методики можно разделить на качественные и количественные, в зависимости от шкал, применяемых для оценки вероятности реализации угрозы и тяжести последствий от её реализации. Кроме того, отличия методик заложены в подходах и процедурах оценки информационной безопасности. К основным из которых можно отнести следующие:

1). Метод оценки информационной безопасности, основанный на построении модели угроз и уязвимостей;

2). Метод оценки информационной безопасности, основанный на построении модели информационных потоков.

Первая методика основана на использовании преимущественно экспертной и статистической информации об угрозах и уязвимостях. Для оценки рисков в информационной системе органов внутренних дел определяется защищенность каждого ресурса при помощи оценки вероятностей реализации угроз, а также уязвимостей, через которые данные угрозы могут быть реализованы. Указанная оценка вероятностей позволяет ранжировать угрозы и уязвимости по степени рисковости.

Во второй - оценки параметров информационных потоков в условиях высокой степени неопределенности условий функционирования системы должны вычисляться с использованием не одной математической модели, а согласованного семейства моделей, адаптивно конструирующихся одна из другой и, таким образом, непрерывно совершенствующихся на основе оптимального выбора исходных данных.

Независимо от выбранной методики, процесс оценки информационной безопасности в себя выполнение следующих задач: определение области оценки информационной безопасности; оценка информационной безопасности; обработка полученных результатов; мониторинг и контроль; совершенствование процесса.

Таким образом, оценки информационной безопасности как в государстве в целом, так в органах внутренних дел в частности – достаточно трудоемкая и значимая задача для любой информационной системы и требующая выполнения ряда условий:

– во-первых, необходимо построение гибких моделей исследуемой информационной системы, описывать ее комплексно, с учетом программных, аппаратных ресурсов, внутренних и внешних угроз и уязвимостей;

– во-вторых, с учетом значительного количества факторов риска, математическая модель оценки информационной безопасности должна допускать разработку эффективных численных алгоритмов обработки информации в моделях;

– в-третьих, должна быть предельно прозрачна методика оценки информационной безопасности, чтобы владелец информации мог адекватно оценить применимость и эффективность методики к конкретной информационной системе.

Полубелова О.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

СТРАТЕГИИ РАЗРЕШЕНИЯ АНОМАЛИЙ ФИЛЬТРАЦИИ МЕЖСЕТЕВЫХ ЭКРАНОВ

Системы защиты информации (СЗИ) в компьютерных сетях, основанные на политиках безопасности, не теряют своей популярности благодаря гибкости в управлении и удобству администрирования. Политика фильтрации формируется специалистами, знающими особенности защищаемой сети и используемых межсетевых экранов (МЭ), на основе общей политики безопасности компании, закрепленной в регламентирующих документах. Однако эта задача является сложной и подверженной ошибкам из-за важности учета различных зависимостей правил, а также необходимости проверки согласованности новых правил со всей политикой. Эта сложность увеличивается по мере роста размера сети. Таким образом, для успешного развертывания СЗИ и поддержания ее функционирования требуется проводить регулярный анализ политики фильтрации на предмет выявления аномалий.

Наиболее полная классификация аномалий выглядит следующим образом:

затенение – когда правило с большим приоритетом обрабатывает все пакеты, которые удовлетворяют условиям правила с меньшим приоритетом, и привилегии (разрешение/запрет) у этих правил – различны. В этом случае правило с меньшим приоритетом никогда не будет активировано;

обобщение – когда множество пакетов, удовлетворяющих условию правила с большим приоритетом, является подмножеством пакетов, удовлетворяющих условию правила с меньшим приоритетом, и привилегии этих правил – различны. Правило с меньшим приоритетом никогда не будет активировано на этом подмножестве;

корреляция – когда пересечение множеств пакетов, задаваемых условиями двух правил, не пусто, но в то же время оно не совпадает ни с одним из этих множеств; при этом привилегии этих правил различны. В этом случае правило с меньшим приоритетом никогда не будет активировано на указанном пересечении;

избыточность – когда пересечение множеств пакетов, задаваемых условиями двух правил, не пусто, при этом привилегии этих правил совпадают. Возможно, такая ситуация связана с ошибкой администратора, и одно из правил можно удалить или разделить на части.

Вторая задача, которая стоим перед администратором безопасности – это разрешение обнаруженных аномалий.

Автором разработана методика верификации правил фильтрации, которая включает в себя следующие этапы: трансляции во внутренний формат, построения верифицируемой модели, вычисления модели, интерпретации результатов, разрешения аномалий. На завершающем этапе разрешения аномалий оператор выбирает, к каким аномалиям применить автоматическую стратегию разрешения, а какие потребуется корректировать вручную. После корректировки процесс верификации запускается снова.

В литературе описаны различные подходы к разрешению конфликтов и аномалий в политиках безопасности для СЗИ, основанных на политиках. Стратегии предусматривают как динамическое, так и статическое разрешение конфликта. Автоматические стратегии могут быть использованы во время функционирования устройства, если будет выявлен конфликт в режиме динамической верификации. Но большая часть стратегий предполагает использование во время автономного режима верификации.

Можно выделить следующие возможные виды стратегий, наиболее часто используемые в современных системах СЗИ: стратегия “первое правило соответствия” (“First matching rule”, FMR); стратегия “более специфицированное правило” (“Most Specific Take Precedence”, MSTP); стратегия “приоритет у запрещающих правил” (“Denials take precedence”, DTP); стратегия “ручное разрешение” (“Manually resolve”, MR).

Рассмотрим более подробно каждую из них. Стратегия FMR основана на том, что всегда выбирается первое правило, которое в том числе имеет наибольший приоритет.

Стратегия MSTP предполагает, что должно быть выбрано правило, задающее более узкий диапазон адресов. Например, в правилах фильтрации приоритет будет у правила, которое фильтрует пакеты, приходящие на конкретный порт, чем то, которое предполагает, что порт может быть любой.

В стратегии DTP приоритет всегда у тех правил, которые запрещают прохождение трафика.

Последняя стратегия, MR, применяется при автоматизированном разрешении, т.е. с участием оператора. Для него будет предоставлены пара правил, вызывающих аномалию, и предложено выбрать, какое из них удалить, либо разбить на части.

Выбор применения тех или иных стратегий зависит от общей заданной политики безопасности.

Работа выполняется при поддержке РФФИ (проекты 11-07-00435-а, 13-01-00843-а) и программы фундаментальных исследований ОНИТ РАН.

Потехин В.С., Синещук Ю.И., Скряга Ю.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,
Военно-морская академия им. Адмирала Флота Советского Союза Н.Г. Кузнецова

ИНФОРМАЦИОННЫЕ УГРОЗЫ И УЯЗВИМОСТИ ТЕХНОЛОГИИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Научные исследования в области управления сложными организационно-техническими системами неразрывно связаны с совершенствованием системы управления, информационной поддержки лица принимающего решение (ЛПР). Процессы управления характеризуются большим разнообразием и динамичностью ситуаций, повсеместным использованием новых высокотехнологичных средств, повышенной потребностью ЛПР всех уровней и звеньев управления в актуальной, достоверной, оперативной и всесторонней информации, необходимой для качественного решения задач управления.

Современный этап информатизации базируется на передовых информационных технологиях и телекоммуникационных сетях, соединяющих в единое целое совокупность разнородных вычислительных средств, ЛВС, удаленных и местных терминалов. Системообразующей основой интеграции процессов управления и средств их автоматизации на разных иерархических уровнях должно стать единое информационное пространство (ЕИП).

Создание столь сложных и глобальных информационно-телекоммуникационных систем не должно проходить без комплексного решения проблемы обеспечения безопасности, вообще, и защиты информации, в частности. В этой связи, задача обеспечения безопасности единого информационного пространства является наиболее приоритетной.

Эффективность ЕИП во многом определяется качеством и безопасностью реализуемых информационных технологий. В начале 2000 годов появилась технология, на которую поначалу не обратили внимания, но со временем стали к ней присматриваться и к 2010 году на рынке информационных услуг появилось новое понятие – «облако».

Согласно определению, выдвинутому IEEE (англ. Institute of Electrical and Electronics Engineers), облачная технология – это концепция, при которой пользовательская информация постоянно хранится на интернет-серверах и лишь временно кэшируется на стороне пользователя. При этом доступ к сервису можно получить используя не только стационарные компьютерные системы, но и любые другие вычислительные средства: ноутбуки, планшеты, смартфоны и т.д.

Сама по себе технология является отражением всеобщей тенденции глобализации информационных систем, развитие которых сопровождается расширением перечня угроз, появлением дополнительных уязвимостей информационным ресурсов и, как следствие, совершенствованием способов реализации информационных атак.

Выделяют следующие виды угроз для облака:

- неправомерное использование облачных технологии;
- небезопасные программные интерфейсы (API);
- внутренние нарушители;
- уязвимости в облачных технологиях;
- потеря или утечка данных;
- кража персональных данных и неправомерный доступ к сервису;
- прочие уязвимости.

Это требует принятия адекватных мер и применения соответствующих средств защиты, которые должны предотвращать:

- ложную инициализацию обмена;
- несанкционированный доступ;
- необоснованный отказ в доступе;
- раскрытие содержания передаваемых данных;
- внесение изменений в передаваемые данные;
- возможность измерения и анализа характеристик информационной системы, которые повлекут раскрытие защищаемой информации.

Решение задачи применения технологии безопасных облачных вычислений, в рамках ЕИП, позволяет:

Во-первых, обеспечить общий доступ и совместную обработку информационных ресурсов.

Во-вторых, повысить устойчивость системы управления и обеспечить быстрое развёртывание ее элементов на другом физическом объекте автоматизации.

В-третьих, получить экономический эффект поскольку отпадает необходимость закупки дорогостоящего программного обеспечения для работы с данными на все существующие комплексы средств автоматизации.

Советов Б.Я., Колбанёв М.О., Татарникова Т.М.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербургский государственный экономический университет

МОДЕЛЬ ФИЗИЧЕСКИХ ХАРАКТЕРИСТИК СИГНАЛОВ

Информационное взаимодействие на материальном метауровне основано на материальной природе данных и может быть количественно описано изменением трех групп физических характеристик сигнала:

– пространственных – это геометрическая мера, которая определяет положение сигнала в пространстве, как, например, плотность размещения оборудования, удаленность пользователей, плотность записей на носителях данных или уровень техпроцесса;

– временных – это мера для сопоставления порядка возникновения событий, связанных с изменением состояния сигнала, например, времена сохранения, доставки и обработки данных, время распространения сигнала, время переключения элементов электрических схем, а также характеристики, обратные времени и имеющие смысл интенсивности наступления событий;

– энергетических – это мера для оценки усилий, которые необходимо совершить для изменения сигнала, например, киловатт-часы потребляемой энергии, выделяемая тепловая мощность или масса выделяемого углеводорода при выработке электроэнергии.

В теории передачи сигналов введено понятие объем сигнала. Этот параметр вычисляется как объем прямоугольного параллелепипеда, ребра которого имеют длину, равную длительности сигнала, его спектру и превышению уровня сигнала над помехой. Объем параллелепипеда пропорционален объему данных, которые поступили от источника и должны быть переданы по каналу связи. Он не зависит от технологий передачи данных и потребляемых ими ресурсов, а лишь определяет достаточные условия для передачи сигнала по каналу связи.

По аналогии, для согласования физических характеристик информационных технологий и требований к ним со стороны пользователей построена модель физических характеристик сигнала в виде прямоугольного параллелепипеда в первом октанте трехмерного пространства. Ребра параллелепипеда, расположенные на осях ординат, абсцисс и аппликат, отображают, соответственно, пространственные, временные и энергетические характеристики сигнала, зависящие от технологии его формирования. Если требования пользователей к физическим характеристикам информационных технологий представить аналогичным образом, то использование технологии станет возможным только тогда, когда параллелепипед, описывающий сигнал, «поместится» внутри параллелепипеда, описывающего требования пользователей. Любой из параметров параллелепипеда, будь то объем, площадь граней, отношения длин ребер и др., могут рассматриваться как характеристики технологии. Например, оценивая производительность и эффективность информационных систем, сегодня используют такие комплексные характеристики:

– объем энергии, потребляемой в расчете на число оказанных информационных услуг в единицу времени,

– стоимость выполнения транзакций в киловатт-часах или объеме выбросов в атмосферу соединений углерода,

– объем выбросов углерода в пересчете на один сервер или на группу пользователей,

– соотношение энергопотребления информационного оборудования, с одной стороны, и инженерных систем, поддерживающих его работу, с другой,

– энергопотребление на 1 кв. м. площади технических помещений и др.

Любая их этих комплексных характеристик всегда может быть вычислена, если известны длины ребер соответствующего параллелепипеда.

В отличие от модели объема сигнала, в которой длительность, спектр и превышение уровня сигнала над помехой не зависят друг от друга, у цифровых информационных технологий, напротив, существует зависимость между параметрами пространства, времени и энергии, такая, что изменение одного из них ведет к изменению других. Это означает, что каждой технологии формирования сигнала соответствует параллелепипед со специфическими свойствами.

Учет затрат на обеспечение информационных технологий физическими ресурсами становится особенно существенным при проектировании мощных информационных систем таких как системы долговременного хранения данных, высокопроизводительные сети связи, центры обработки данных или суперкомпьютеры. Для пользователей таких систем важны не только возможности информационных технологий в части объемов хранения, скорости передачи и обработки данных, но и объемы занимаемого пространства, временные параметры физических процессов и потребляемая энергия. Поэтому при проектировании подобных информационных систем следует рассматривать все

доступные информационные технологии сохранения, распространения и обработки, учитывать в процессе выбора все их физические характеристики и согласовывать эти характеристики с задачами, которые формулируют и решают пользователи.

Предлагаемая модель призвана помочь при принятии соответствующих решений.

Саенко И.Б., Куваев В.О.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН, Военная академия связи им. С.М. Буденного

ОБ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЕ РАЗГРАНИЧЕНИЯ ДОСТУПА К РЕСУРСАМ ЕДИНОГО ИНФОРМАЦИОННОГО ПРОСТРАНСТВА ДЛЯ РАЗНОРОДНЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Интеграция информационных ресурсов, используемых разнородными автоматизированными системами, принадлежащими к одной или нескольким организациям либо ведомствам, в единую техническую систему, определяемую термином «единое информационное пространство» (ЕИП), является характерной тенденцией дальнейшего развития современных информационных систем и технологий в административно-государственной, промышленной, финансовой, оборонной и других сферах общественной жизни. При этом вопросы разграничения доступа в ЕИП, как и другие аспекты обеспечения его безопасности, становятся достаточно актуальными. Это обусловлено тем, что разнородность ресурсов, интегрированных в ЕИП, предполагает наличие не только аппаратных, программных и информационных различий в области их построения и использования, но и различий в политиках обеспечения их безопасности, в применяемых механизмах защиты, в схемах разграничения доступа и т.д. Совместное использование этих ресурсов разнородными автоматизированными системами с необходимостью предполагает уточнение и доработку соответствующих политик безопасности и механизмов защиты и создания специальной системы разграничения доступа к ресурсам ЕИП.

При разработке архитектуры, моделей и методов функционирования такой системы разграничения доступа предлагается ориентироваться на методы искусственного интеллекта. Такой подход во многом обусловлен неполнотой и/или противоречивостью исходных данных, масштабностью вычислительных затрат, необходимых для решения этой задачи традиционными математическими методами, а также имеющимися результатами анализа мирового опыта разработки и успешного использования интеллектуальных средств и механизмов защиты информации в компьютерных системах и сетях. Предполагается, что разрабатываемые для этой цели модели, методы и методики будут базироваться на следующих подходах: методах эволюционного моделирования нарушителя и средств защиты; верификации политик разграничения доступа на основе темпоральных, дескрипционных и других видов логик; представлении схем разграничения доступа с помощью XML-ориентированных языков и форматов представления, включая онтологические языки OWL (Web Ontology Language) и SWRL (Semantic Web Rule Language); совершенствовании политик и схем разграничения доступа на основе биоинспирированных методов оптимизации (включая генетические алгоритмы); оценке и прогнозировании состояния ресурсов с помощью временных рядов и нейросетевых моделей; анализе и контроле уровня обеспечения требований по разграничению доступа путем интеграции методов моделирования и методов интеллектуального анализа данных.

К числу основных задач, решение которых позволит осуществить построение интеллектуальной системы разграничения доступа к ресурсам ЕИП, предлагается отнести следующие.

1. Оценка защищенности ресурсов ЕИП от несанкционированного доступа и эффективности построения системы разграничения доступа к ресурсам ЕИП. Результаты такой оценки необходимы в первую очередь для мониторинга безопасности ЕИП. Из-за масштабности и разнородности ЕИП она требует обработки крайне большого объема данных в условиях дефицита времени.

2. Ориентированное на знания представление, верификация и оптимизация политик и схем разграничения доступа к ЕИП. Построение ЕИП требует перехода на использование единых принципов, форматов и языков представления данных, предусматривающее конвертацию локальных политик и схем доступа в единые централизованные политики и схемы. Предлагается использовать для этих целей XML-ориентированные языки представления онтологий OWL и SWRL.

3. Интеллектуальная поддержка принятия решений по разграничению доступа к ресурсам ЕИП на основе логического вывода и визуализации данных о политиках, схемах и событиях доступа. Для реализации логического вывода в ЕИП предлагается ориентироваться на методы верификации, в частности, на Model checking («проверка на модели»). Визуализация данных в свою очередь предлагает достаточно эффективный подход к анализу политик и схем разграничения доступа.

4. Управление уровнем защищенности ресурсов ЕИП на основе применения методов адаптации политик и схем разграничения доступа к изменениям условий и режимов функционирования ЕИП. Для решения этой задачи предлагается использовать модели временных

рядов и нейронных сетей, методы моделирования угроз, атак, вторжений, уязвимостей и методы интеллектуального анализа данных.

Работа выполняется при поддержке РФФИ (проекты 11-07-00435-а, 13-01-00843-а и 13-07-13159-офи_м_РЖД) и программы фундаментальных исследований ОНИТ РАН.

Сенцова А.Ю., Машкина И.В.
Россия, Уфа, Уфимский государственный авиационный технический университет

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОЙ НЕЙРОННОЙ СЕТИ ДЛЯ ОЦЕНКИ РИСКА НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

В настоящее время технология облачных вычислений интенсивно развивается и получает все более широкое распространение. Компании – поставщики облачных сервисов (вендоры) предлагают несколько видов моделей развертывания взаимодействий в облаке, организация-заказчик должна определить, какая из моделей необходима для реализации бизнес-процессов.

С точки зрения информационной безопасности облачные вычисления имеют некоторые особенности, связанные с тем, что заказчик не имеет доступа к облачной инфраструктуре вендора. При этом заказчик имеет тот уровень защищенности в облачной системе, который обеспечивается вендором. Поэтому существует необходимость анализа и оценки возможных рисков нарушения информационной безопасности в системе облачных вычислений (СОбВ).

В работе рассматривается возможность расчета оперативного значения уровня риска нарушения информационной безопасности в системе облачных вычислений. Для решения этой задачи разработана модель угроз в виде нечетких когнитивных карт и используется механизм искусственной нейронной сети.

СОбВ является информационной системой, в которой взаимодействуют заказчик услуг и вендор. Оценить риск нарушения информационной безопасности в общем виде невозможно. Поэтому, на основе анализа известных описаний облачных архитектур и технологий клиент-серверного взаимодействия, в работе предложен вариант построения СОбВ.

Опасность возникновения ущерба или убытков в результате использования организацией облачных сред может быть оценена величиной риска нарушения информационной безопасности в системе облачных вычислений. Риск обусловлен наличием угроз нарушения безопасности информации. Необходимо в первую очередь идентифицировать все возможные угрозы, источники угроз, каждая угроза должна быть детализирована и оценена с учетом наличия уязвимостей на путях ее распространения. Разработанная модель угроз представляет собой нечеткие когнитивные карты (НКК), построенные с учетом архитектуры системы облачных вычислений.

Нечеткие когнитивные карты были разработаны с учетом компонентов инфраструктуры СОбВ, расположенных на путях распространения атак, с учетом всех возможных источников угроз, реализуемых злоумышленником, внутренним пользователем заказчика, другим клиентом вендора, администратором вендора в СОбВ.

Использование НКК позволяет произвести моделирование процессов распространения угроз в системе облачных вычислений через используемые уязвимости компонентов ее архитектуры. При этом полученная модель обладает свойством наглядности.

Значения уязвимостей на путях распространения атак определены нормализацией значений из международной базы данных NVD, в случае отсутствия значения уязвимости компонента в NVD, значение задается равным 0,5, что дает наименьшую погрешность.

Метод расчета прогнозируемого значения риска нарушения ИБ на основе построения нечетких когнитивных карт был описан в предыдущих работах. Предлагается применить данный метод для нового объекта – системы облачных вычислений. Метод позволяет получить оценку прогнозируемого значения риска для наихудшего случая, когда активизируются одновременно все возможные источники угроз. Он применим на стадии проектирования системы информационной безопасности для СОбВ, а также может быть использован для расчетов с целью формирования множества данных обучающей выборки для обучения искусственной нейронной сети (ИНС).

После настройки ИНС может быть использована для оценивания риска нарушения ИБ в реальном масштабе времени.

Для обучения ИНС с помощью сформированного массива данных был использован программный модуль Matlab 6.0. В процессе настройки нейронной сети был выбран однослойный персептрон с числом нейронов в скрытом слое равным двадцати. Нейронная сеть прошла 33 эпохи, постепенно обучаясь и сокращая ошибку обучения. В конце эксперимента ошибка была равна 10^{-7} мсэ.

Предлагаемые решения на основе НКК и ИНС могут быть применимы специалистами по ИБ, для управления рисками нарушения ИБ в СОбВ, а именно уменьшения оперативного значения уровня риска до приемлемого уровня за счет выбора рационального варианта реагирования на атаку в реальном масштабе времени.

Соколов С.С., Бориев З.В.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова

МЕТОД ОБЕЗЛИЧИВАНИЯ КАК ФАКТОР УМЕНЬШЕНИЯ РИСКОВ РЕАЛИЗАЦИИ УГРОЗЫ РАЗГЛАШЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ХРАНЕНИИ В ИНФОРМАЦИОННЫХ БАЗАХ ДАННЫХ

27 июля 2006 года Президент России подписал закон №152-ФЗ «О персональных данных». В сферу действия этого нормативного акта попадают все юридические и физические лица, являющиеся обработчиками приватных сведений других граждан. Новый закон требует, чтобы каждая организация, владеющая персональными данными своих сотрудников, клиентов, партнеров и т.д., обеспечила конфиденциальность всей этой информации. В случае нарушения положений закона компания может лишиться лицензии и подвергнуться судебному преследованию со стороны граждан, чьи приватные записи были обнародованные. Кроме того, виновные лица, нарушившие требования закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством РФ ответственность.

Как правило, обработка персональных данных в современных организациях осуществляется с использованием информационных средств автоматизации деятельности с непосредственным хранением в базах данных. Основными программными средствами, обеспечивающими функционирование баз данных, являются системы управления базами данных. СУБД является инструментом для разработки прикладных программ, с помощью которых можно создавать, наполнять и работать с базами данных. По типу управляемой базы СУБД делятся на 5 групп:

– Иерархические СУБД имеют централизованную структуру, т.е. безопасность данных легко контролировать. Поиск записи осуществляется методом прямого обхода структуры. Их необходимо правильно упорядочивать, чтобы время их поиска было минимальным.

– Сетевые СУБД расширяют иерархическую модель СУБД, позволяя группировать связи между записями в множества. С логической точки зрения связь — это не сама запись. Связи лишь выражают отношения между записями. Сетевая модель поддерживает специальные языки, предназначенные для определения структуры базы данных и составления запросов. В сетевой модели допускаются отношения «многие ко многим», а записи не зависят друг от друга.

– Реляционные СУБД в сравнении с иерархическими и сетевыми моделями требуют от сервера СУБД более высокого уровня сложности. Здесь база данных представляет собой централизованное хранилище таблиц, обеспечивающее безопасный одновременный доступ к информации со стороны многих пользователей. В реляционной модели СУБД достигается информационная и структурная независимость. Записи не связаны между собой настолько, чтобы изменение одной из них затронуло остальные. В реляционных СУБД применяется язык SQL, позволяющий формулировать произвольные, нерегламентированные запросы.

– Объектно-ориентированные СУБД решают две проблемы. Во-первых, сложные информационные структуры выражаются в них лучше, чем в реляционных базах данных, а во-вторых, устраняется необходимость транслировать данные из того формата, который поддерживается в СУБД. ООСУБД выполняют много дополнительных функций. Это окупается сполна, если отношения между данными очень сложны. В таком случае производительность ООСУБД оказывается выше, чем у реляционных СУБД.

– Объектно-реляционные СУБД объединяют в себе черты реляционной и объектной моделей. Их возникновение объясняется тем, что реляционные базы данных хорошо работают со встроенными типами данных и гораздо хуже — с пользовательскими, нестандартными. Когда появляется новый важный тип данных, приходится либо включать его поддержку в СУБД, либо заставлять программиста самостоятельно управлять данными в приложении. Не всякую информацию имеет смысл интерпретировать в виде цепочек символов или цифр. Объектно-реляционная СУБД позволяет загружать код, предназначенный для обработки «нетипичных» данных. Таким образом, база данных сохраняет свою табличную структуру, но способ обработки некоторых полей таблиц определяется извне, т.е. программистом.

Несмотря на все различия между типами СУБД, одной из главных задач является защита хранимой информации.

Защита программных средств достаточно сложна и трудоемка, а также имеет специфику в зависимости от типа программного обеспечения.

Конфиденциальность, являясь одним из свойств защищаемой информации, требует современных средств и методов обеспечения безопасности. Одним из таких методов является метод обезличивания данных. Обезличивание может быть выполнено по различным признакам и имеет специфику в зависимости от структуры данных. Например, возможно обезличивать, изменяя и удаляя фамилию, имя, отчество, паспортные данные. Однако, в ряде структур каждый сотрудник имеет строгую идентификационную метку и может быть по ней идентифицирован, в этом случае необходимо отдельно экспертно определять определяющие человека параметры и направлять методы обезличивания на них.

Соколов С.С., Ежгуров В.Н.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова

СИТУАЦИОННАЯ МОДЕЛЬ НАРУШИТЕЛЯ В ИНФОРМАЦИОННЫХ СИСТЕМАХ НА ТРАНСПОРТЕ

Формируя модель нарушителя в информационных системах на транспорте (ИСТ) следует учитывать фактор неоднородности природы информационных ресурсов, каналов передачи данных и информации ИСТ.

Прежде, чем рассматривать модель нарушителя в динамике изменения ситуаций следует определиться с понятиями.

Под нарушителем информационной безопасности транспортной системы (ТС) понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб информационным ресурсам ТС. Нарушители могут быть внутренними и внешними.

К внутренним нарушителям можно отнести следующих сотрудников предприятий транспортной отрасли: обслуживающий персонал (системные администраторы, администраторы баз данных, администраторы приложений и т.п., отвечающие за эксплуатацию и сопровождение технических и программных средств), программисты, отвечающие за разработку и сопровождение системного и прикладного программного обеспечения, технический персонал, сотрудники основных подразделений транспортной сферы, которым предоставлен доступ на объекты (помещения, транспортные средства и т.п.), где расположено компьютерное или телекоммуникационное оборудование; а так же лиц находящихся под присмотром сотрудников, имеющих доступ к оборудованию, но не являющихся персоналом организации.

К внешним нарушителям относятся лица, пребывание которых в помещениях с оборудованием без контроля со стороны сотрудников объекта невозможно.

Модель вероятного нарушителя безопасности ИС необходима для систематизации информации о методах несанкционированных воздействий со стороны нарушителя, целях несанкционированных воздействий субъектов и выработки адекватных организационных и технических мер противодействия.

При разработке модели нарушителя ИС учитываются:

– предположения о категориях лиц, к которым может принадлежать нарушитель;
– тип нарушителя;
– предположения о мотивах действий нарушителя (преследуемых нарушителем целях);
– предположения о квалификации нарушителя (уровень подготовленности) и его технической оснащенности (об используемых для совершения нарушения методах и средствах);
– ограничения и предположения о характере возможных действий нарушителей;
– характер информационных угроз;
– доступные ресурсы (требуемая материальная база для подготовки взлома конкретного участка системы).

Для того, чтобы модель нарушителя приносила максимальную пользу, она должна быть сориентирована на конкретный объект защиты (модель не может быть универсальной), учитывать мотивы действий и социально-психологические аспекты нарушения, потенциальные возможности по доступу к информационным ресурсам различных категорий внешних и внутренних нарушителей на различных пространственно-временных срезах объекта защиты.

Правильно построенная модель нарушителя информационной безопасности, (адекватная реальности), в которой отражаются его практические и теоретические возможности, априорные знания, время и место действия и т.п. характеристики - важная составляющая успешного проведения анализа риска и определения требований к составу и характеристикам системы защиты.

Анализ ранее проведенных атак позволяет сформировать первый рубеж модели информационной безопасности, обучаясь на опыте других.

Успех реализации атаки на информационные ресурсы со стороны нарушителя определяется не только личностью нарушителя, но и рядом других обстоятельств: ситуацией, степенью правильности выбранной стратегии атаки, методов и средств её проведения, характером защищенности ресурса. Ситуационный подход к изучению эффективности реализации угрозы требует исследования взаимодействия различных ситуационных переменных для того, чтобы обнаружить причинно-следственную зависимость между обстоятельствами атаки и успешностью её реализации, позволяющую предсказать возможное поведение нарушителя и возможные последствия его поведения.

В связи с бурным развитием информационных технологий, методов и средств противодействия угрозам информационной безопасности, наиболее эффективные нарушители находятся в постоянном поиске новых идей и средств реализации атаки. В этой связи необходимо строить и исследовать модель нарушителя не с точки зрения только стандартных, шаблонных подходов, а с точки зрения возможной динамики, путей их развития и последствий, к которым это может привести.

Солодянников А.В.
Россия, Санкт-Петербург, ЗАО «Ассоциация специалистов информационных систем»

ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ В ОБЩЕЙ СИСТЕМЕ ДЕЛОПРОИЗВОДСТВА ПРЕДПРИЯТИЯ

Проблема восстановления программного обеспечения (ПО), функционирующего в комплексах специального назначения, заключается в отсутствии средств, позволяющих неограниченное число раз и за короткий срок после аварийного завершения работы ввести комплекс в действие.

Успешность организации в современных условиях не может быть надежно стабильной, если в ней не работают стандартные правила конфиденциального делопроизводства. Жесткая конкурентная борьба в условиях рыночной экономики порождает такие явления как промышленный шпионаж и финансовая разведка.

Конфиденциальное делопроизводство должно распространяется на документы, которые содержат в себе сведения, составляющие коммерческую и служебную тайну.

Необходимость объединения конфиденциальных документов, содержащих и коммерческую, и служебную тайну, в одно делопроизводство обусловлено тем, что эти документы идентичны по технологическим процедурам их составления, обработки, обращения, хранения и защиты.

Обязательность ведения делопроизводства в организациях и на предприятиях всех форм собственности обусловлена нормами действующего законодательства Российской Федерации.

Конфиденциальное делопроизводство в отличие от открытого имеет ряд особенностей, обусловленных конфиденциальностью документированной информации. Эти отличия касаются как сферы конфиденциального делопроизводства, так и видов и содержания работ с документами.

Конфиденциальное делопроизводство определяется как деятельность, охватывающая документирование конфиденциальной информации, организацию работы с конфиденциальными документами и защиту содержащейся в них информации. При этом под документированием информации понимается процесс подготовки и изготовления документов, под организацией, работы с документами – их учет, прохождение, исполнение, отправление, классификация, систематизация, подготовка для архивного хранения, уничтожение, режим хранения и обращения, проверки наличия.

Конфиденциальное делопроизводство в силу условий работы с конфиденциальными документами распространяется не только на управленческую, но и на различные виды производственной деятельности, включает в себя наряду с управленческими и научно-технические документы (научно-исследовательские, проектные, конструкторские, технологические и др.). Кроме того, конфиденциальное делопроизводство распространяется как на официальные документы, так и на их проекты, различные рабочие записи, не имеющие всех необходимых реквизитов, но содержащие информацию, подлежащую защите.

Особенностью конфиденциального делопроизводства является и своеобразное переплетение некоторых функций, которые как бы взаимоисключают друг друга. В частности, функциями по реализации задачи документационного обеспечения конфиденциальной деятельности являются:

– создание документов, необходимых и достаточных для такой деятельности;

– предоставление каждому пользователю всех документов, требующихся для выполнения должностных обязанностей, а параллельными им функциями по реализации задачи защиты конфиденциальной информации могут быть:

– предотвращение необоснованного издания и рассылки документов,

– исключение необоснованного ознакомления с документами.

Это означает, что конфиденциальная деятельность должна обеспечиваться минимальным количеством документов при сохранении полноты и достоверности информации – предоставление пользователям всех необходимых документов, но только тех, которые действительно требуются для выполнения должностных обязанностей. По видам работ конфиденциальное делопроизводство отличается от открытого, с одной стороны, большим их количеством, с другой, – содержанием и технологией выполнения многих видов. Помимо этого, третья составляющая конфиденциального делопроизводства – защита содержащейся в конфиденциальных документах информации – вообще не предусмотрена в определении открытого делопроизводства, хотя определяемая собственником часть открытой информации должна защищаться от утраты.

Конфиденциальная информация должна защищаться и от утраты, и от утечки.

К утрате конфиденциальной информации могут привести полные или частичные, безвозвратные или временные потеря документа, хищение или несанкционированное уничтожение документа либо содержащейся в нем информации, искажение и блокирование (для правомочных пользователей) информации.

Под утечкой конфиденциальной информации понимается неправомерный выход информации за пределы защищаемой зоны ее функционирования или установленного круга лиц вследствие разглашения информации, потери носителя информации, хищения носителя информации или содержащейся в нем информации, результатом которых является получение информации лицами, не имеющими к ней санкционированного доступа.

Утрата и утечка конфиденциальной документированной информации обусловлены уязвимостью информации. Уязвимость информации это ее доступность для дестабилизирующих воздействий, т.е. таких воздействий, которые нарушают установленный статус информации.

Наиболее опасными формами проявления уязвимости конфиденциальной документированной информации являются потеря, хищение и разглашение - первые две одновременно могут привести и к утрате, и к утечке информации, вторая (хищение информации при сохранности носителя) и третья могут не обнаружиться, со всеми вытекающими из этого последствиями.

Таким образом, защита содержащейся в конфиденциальных документах информации должна быть направлена на предотвращение потери, хищения, несанкционированного уничтожения, искажения, блокирования и разглашения информации.

Сущность конфиденциального делопроизводства обусловливает его организационные и технологические особенности.

Особенностью конфиденциального документа является то, что он одновременно представляет собой: массовый носитель ценной, защищаемой информации; основной источник накопления и объективного распространения этой информации, а также ее неправомерного разглашения или утечки; обязательный объект защиты.

Таким образом, деятельность по обеспечению конфиденциальности в общем документообороте должна обеспечиваться минимальным количеством документов при сохранении полноты и достоверности информации – предоставление пользователям всех необходимых документов, но только тех, которые действительно требуются для выполнения должностных обязанностей.

Уварова Ю.А.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В УСЛОВИЯХ БЫСТРОЙ СМЕНЫ ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКОЙ СРЕДЫ ГОРОДА СОЧИ

В рамках комплекса мероприятий по подготовке к XXII Олимпийским зимним играм и XI Паралимпийским зимним играм «Сочи 2014» произошли значительные изменения информационно-технологической инфраструктуры города Сочи, что потребовало от учреждений и предприятий, осуществляющих экономическую деятельность в Сочи, перехода на более высокоскоростное электронное взаимодействие.

Быстрая вынужденная смена технологии деятельности в сфере защиты информационных систем персональных данных (ИСПДн) не сопровождена комплексным освоением должностными лицами, уполномоченными на обработку персональных данных (ПДн), нормативного правового поля, организационных мер и технологии защиты ПДн. В результате, в деятельности учреждений/предприятий города Сочи периодически выявляются следующие нарушения. Приведем ряд примеров.

НОЧУ «Экоцентр–Профи», ООО «Новое время», ООО «Левша», ООО «Восьмое небо», ООО «Дагомысская чаеразвесочная фабрика», ООО «Декора-Люкс-1», ООО «ИДС» и ООО «Алмазный берег» до мая 2013 года не уведомили уполномоченный орган по защите прав субъектов ПДн о намерении осуществить обработку ПДн и не сообщили по запросу Роскомнадзора требующуюся информацию в срок, установленный законом.

ООО «Лор Клиника» и ООО «Южное коллекторское агентство» (по состоянию на июнь 2012 года), ФГУ санаторий «Юность» (по состоянию на ноябрь 2011 года) и ОАО «Гостиница «Москва» (по состоянию на декабрь 2010 года) без письменного согласия граждан на обработку биометрических персональных данных осуществляли изготовление и хранение копий страниц их паспортов при трудоустройстве или оказании услуг, обрабатывали избыточные персональные данные.

Ряд нарушений в хранении и обработке ПДн выявлены в июне-сентябре 2012 года в Закрытом акционерном обществе «Санаторий «Светлана»», ОАО «Вымпел-Коммуникации», ООО «Управляющая компания ЖЭУ №1», ТСЖ «Авиатор333», ФГУП «Почта России», ООО «Южное коллекторское агентство». В договорах ФГУ «Санаторий «Юность»» по состоянию на ноябрь 2011 года, по которым предоставляются ПДн для внешней обработки, не были установлены обязанности обработчика по соблюдению конфиденциальности и обеспечению безопасности персональных данных. На официальном сайте администрации города Сочи в 2010 году были опубликованы списки крупных должников по имущественным налогам, содержащие ПДн, без согласия на это самих граждан.

В рамках мероприятий по предотвращению указанных выше нарушений Краснодарский Центр научно-технической информации ФГБУ «РЭА» Минэнерго России для руководителей организаций, специалистов кадровых и юридических служб, лиц, ответственных за работу по обработке персональных данных в организации 6 мая 2013 года провел в г. Сочи семинар «Организация защиты персональных данных на предприятии в рамках реализации требований законодательства РФ».

Коммерческие услуги, способствующие выполнению требований и стандартов в области информационной безопасности, в городе Сочи предоставляют пользователям программного продукта «1С» компания «Первый БИТ» и ООО «Сан-Сити». Выполнение работ (оказание услуг) по созданию системы защиты персональных данных для Автономной некоммерческой организации «Организационный комитет XXII Олимпийских зимних игр и XI Паралимпийских зимних игр 2014 года в Сочи» поручило компании ЗАО «ЛЕТА».

Учитывая высокие темпы изменений технологической среды информационного взаимодействия, в рамках которого осуществляется передача, сбор, обработка и хранение ПДн, с целью повышения скорости достижения необходимого уровня безопасности ПДн, рационально внедрение в деятельность Операторов ИСПДн информационной системы поддержки принятия решений в аудите информационной безопасности.

Фаткиева Р.Р.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

МНОГОМАШТАБНЫЙ АНАЛИЗ СЕТЕВОГО ТРАФИКА

В настоящее время широкое применение нашли атаки типа «отказ в обслуживании» (Denial of Service) – DoS-атак. Цель таких атак – вывести ИС из строя и лишить пользователей возможности доступа к серверу. Грамотно организованная масштабная распределенная DDoS-атака в большинстве случаев приводит к значительным финансовым потерям со стороны жертвы. Такие нападения отличаются простотой организации и высокой эффективностью. Именно эти особенности привлекают к DDoS внимание как специалистов по сетевой безопасности, так и злоумышленников, и обусловливают актуальность исследования DDoS-атак. Построение эффективной системы защиты от атак DDoS является сложной задачей, система должна включать в себя: механизмы предупреждения атаки, обнаружения факта атаки, определения источника атаки и противодействия атаке.

Для решения задач обнаружения был использован статистический метод анализа, основанный на измерении выявленных в ходе исследования характеристик атакуемого сервера:

– объема входящего и исходящего трафика, в том числе и по различным протоколам;
– количества флагов в TCP-пакетах;
– уровня загрузки памяти и ЦПУ и т.д.

На основе этих характеристик было построено множество метрик системного и сетевого трафика. Построение было выполнено с таким расчётом, чтобы обеспечить чувствительность метрик к вредоносному трафику и инвариантность к легальному.

Разработанный в ходе исследования стенд моделирования атак позволяет оценить изменение метрик и выявить их пороговые значения. Выход значения метрики за пределы заданного для неё интервала служит признаком наличия атаки. Улучшение точности обнаружения атаки достигается также рассмотрением множества метрик в совокупности, что позволяет не только констатировать факт атаки, но и определить её тип по комбинации метрик, принимающих недопустимые значения.

Результаты проведённых исследований использованы для разработки программного продукта, в возможности которого входит детектирование атак на компьютерную систему в режиме реального времени. Программный продукт успешно прошёл тестирование для различных видов DDoS-атак.

С учётом следующих тенденций развития Интернет: внедрение шестой версии протокола IP, введение нелатинских символов, – технологии открытого потока задача детектирования атак приобретает еще большую актуальность. Поэтому для повышения точности и достоверности обнаружения атак возможно использование спектральных статистических методов (анализа сингулярного спектра и вейвлет-анализа), а также использование метописания атак для более точной структуризации и детектирования.

Федорченко Л.Н.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ОБ АСПЕКТАХ ОНТОЛОГИЧЕСКОГО АНАЛИЗА ДОКУМЕНТОВ В СТАНДАРТАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В информационных технологиях онтология характеризует то, что реально существует в предметной области: объекты (индивиды), их виды, свойства видов, взаимоотношения видов – и выражает это на языке экспертов предметной области. Таким образом, онтология, в частности, документирует язык предметной области.

В соответствии со стандартом IDEF5 (Integrated Definition for Ontology Description Capture Method) онтология (ontology) предметной области (domain) – это совокупность трех составляющих:

1) Лексика (lexicon) – толковый словарь предметной области (domain explanatory dictionary);

2) Набор ограничений (restrictions), в соответствии с которыми из терминов словаря строятся описательные утверждения (descriptive statements) о предметной области; например, в виде порождающей КС-грамматики в БНФ:

I5-ontology-sentence>::= <I5-ontology-decl> | <I5-ontology-context-decl> |<I5-ontology-viewpoint-decl> | <I5-ontology-purpose-decl> |<I5-ontology-project-decl> | <I5-ontology-analyst-decl> |<I5-ontology-reviewer-decl> | <I5-ontology-description-decl>.

<I5-ontology-decl> ::= (I5-ontology <I5-ontology-constant> | <indvar>).

<I5-ontology-context-decl> ::= (I5-ontology-context <I5-ontology-constant> | <indvar> string)

…..

3) Модель предметной области (model) – инструментальное средство, позволяющее по набору достоверных описательных утверждений (valid descriptive statements), описывающих некоторую известную ситуацию в предметной области, порождать (генерировать) соответствующие (appropriate) дополнительные (additional) утверждения, так называемые санкционированные (подтвержденные, одобренные экспертами) заключения (sanctioned inferences), представляющие собой новое знание о предметной области. Такой машиной порождения новых утверждений может быть экспертная система, система логического или грамматического вывода.

В рамках стандарта IDEF5, онтология стандартов информационной безопасности строится поэтапно. Весь процесс построения онтологии в стандарте (или любом другом текстовом документе) называется онтологическим анализом стандарта и выполняется последовательно, в два этапа:

1) построение полуформальной онтологии на языке схемы (IDEF5 schematic language);

2) построение формальной онтологии на языке уточнений (IDEF5 Elaboration Language) со строгим синтаксисом.

В представленном докладе синтаксис языка уточнений сформулирован в виде специальной грамматики в регулярной форме, учитывающей семантику концептов предметной области, для обработки которой применяется готовый программный инструмент. В качестве примера рассмотрен фрагмент задания политик безопасности организации как совокупность руководящих принципов, правил, процедур и практических приёмов в области безопасности, которые регулируют управление, защиту и распределение информации.

Филиппов А.Н., Стародубцев А.А.
Российская Федерация, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

МЕТОДЫ СОЗДАНИЯ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ В ПРИБОРОСТРОЕНИЕ

Применение интеллектуальных систем позволяет значительно увеличить скорость подготовки технологической документации, а так же уберегает от ошибок человеческого фактора, что позволяет не только существенно сэкономить ресурсы предприятия, выделяемые на процесс подготовки производства, но и уберечь предприятие от аварий и катастроф которые могут произойти вследствие ошибок совершённых человеком.

В силу вышеперечисленных факторов, актуальность применения интеллектуальных систем не оставляет сомнения, но как заставить компьютер думать подобно человеку?! Давайте рассмотрим существующие методы решения данной задачи и как следствие виды интеллектуальных систем, полученных в следствие применения данных методов.

Экспертные системы

Экспертные системы — это направление исследований в области искусственного интеллекта по созданию вычислительных систем, умеющих принимать решения, схожие с решениями экспертов в заданной предметной области. Примечательно то, что экспертные системы является одним из первых видов практически применимых интеллектуальных систем в силу своей узкой направленности. Подобно тому, как хороший эксперт компетентен только в своей проблемной области, экспертная система работает в чётко детерминированном пространстве, то есть способна решать только определённое количество специальных задач.

Многоагентные системы

В традиционном подходе решение задачи искусственного интеллекта сводится к написанию одной сложной интеллектуальной системы. Однако такой подход влечёт за собой ряд сложностей: проблематичность отладки и выявления слабых мест в системе, сложности в масштабировании и проведении распределенных вычислений, сложность в привлечении сторонних разработчиков. Для устранения вышеописанных проблем применяется многоагентная система. Суть данной системы в том, что для решения сложной задачи или проблемы используются системы, состоящие из множества взаимодействующих агентов. Каждый из агентов сам является интеллектуальной системой, решающей узкий круг задач, в то же время агенты активно взаимодействуют друг с другом, для решения общей глобальной задачи.

Генетические алгоритмы

Генетические алгоритмы (ГА) — это относительно новое направление в алгоритмике. Они способны не только решать и сокращать перебор в сложных задачах, но и легко адаптироваться к изменению проблемы.

Вначале ГА-функция генерирует определенное количество возможных решений, а затем вычисляет для каждого 'уровень выживаемости' (fitness) - близость к истине. Эти решения дают потомство. Те что 'сильнее', то есть больше подходят, имеет больший шанс к воспроизводству, а 'слабые' постепенно отмирают. Идет эволюция.

Существующие решения

На данный момент мы имеем множество небольших интеллектуальных систем, решающих частные задачи в предметных областях, в частности, приборостроение, однако эти системы имеют лишь некоторые признаки интеллекта, и решают на данный момент лишь малую долю интеллектуальных задач, более того, даже если они условно и считаются обучаемыми, обучение проходит как правило при помощи человека, с большими затратами временных ресурсов, в результате по прежнему основную часть интеллектуальных задач решают люди, что становится всё проблематичнее в условиях постоянного усложнения задач производства.

Чудиловская Т.Г.
Беларуссия, Минск, Академия МВД Республики Беларусь

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЛАЧНЫХ ТЕХНОЛОГИЙ

В настоящее время технологической инновацией, связанной с развитием информационных технологий и возможностей Интернета, являются облачные технологии (англ. cloud computing). Согласно документу, подготовленному специалистами Института инженеров по электротехнике и электронике IEEE, опубликованному в 2008 году, «облачная обработка данных – это парадигма, в рамках которой информация постоянно хранится на серверах в интернете и временно кэшируется на клиентской стороне, например, на персональных компьютерах, игровых приставках, ноутбуках, смартфонах и т. д.».

Характерными чертами облачных технологий как вида услуг, предоставляемых через Интернет, являются: выделение ресурсов пользователю в режиме самообслуживания (англ. on-demand self-service); широкополосный доступ к ресурсам из любой точки сети (англ. broad network access); организация ресурсов в пулы (англ. resource pooling), которые не зависят от местоположения самих ресурсов; быстрая адаптация к увеличению или уменьшению нагрузки (англ. rapid elasticity), а также измеряемый уровень сервиса (англ. measured service).

Мировой рынок облачных технологий растет быстрыми темпами. По подсчетам аналитиков Forrester Research к 2020 году объем мирового облачного рынка составит $241 млрд. против $40 млрд. в 2011 году.

Однако стремительные темпы развития облачных вычислений несут в себе потенциальную угрозу информационной безопасности. Проблемы защиты данных, операционной целостности, управления уязвимостью, непрерывности деятельности, восстановления работоспособности после аварий, управления идентичностью, обеспечения конфиденциальности информации являются наиболее актуальными аспектами облачных вычислений. Среди наиболее характерных угроз для облачной архитектуры специалисты выделяют: DDoS-атаки на сетевую инфраструктуру со стороны облака, попытки перехвата аутентификационных данных, перехват непосредственно данных, недостаточная очистка клиентской информации со стороны провайдера облачных технологий.

По причине разнородности облачных сред обеспечение облачной защищенности – задача чрезвычайно сложная. Проблема организации защищенной среды облачных сервисов обусловлена отсутствием принятого большей частью рынка стандарта обеспечения безопасности облачных вычислений. Несмотря на существование разных сертификационных процедур, базирующихся на критериях и требованиях безопасности, единого подхода и методики для обеспечения защищенности облачных вычислений пока нет, нет и единой методики проверки адекватности защиты провайдера подобных сервисов.

Эффективное обеспечение безопасности облачных сервисов возможно при соблюдении баланса между мерами обеспечения информационной безопасности, ответственность за которые несет поставщик услуг, и средствами защиты, применяемыми клиентом.

В набор средств защиты, обеспечивающих безопасность пользователя при использовании облачных сервисов, входят:

- безопасная регистрация получателя услуги в «облаке»;
- аутентификация получателя услуги в «облаке»;
- электронная подпись данных;
- защита обмена информацией между получателем услуги и «облаком»;
- защита от атак, связанных с подменой «облака» (фишинг и т. п.);
- обеспечение доверенной среды (операционная система, в которой работает клиент, должна быть свободной от вирусов, программ-шпионов и иного вредоносного программного обеспечения).

Щиголева М.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им.В.И.Ульянова (Ленина)

ОПРЕДЕЛЕНИЕ УРОВНЯ РАЗРЕШЕННЫХ ПОТЕРЬ СЕМАНТИЧЕСКОЙ БИОФИЗИЧЕСКОЙ МОДЕЛИ С СОХРАНЕНИЕМ КАЧЕСТВА ДОСТАТОЧНОСТИ ЦЕЛЕВОЙ УСТАНОВКЕ ПОСТРОЕНИЯ МОДЕЛИ

В системе биореагирования на целевое управляющее воздействие основной характеристикой биосуществования является наличие результирующего отклика: система восприняла – среагировала – откликнулась. Если воздействие оказывается с определенной целью, то характеристикой реакции биообъекта будет достижение планируемого результата. Тогда можно обозначить три области, вносящие свой вклад в достижение цели: воздействия, реагирования, реакции. В этой триаде существует степень вклада каждой составляющей в пределах допустимых диапазонов: присущих или устанавливаемых. Приоритетным правилом обращения к центральной части триады – биосистеме, является недопустимость разрушения её существования, т.е. реакция может быть от свободного пропускания воздействия до напряженного разной степени, но не разрушающего ее биосуществование. К системе требуется подобрать воздействие такого уровня, чтобы реакция достигла поставленной цели из перечня целей, которые лежат в границах решаемых биосистемой задач. Реакция системы включает зоны реагирования, способные формировать отклик на поступившее воздействие, и из разрешенных зон формирует конфигурацию, пригодную для достижения цели. Порядок объединения зон в предпочтительную конфигурацию осуществляется по правилам притяжения сосуществующих аттрактов, исходя из исследуемого состояния системы: обязательная связность, ситуационная, специфичная, исключаемая.

Первоначальная постановка задачи состояла в поиске, исследовании и оценке многозонного объединения конфигураций, способных обеспечить достижение цели, и выборе из них наиболее предпочтительной. При этом конфигурирование производилось по всей области существования биосистемы, что свидетельствует об обязательной связности элементов биообъекта и расширении возможностей биовыбора тракта проведения управляющего воздействия. Вместе с тем большой интерес представляет и отсекаемая часть модели биосистемы. Аналогией является скульптурный подход отсекания от глыбы породы всего лишнего. В целостной биосистеме по целевому управляющему воздействию формируется необходимая для этой цели многозонная конфигурация – вырезаемая часть биосистемы, и оставшаяся часть – разрешенные потери системы, которая из целостного описания и рассмотрения не выпала, но осталась незадействованной при построении тракта прохождения управляющего сигнала. По мере накопления конфигураций типичных топологий многозонной связности, дополнений специфичными топологиями, сосуществующими притяжениями аттрактов, остается остаточная структура, из которой можно исключить зоны возможного реагирования в качестве физиологических резервов и специфичных предпочтений. Помимо понижения размерности исследуемой модели происходит отсекание ложно срабатываемой периферии, вносящей искажение и инерционность в проводимость управляющего сигнала. Таким образом, отсеченная структура сортируется на исключаемую и резервную, избыточно поглощающую входной сигнал, но, в случае инвертирования, имеющую специфичную притягательность. В этом случае, подключение выявленного резерва в качестве дополняющих зон, может иметь эффект катализации и подлежит обязательной регистрации. Подход к выявлению уровня разрешенных потерь семантической модели позволил сократить модель до рабочей части модели, выявить потенциально возможные дополнительные резервы, конкретизировать механизмы персонификации теоретической модели и наметить контуры тренируемого отсекания тех зон потерь, которые поглощают прохождение входного управляющего воздействия.

Ярошевич Л.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет кино и телевидения

ПАУЗЫ В ИЗОБРАЗИТЕЛЬНЫХ СИСТЕМАХ

Информационные системы не могут быть построены хаотично, если это не запланировано по содержанию. Порядок построения изображений должен соответствовать законам аудио-визуального восприятия и отражения информации. Композиционная динамика отдельных фаз изобразительной системы предполагает наличие связеобразующих величин между фразами. Пауза в системе изложения информации является неотъемлемой структурной составляющей частью, что связано с особенностями дыхания и визуального восприятия человека.

Изобразительные приёмы идентичны в своей функциональной значимости, поэтому системы построения изображений имеют сходные принципы внутренней организации. Паузы - обязательные составляющие изобразительных систем. На первый взгляд это – остановки. Будем рассуждать так: человек осуществляет свою деятельность в условиях движения пространства и времени. Какой бы вид (объект) не находился в поле зрения человека, всегда, речь идёт ещё и о пространстве на фоне

которого представлен объект. Это либо - естественное пространство, либо – фон, плоскость, имитирующая пространство, либо – пространственные интервалы в текстах и т.д. Паузы разделяют информацию на отдельные части и, одновременно, соединяют их в иерархическую структуру. В изображениях паузы имеют своё начало, протяжённость и завершение. Это движущиеся величины со свойствами пространства и времени. Пространственные паузы существуют внутри и вне градостроительных комплексов. А также, искусство скульптуры имеет целый арсенал средств для моделирования перспективы пространственных глубин. "Круглая" скульптура является композиционным центром изобразительного пространства, далее используется горельеф (более половины величины объёма, выступающего над плоскостью), следующий пространственный уровень выстраивается с помощью барельефа (менее чем на половину объёма над плоскостью). Глубокий пространственный уровень моделируется обычным мелким рельефом. Кроме того, существует контррельеф. Всё вместе образует т.н. картинный принцип построения пространства. Паузы между видами скульптуры могут быть как реальным пространством, так и фоном, плоскостным или несущим на себе косвенную информацию 2-го, 3-го, …., и последнего планов. Пауза может быть завершающей стадией процесса внимания, либо промежуточной (более короткой) в процессах переключения внимания с одного объекта на другой, либо при рассматривании частей целого изображения. Другой пример, архитектурный стилевой дизайн служит для оформления "пространственной динамики" фасадов, здесь также работает принцип картинной плоскости, построения перспективы глубинного пространства. В барокко, например у Б.Ф.Растрелли, изобразительная динамика скульптурного декора соответствует высоким скоростям атмосферного движения, психологическому состоянию веселья и радости. Цвет фасадов преимущественно пространственный небесный голубой.

В классицизме больше порядка и покоя, снижение "пространственных скоростей". На фасадах солнечная "согревающая" теплая охра, более спокойный и торжественный декор, совсем другие темпы и ритмы, хотя принципы построения картинного пространства остаются: композиционный центр – портик, далее скульптурный декор выстроен по планам.

В модерне, например у Ф.И.Лидваля, на фасадах зданий объём крупных средств декора почти не используется, вместо колонн всё чаще, чем в классицизме применяются пилястры, легкий рельеф и контррельеф. Вероятно, суть заключается в том, что здания в тот период времени возрастают в объёме и требовались средства декора, предназначенные для обозначения ещё более глубокой иллюзорной перспективы в тесном городском пространстве. Происходит преимущественное моделирование последних планов "плоскости картины" фасада, при этом остаётся место для небольшого композиционного центра, уровни пространственных планов сохраняются.

С помощью пауз в изобразительных системах обеспечиваются адаптация и комфорт аудиовизуального восприятия приближённых и удалённых планов иллюзорного пространства. В.И.Вернадский в своих научных трудах призывал человечество строить пространство ноосферы по принципам и подобию биосферы, в основе которых лежит закон сохранения энергии.

СОВРЕМЕННЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Абрамов М.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ЗАЩИТА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ НА ИНТЕРНЕТ-ПОРТАЛЕ РЕДАКЦИИ ЭЛЕКТРОННОГО НАУЧНОГО ЖУРНАЛА

При создании интернет-портала редакции электронного научного издания разработчиками огромное внимание уделялось проблемам информационной безопасности конфиденциальных данных, хранящихся на наших серверах. Пренебрежение этим аспектом при разработке программного комплекса недопустимо и может привести к серьёзным последствиям. На портале предусмотрен функционал для заполнения, корректирования данных по статьям без их отправки в редакцию. В случае, если злоумышленник получит доступ к базе данных, в которой фиксируются все выше перечисленные изменения, он получит возможность присвоить результаты чужой научной деятельности себе. Также он может получить доступ к базе телефонных номеров и прочих контактов зарегистрированных пользователей и совершить иные действия.

При регистрации на портале пользователь проходит процедуру внесения личных данных, включающую в себя также заполнение поля символами на картинке – «капчи», что позволяет избежать регистрации так называемых «ботов». Завершает этот этап активности пользователя на портале проверка корректности введённого адреса электронной почты путём направления на него письма с просьбой перейти по ссылке для подтверждения регистрации. Стоит заметить, что на каждой форме внесения данных личной карточки действуют интерактивные онлайн подсказки, совмещённые с проверкой вводимой информации. Существенная часть сил была сосредоточена на предотвращении SQL-инъекции. Пароли, задаваемые пользователями при регистрации, либо во время редактирования личных данных проходят проверку на сложность и трудоёмкость их генерации путём подбора. Если они удовлетворяют заявленным требованиям, то подвергаются двойному хешированию и закрепляются за данной учётной записью. Для того чтобы произвести расшифровку такого пароля при имеющихся на данном этапе мирового развития ресурсов потребуется более года времени, но система настоятельно просит пользователя менять пароль каждые 6 месяцев. Программным комплексом также отслеживается и блокируется несвойственная человеку активность, например, система блокирует попытки осуществить единовременную загрузку более фиксированного количества страниц.

Аранов В.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

ЗАЩИТА ИСПОЛНЯЕМОГО МАШИННОГО КОДА ОТ ОБРАТНОГО ПРОЕКТИРОВАНИЯ ПРИ ПОМОЩИ МНОГОУРОВНЕВОЙ ВИРТУАЛИЗАЦИИ

В настоящее время реальное положение дел в области защиты программного обеспечения (ПО) таково, что, государство не может решить проблему защиты производителей ПО от создания нелицензионных копий правовым путем, и наиболее эффективными являются программные и аппаратные методы защиты. Не смотря, на постоянное изменение законодательной базы, защита программного кода, как от нелицензионного копирования, так и от банальной кражи наукоемких алгоритмов, является актуальной задачей.

Существует три основных подхода к защите ПО, которые не допускают запуск нелицензионной копии на неавторизованном оборудовании: использование программно-аппаратных комплексов с целью создания доверенной вычислительной среды, создание стойких криптоконтейнеров, распаковка которых зависит от отпечатка оборудования, на котором запущен криптоконтейнер, и обфускация кода с целью затруднения поиска и устранения механизмов защиты.

К сожалению, только первый из этих способов является абсолютно надежным. Однако, не всегда создание доверенной вычислительной среды является возможным, и, в таком случае, приходится пользоваться методами обфускации, ибо второй метод также является неустойчивым в том случае, если злоумышленником оказывается легальный покупатель ПО.

Таким образом обфускация является ведущим методом обеспечения взломоустойчивости ПО в случае невозможности создания доверенной вычислительной среды. Существует множество методов обфускации, однако, большинство из них характеризуется неустойчивостью против современных

методов анализа и отладки кода, что порождает задачу разработки новых способов обфускации с невозможностью автоматического или полуавтоматического исходного алгоритма. Методы защиты при помощи виртуальных машин выгодно выделяются среди остальных методов тем, что не существует эффективных публичных методов анализа кода, защищенного с использованием технологий виртуализациии исполняемого кода.

Очевидно, эффективным решением является многократное применение виртуализации исполняемого кода, что, однако, влечет за собой целый ряд трудностей таких как:

– существенное замедление выполнения защищенного кода;

– значительное снижение трудоемкости снятия повторных уровней виртуализации при известной структуре виртуальной машины;

– простое детектирование кода виртуальной машины и связанных с ним структур данных.

Для преодоления вышеуказанных недостатков и эффективной защиты исполняемого машинного кода предлагается использовать генератор существенно различных вложенных виртуальных машин, обладающих целым рядом различающихся признаков:

– Использованием различных систем команд отличающихся друг от друга по:
  - семантике команд;
  - кодировке инструкций;
  - методам адресации;
  - способам вызова подпрограмм;
  - типам регистров виртуального ЦП;
  - размеру регистров виртуального ЦП.

– Использованием существенно различного байт-кода за счет создания компилятора для каждой виртуальной машины непосредственно в процессе защиты конкретного экземпляра ПО.

– Защитой интерпретатора виртуальной машины стандартными методами обфускации и антиотладки, однако, примененными с разными настройками, такими как:
  - создание шитого кода интерпретатора;
  - использование самомодифицирующегося кода интерпретатора;
  - вставка мусорного и зеркального кода с целью затруднения работы анализаторов типа IDA и HEX-RAYS;
  - вставка команд, препятствующих отладке на реальном процессоре;
  - вставка элементов для определения эмулирующих отладчиков типа Bosch.

Проблема замедления исполнения защищаемого ПО адресуется использованием профилирования и полуавтоматическим выбором защищаемых частей ПО.

Только грамотное и совместное использование систем обфускации и методов классической криптографии способно существенно замедлить появление взломанных версий ПО в сети Интернет или даже сделать взлом ПО коммерчески невыгодным, делая стоимость взлома ПО в несколько раз, а то и на несколько порядков выше стоимости лицензионной копии.

Алексеев А.В., Марченко А.В., Удодова Е.Н., Горбачев Р.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

ПРАКТИКА ФОРМИРОВАНИЯ КОГНИТИВНЫХ БАЗ ДАННЫХ И ЗНАНИЙ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЭКСПЛУАТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ И ОЦЕНКИ КОНКУРЕНТНОЙ СПОСОБНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Среди проблемных вопросов в области автоматизации процессов защиты информации и обеспечения безопасности эксплуатации объектов информатизации одно из ключевых мест занимает проблема формирования баз данных и знаний (БДЗ) для проведения квалиметрического анализа и ранжирования технологических решений по обеспечению конкурентной способности автоматизированных систем в защищенном исполнении.

Создание подобных БДЗ, включая комплексную оценку уровня информационной эффективности комплексов автоматизации в защищенном исполнении, конфиденциальности, доступности и целостности обрабатываемой информации, а также уровня компетенций персонала и эффективности эксплуатации объекта информатизации приобретает качественно новый уровень. Более того, это позволяет практически перейти к сравнительному анализу конкурентноспособности разрабатываемых средств и систем обработки информации в защищенном исполнении.

Однако, в готовом для использования виде подобных БДЗ, входящих в состав, например, систем типа SmartEvent сегодня нет и не предвидится, а их создание методически и организационно представляется весьма трудоемким. Кроме того, при этом требуют особого внимания наряду с вопросами формирования подобных БДЗ вопросы их непрерывной актуализации, учета соответствующих корпоративных и ведомственных разграничений и многие другие.

В ходе проведенных в Санкт-Петербургском государственном морском техническом университете специальных научных исследований к настоящему времени сформирована концепция и

создан базовый вариант так называемой когнитивной «БДЗ-БЖ 3.0» в составе специализированного программного комплекса. Она позволяет создавать, систематизировать и обрабатывать новые знания применительно к системам информационной поддержки принятия решений обеспечении безопасности эксплуатации, локализации аварийных ситуаций и инцидентов объектов информатизации повышенного риска.

Созданная «БДЗ-БЖ_3.0» включает сегодня более 210 технологических решений, в том числе на основе отечественных и международных патентов, изобретений и полезных моделей. Выполняемый анализ вошедших в БДЗ решений позволяет выявить наиболее «сильные» из них, лучшие практики по информационной поддержке принятия решений при обеспечении безопасности эксплуатации. В том числе - определять решения среди прошедших квалиметрическое ранжирование достигнутый уровень технологического развития (совершенства).

При актуализации и расширении состава технологических решений в БДЗ, предусмотренное дальнейшими исследованиями, планируется дать обоснованный ответ на вопрос о конкретных «представителях» ведомственного, национального и даже мирового уровня технологического развития, а также их конкурентной способности в рассматриваемой предметной области. В том числе при обосновании проектных решений по организации и технологии защиты информации – в соответствии с данными из Государственного реестра сертифицированных средств защиты информации (http://fstec.ru/sistema-sertifikatsii-tzi/). При разнообразии функциональных задач порядка 30 в его составе сегодня уже более 2900 альтернативных вариантов проектного выбора.

В интересах повышения достоверности формируемых данных и знаний на основе концепции полимодельного анализа и синтеза при формировании «БДЗ-БЖ_3.0» успешно использованы программные комплексы ASPID-3W, APIS (технология анализа и синтеза при информационном дефиците профессора Хованова Н.В.), MPRIORIRY 1.0 (технология по методу анализа иерархий Т.Саати), OPTIMUM 1.0, OPT-PROx 1.0, T-CHOICE 1.0 (технология глобальной оптимизации решений Абакарова А.Ш., Сушкова Ю.А.), а также специализированные для сравнительного анализа средств и систем защиты информации программные комплексы КРОПУР (технология квалиметрической ранговой оптимизации проектных и управленческих решений, свид. о гос. рег. №2013612649 от 11.03.2013, СПбГМТУ) и АСОР (технология анализа, синтеза и оптимизации решений).

Использования разработанной БДЗ уже сегодня обеспечивает: выявление перспективных направлений совершенствования сложных организационно-технических систем в защищенном исполнении; проведение сравнительных экспертиз с квалиметрическим ранжированием планируемых и реализованных технологических решений; ранговую сертификацию технических заданий, практических алгоритмов обработки информации с оценкой валидности, новизны национального и мирового уровня (в сопоставлении с конкретными аналогами из состава БДЗ на конкретный момент времени) и других документов; выявление и мониторинг лучших практик; содействие выполнению работ в области автоматизации процессов обеспечения безопасности эксплуатации, локализации аварий и борьбы за живучесть судов повышенного риска и других объектов информатизации.

Алексеев А.В., Потехин В.С.
Россия, Санкт-Петербург, Институт автоматизации процессов борьбы за живучесть корабля, судна, НИИ (оперативно-стратегических исследований строительства ВМФ) ВУНЦ ВМФ «Военно-морская академия»

ТЕХНОЛОГИЯ И ПРАКТИКА ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ И ИНТЕЛЛЕКТУАЛЬНОЙ ПОДДЕРЖКИ ЛИЦ, ОБОСНОВЫВАЮЩИХ И ПРИНИМАЮЩИХ РЕШЕНИЯ, КАК СРЕДСТВО ЗАЩИТЫ ОТ ВНУТРЕННИХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Среди современных проблем обеспечения информационной безопасности (ИБ) сложных организационно-технических комплексов и систем (ОТС) особое место занимает комплекс вопросов и проблем, связанных с защитой от такой внутренней угрозы ИБ, как пресловутый «человеческий фактор» (ЧФ). Он может быть обусловлен, как ошибками эксплуатации (обслуживания) технических средств (ТС), неквалифицированностью персонала, несовершенством технологических решений, так и неадекватностью мотивации его действий, например, администратора сети, разного рода хакеров.

Особенно критичным является воздействие этого субъективного внутреннего фактора ИБ при обеспечении безопасности эксплуатации (ОБЭ), локализации аварийных ситуаций (АС) и аварий (ЛА), а также борьбы за живучесть корабля, судна (БЖКС). На объектах повышенного риска (атомные суда, танкеры, газовозы, химовозы, морские платформы и др.) нейтрализация негативного воздействия ЧФ представляет собой исключительно сложную системную, научно-методологическую, организационно-техническую и технологическую проблему. Возникающие при этом риски подчас во много раз превосходят ресурсные затраты на создание и эксплуатацию самих объектов информатизации.

Одним из магистральных путей решения проблемы ЧФ признано считать создание совершенных систем информационной, информационно-аналитической и интеллектуальной

поддержки (СИП) лиц, обосновывающих (ЛОР) и принимающих (ЛПР) ответственные проектные (проекты решений) и управленческие решения (ПУР), а также лиц, исполняющих эти решения (ЛИР).

Следует отметить, что природа проявления ЧФ имеет сходные черты практически для всех ОТС, режимов ОБЭ, ЛА и БЖКС и обусловлена спецификой взаимодействия «ЭВМ-ЛПР (ЛОР, ЛИР)», а создание совершенных СИП продолжает оставаться одной из злободневных задач.

В контексте решения именно задач ИБ в различных вариантах создаваемых СИП по-прежнему требуют уточнения неоднозначно решаемые вопросы минимизации их структурной и информационной сложности (избыточности), системной оптимизации, технологии визуализации и автоматизации задач интеллектуальной обработки многочисленных и разнородных данных.

Результаты анализа теории, технологий и практики создания СИП показывают, что новое качество обеспечения ИБ следует ожидать при переходе к концепции бинарной визуализации и оценки обстановки при ОБЭ, ЛА и БЖКС. По частным показателям качества (ЧПК) – для ЛОР и ЛИР, а для ЛПР – по групповым (ГПК) и сводному показателю качества (СПК). В сочетании с переходом от непрерывного мониторинга обстановки (по ЧПК, ГПК и СПК) к дискретному анализу и оценке обстановки с 4-х уровневым квантованием показателей ИБ (включая верификацию действий ЛПР, ЛОР и ЛИР), ОБЭ, ЛА и БЖКС. Например, по схеме: «зеленый» уровень - безопасное состояние, «желтый» – угроза аварийной ситуации, «красный» - аварийная ситуация, «черный» - чрезвычайная ситуация.

Наряду с существенным сокращением информационной избыточности, реализация данной концепции позволяет перейти ЛПР, ЛОР и ЛИР к анализу обстановки на уровне распознавания образов, что создает существенно более «комфортную» психо-физиологическую обстановку при принятии решений, классификации данных и обстановки, их идентификации и хранении. Вместе с тем, переход к анализу от ЧПК к ГПК и СПК, наоборот, повышает ценность информационных потоков, оперативность и достоверность данных, т.е. повышает информационную эффективность (>80%) каналов и системы контроля состояния ТС и устойчивость системы управления процессами ОБЭ, ЛА, БЖКС в целом.

Наконец, качественно новый (когнитивный) характер приобретают процедуры формирования баз данных и знаний (БДЗ) СИП. В силу «информационной прозрачности» и большей дружественности интерфейса алгоритмов ОБЭ, ЛА и БЖКС при актуализации БДЗ появляется возможность привлекать самих ЛПР, ЛОР и ЛИР, а не только проектировщиков, как это принято сегодня.

С другой стороны, квантование оценок ИБ, ОБЭ, ЛА и БЖКС минимизирует число циклов принятия ПУР, снижает неопределенность данных и «напряженность» при их принятии.

К числу первоочередных задач развития представляемой и уже апробированной технологии СИП относятся: формирование единых БДЗ с соответствующими квалиметрическими сравнительными оценками на множестве типовых и уникальных сценариев развития обстановки; экспериментальная отработка и освоение эффективных алгоритмов бинарной визуализации многомерных данных и их визуальной обработки; оптимизация алгоритмов действий ЛОР, ЛПР и ЛИР в учебно-тренировочном режиме на основе методов ситуационного моделирования и полимодельного квалиметрического ранжирования; ранговая сертификация альтернативных технологий и алгоритмов СИП.

Данное направление и технология СИП развивается в рамках проводимых НИОКР, в том числе по ФЦП, были обсуждены и одобрены на Первой научно-практической конференции «АПБЖ-2012».

Андрущенко Д.М.
Украина, Запорожье, Запорожский национальный технический университет

МЕТОД ЗАЩИТЫ АВТОРСКОГО ПРАВА НА ЦИФРОВЫЕ ИЗОБРАЖЕНИЯ

Цифровые изображения, как продукт творческой деятельности специалистов, часто создаются в коммерческих целях. Поэтому несанкционированное использование изображений зачастую несет убытки его правообладателю.

Закон «Об авторском праве и смежных правах» гласит, что авторское право на произведение возникает в результате факта его создания. Для возникновения и осуществления авторского права не требуется регистрация авторского произведения. Но вследствие возникновения споров может понадобиться подтверждение факта создания фотографического произведения настоящим автором в судебном порядке или подтверждения факта заключения лицензионного договора. Поэтому в настоящее время используют способы защиты авторских произведений от несанкционированного распространения, а также способы, которые позволяют авторам произведений выявлять правонарушителей в случае появлений контрафактных копий.

Существуют способы, предназначенные для создания технологических препятствий нарушению авторских и смежных прав на цифровые изображения, которые основанные на том, что

устройство, на котором воспроизводится цифровой объект, получает информацию о наличии прав у издателя и принимает решение о разрешении доступа к информации пользователю. Однако, к сожалению, они не позволяют предотвратить возможность недобросовестным пользователям, которые получили разрешение на доступ к информации, сделать контрафактную копию цифрового объекта. А если количество пользователей достаточно велико, правообладатель не сможет обнаружить правонарушителя.

Другие способы защиты авторских прав изображений основаны на встраивании цифровых водяных знаков (ЦВЗ) путем изменения частотных коэффициентов в пределах матрицы преобразования. Тогда в случае правонарушения, наличие ЦВЗ в изображении подтверждает права автора. Однако такие способы не предусматривают возможности определения правонарушителя авторских прав при выявлении факта появления контрафактной копии.

В предлагаемом методе, ЦВЗ создается из электронных цифровых подписей сторон, участвующих в процессе передачи авторского права. При передаче имущественного права на объект авторского права составляется лицензионное соглашение, которое подписывается электронными цифровыми подписями разных сторон. Таким образом, они подтверждают согласие друг с другом. После того доверенное лицо или аппаратное устройство встраивает цифровой водяной знак в оригинал изображения, состоящий из этих электронных цифровых подписей таким образом, что биты ЦВЗ состоят поочередно с бит электронных цифровых подписей. При этом каждая из цифровых подписей формирует отдельную часть ЦВЗ. Для сокрытия данных используют частотную область контейнера. Изображение разбивается на блоки размерностью 8 × 8 пикселей и к каждому блоку применяется двумерное дискретное косинусное преобразование (ДКП). Каждый блок пригоден для записи одного бита информации. Перед встраиванием ЦВЗ произвольным образом выбирается столько блоков ДКП, сколько битов в ЦВЗ.

Далее для встраивания каждого бита данных принимают очередной блок ДКП, входящий в выбранную группу блоков. Выбирается N произвольных коэффициентов ДКП с полосы средних и низких частот. Также выбирается две фиксированные величины P1 и P2. Для передачи бита «0» выбранные коэффициенты меняются так, чтобы среднее арифметическое этих коэффициентов стало не ниже величины P1. А для передачи бита «1» меняются так, чтобы их среднее арифметическое стало не выше, чем P2. После этого проводится обратное ДКП. Для выбора оптимальных значений P1 и P2, вычисляют математическое ожидание значений коэффициентов с выбранными координатами на основе произвольной выборки некоторого количества блоков ДКП (не менее 1000 блоков). Порог встраивания влияет на устойчивость стеганосистемы, а именно чем больше P1 и меньше P2, тем больше устойчивость стеганосистемы к искажениям контейнера, но тем больше ухудшается качество изображений при встраивании информации. Для извлечения бита данных формируется ключ, который состоит из номеров блоков ДКП и координат выбранных коэффициентов.

При извлечении битов цифрового водяного знака из известных блоков ДКП и известных коэффициентов с выбранными координатами (записанными в ключе), если среднее арифметическое значение коэффициентов больше P1, то извлекается значение 0, а если меньше P2, то извлекается значение 1.

Использование предложенного метода позволяет снизить риски несанкционированного распространения цифровых изображений, а в случае если это произошло, позволяет правообладателю выявить правонарушителя и защитить свое право в судебном или административном порядке.

Березин А.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ПОДХОДЫ К ПОСТРОЕНИЮ КРИПТОСХЕМ НА ОСНОВЕ ЗАДАЧ ФАКТОРИЗАЦИИ И ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ

Для обеспечения информационной безопасности широко используются криптографические схемы с открытым ключом, лежащие в основе криптографических протоколов. Безопасность таких криптосхем основывается на следующих двух фактах: 1) решение используемой трудной задачи является вычислительно нереализуемой за приемлемое время при использовании наилучшего алгоритма, то есть задача обладает достаточно высокой стойкостью; 2) вероятность появления вычислительно эффективного алгоритма в ближайшем будущем для решения используемой вычислительно трудной задачи пренебрежимо мала. Это означает, что количественная характеристика безопасности криптосхем включает два количественных параметра – стойкость и вероятность появления эффективного алгоритма решения. Повышения уровня безопасность криптосхемы может быть достигнуто путём синтеза новых криптосхем на основе нескольких трудных задач. Таким образом, для взлома криптосхемы потребуется появление сразу двух вычислительно эффективных алгоритмов решения двух различных трудных задач.

Наиболее широкое распространение при построении различных типов криптосхем получили задачи факторизации (ЗФ) и дискретного логарифмирования (ЗДЛ). Они также используются для построения криптосхем, взлом которых требует одновременного решения двух трудных задач.

В настоящем сообщении рассматривается подходы для построения криптосхем, взлом которых требует одновременного решения двух трудных задач, на основе ЗФ и ЗДЛ.

Наиболее очевидным подходом является комбинирование двух различных криптосхем. Например, формирование двух электронных цифровых подписей (ЭЦП) к одному документу, шифрование сообщения последовательным выполнением двух различных алгоритмов. Очевидно, что данный подход имеет существенные недостатки в виде дополнительных временных затрат на проведение вычислений, большого размера ЭЦП и необходимость хранения нескольких секретных ключей.

Второй подход, основан на внесении изменений с существующие криптосхемы, например, ЭЦП Эль-Гамаля, ЭЦП Шнорра, ГОСТ Р 34.10-94. В них используется ЗДЛ по простому модулю. Подход основан на возведении в некоторую степень параметра S в этих криптосхемах и наложении дополнительных требований на модуль. Вместо простого модуля используется модуль, функция Эйлера от которого содержит составное число трудное для факторизации, из-за этого для вычисления корня потребуется решить ЗФ этого числа. Благодаря возведению в некоторую степень параметра S достигается необходимость одновременного решения ЗФ и ЗДЛ. На основе данного подхода было предложено достаточно большое количество схем ЭЦП. Однако данный метод построения даёт довольно низкую производительность, по сравнению с базовыми криптосхемами, большой размер ЭЦП, который зависит от размера используемого модуля, и не всегда есть возможность её сокращения. Не очевидно как использовать данный подход для построения криптосхем других типов.

Третий, наиболее перспективный, подход основан на том, что за исключением переборных алгоритмов, для решения ЗДЛ по составному модулю, потребуется знать факторизацию составного модуля и уметь решать ЗДЛ для каждого простого делителя составного модуля. Благодаря этому для взлома криптосхемы потребуется одновременное решение ЗДЛ по простому модулю и ЗФ составного модуля. С использованием данного подхода возможно построение криптосхем, обладающих одинаковой стойкостью ЗФ и ЗДЛ, что позволяет гарантировать некоторую общую стойкость криптосхемы на одном уровне (т.е. стойкость такой криптосхемы не изменится в случае открытия прорывного алгоритма для решения одной из рассматриваемых задач.). Это достигается путём использования в качестве модуля произведения двух сильных простых чисел с соотношением размеров два к одному. Данный подход является интересным и достаточно универсальным для построения криптосхем различных типов, основанных на трудности одновременного решения ЗФ и ЗДЛ. При его применении к существующим криптосхемам потребуется минимальная их модификация, при этом производительность понизится незначительно. В случае построения схем ЭЦП, возможно достижение 80 битовой стойкости при размере подписи в 320 и даже 240 бит, что существенно меньше размеров для известных схем ЭЦП.

Березин А.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ВАРИАНТЫ ЗАДАЧИ ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ ПО СОСТАВНОМУ МОДУЛЮ

Трудность задачи дискретного логарифмирования (ЗДЛ) широко используется для построения криптосхем с открытым ключом: шифрования с открытым ключом, схем обмена ключами, электронной цифровой подписи (ЭЦП) и т.д. Эта задача определяется над конечными циклическими группами, например над мультипликативной группой колец классов вычетов по модулю (в большинстве случаев модуль равно 1024-битовому простому числу).

В настоящем сообщении рассматривается вопрос построения ЗДЛ с использованием составного модуля равного произведению двух сильных простых чисел большого размера. ЗДЛ по составному модулю состоит в нахождении степени числа по составному модулю, при известном основании, модуле и результате возведения в степень.

Отметим что, за исключением переборных алгоритмов, решение ЗДЛ по составному модулю выполняется путем факторизации составного модуля и нахождения дискретного логарифма по модулю каждого простого делителя этого модуля. Поэтому, если трудность факторизации составного модуля достаточна высока и примерно равна сложности нахождения дискретного логарифма по модулю наибольшего простого делителя этого модуля, при использовании лучших известных алгоритмов для решения этих задач, то решение ЗДЛ по составному модулю, потребует одновременного решения двух трудных задач: ЗФ и ЗДЛ, вычислительная сложность которых имеет одинаковый порядок.

Сложность факторизации составного модуля, определяется размером меньшего простого множителя. Сложность решения ЗДЛ по модулю простых множителей составного модуля примерно равна сложности ЗФ составного модуля, если простые множители составного модуля подобраны с соотношением размеров 2:1. Тогда, сложность решения ЗДЛ по составному модулю, сложность решения ЗДЛ по модулю простых множителей составного модуля, и сложность решения ЗФ составного модуля являются значениями одного порядка.

Однако значение основания должно быть выбрано правильно, для того чтобы предотвратить использование специальных методов факторизации. Возможны следующие два варианта выбора основания.

Генерируются два простых числа, такие что, функция Эйлера от них содержит достаточно большой (160 бит и более) простой делитель. Число, имеющее порядок равный этому простому делителю по составному модулю, выбирается в качестве основания. В этом случае значение порядка основания будет несекретным.

Генерируются два простых числа, такие что, функция Эйлера от первого содержит достаточно большой простой делитель, который не содержится в функции Эйлера от второго, а функция Эйлера от второго содержит достаточно большой простой делитель, который не содержится в функции Эйлера от первого. Число, имеющее порядок равный произведению этих делителей по составному модулю, выбирается в качестве основания. В этом случае значения двух делителей и их произведения являются секретными. Решение ЗДЛ по составному модулю, позволит вычислить произведение делителей, однако нахождение его делителей является ЗФ. Таким образом, для факторизации составного модуля после решения ЗДЛ снова требуется решить ЗФ, но уже по отношению к произведению делителей меньшего размера. Однако выбранные размеры делителей таковы, что разложить его на множители является практически невыполнимой задачей при использовании лучшего известного алгоритма факторизации. Требуется выбирать простые делители функции Эйлера с учётом, что второй множитель является достаточно большим четным числом, это связано с тем, чтобы сделать практически невыполнимым нахождение значения функции Эйлера путем подбора возможных значений вторых множителей при известном значении произведении делителей.

Фактически, вариант ЗДЛ по составному модулю, является частным случаем ЗДЛ по двумерному основанию и формулируется следующим образом. Для двух оснований, имеющих порядок, равный значению обобщенной функции Эйлера, по составному модулю. При этом важно, что бы основания относились к разным циклическим подгруппам мультипликативной группы кольца вычетов по составному модулю. Для произвольного результата произведения по составному модулю оснований, возведенных в различные степени, требуется найти эти степени.

Данные варианты ЗДЛ по составному модулю представляют интерес для синтеза криптосхем, основанных на одновременном решении двух трудных задач: ЗДЛ и ЗФ. В случае построения криптосхем со 128 битной стойкостью значения делителей функции Эйлера от сомножителей составного модуля должны иметь следующие размеры: 256 бит, 128 бит и 128 бит. А при выборе значений простых множителей составного модуля длиной 1232 бит и 2464 бит, сложность факторизации составного модуля и сложность ЗДЛ по модулю наименьшего множителя составного модуля равна примерно 2^128 операций модульного умножения.

Березин А.Н., Демьянчук А.А., Рыжков А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ПРОТОКОЛЫ С НУЛЕВЫМ РАЗГЛАШЕНИЕМ, ИСПОЛЬЗУЮЩИЕ АЛГОРИТМЫ ОТКРЫТОГО ШИФРОВАНИЯ

Протоколы с нулевым разглашением секрета относятся к двухключевым криптосистемам и применяются для аутентификации удаленных абонентов информационно-телекоммуникационных систем. Они также называются протоколами без разглашения секрета.

В настоящем сообщении рассматривается подход к построению протоколов с нулевым разглашением, основанный на идее использования алгоритмов открытого шифрования в качестве основного механизма протокола. В протоколах такого типа предполагается использование некоторого алгоритма открытого шифрования Publ_Encr. Проверяющий может направить доказывающему некоторое случайное сообщение M, предварительно зашифровав его по открытому ключу (ОК) доказывающего, т.е. направив доказывающему криптограмму C=Publ_Encr(M, P), где P – открытый ключ доказывающего. Прочитать это сообщение может только тот, кто знает личный секретный ключ (ЛСК), связанный с ОК P, т.е. только подлинный доказывающий. Получив значение C в качестве случайного запроса, доказывающий должен расшифровать криптограмму и направить проверяющему в качестве своего ответа исходное сообщение M, т.е. проверяющий получает значение которое уже знает. Поскольку проверяющий

не получил никакого нового сообщения, то и утечки информации о ЛСК доказывающего не происходит. При этом проверяющий получает информацию о том, что доказывающий является подлинным.

Однако следует учитывать и то, что проверяющий имеет возможность выбрать случайный запрос, а не формировать его как криптограмму, полученную с помощью процедуры открытого шифрования. В этом случае проверяющий не знает заранее ответа на свой запрос, а следовательно нужно считать, что он получает некоторую информацию о секретном ключе, т.е. он может как-то использовать эту возможность для раскрытия ЛСК доказывающего.

Поэтому, в предлагаемых реализациях двухшаговых протоколов с нулевым разглашением используется механизм включения заранее специфицированных меток в исходное сообщение, которое шифруется проверяющим. Наличие такой метки в расшифрованном доказывающим сообщении убеждает последнего в том, что метка была сформирована корректно. Размер меток выбирается равным от 80 до 512 бит, благодаря чему вероятность того, что расшифрование некорректно сформированного запроса даст текст, в котором будет присутствовать метка является пренебрежимо малой. Использование меток устраняет необходимость дополнительного использования хэш-функций и выполнения вычисления хэш-кода как проверяющим, так и доказывающим.

Предлагаются конкретные варианты построения протоколов в рамках предложенного подхода, в которых используются различные алгоритмы открытого шифрования: RSA, Эль-Гамаля, Рабина. В предложенных протоколах используется проверка доказывающим того, что отправляемый им ответ уже известен проверяющему, как проверка наличия специфицированных меток в расшифрованном значении.

Другим подходом к построению двухшаговых протоколов аутентификации с нулевым разглашением секрета является применение схем открытого согласования ключа и генерации разовых открытых ключей. В рамках такого подхода наиболее эффективная реализация протокола связана с использованием вычислений на идеальной эллиптической кривой или в поле двоичных многочленов, порядок мультипликативной группы которых равен простым числам Мерсена. Можно выбрать трёхчлены со степенями равными степеням Мерсена в качестве модуля, операция модульного умножения двоичных многочленов в поле может быть выполнена путем осуществления одной операции арифметического умножения многочленов, двух операций арифметического сдвига и шести операций сложения. Выполнение операции деления многочленов не требуется, что существенно снижает сложность вычислений в поле и повышает быстродействие протокола аутентификации. В этом варианте протокола нет необходимости выполнять проверку корректности запроса, поскольку любая ненулевая битовая строка, интерпретируемая как элемент поля имеет порядок равный простому числу Мерсена, т.е. никакие запросы со стороны проверяющего не могут быть им использованы для получения хотя бы одного бита информации о ключе. В настоящее время представляют интерес для практической реализации разработанных протоколов следующие шесть значений степеней Мерсена: 1279, 2203, 2281, 3217, 4253, 4423, поскольку при их использовании достигается приемлемый компромисс между стойкостью и производительностью.

Блюм В.С. Заболотский В.П.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ПОЛНОТА ИНТЕГРИРОВАННОЙ ЭЛЕКТРОННОЙ МЕДИЦИНСКОЙ КАРТЫ, КАК УСЛОВИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПАЦИЕНТА

Информационная безопасность личности – это состояние и условие жизни личности, при которой реализуются ее права и свободы. В том числе, и в первую очередь, право на жизнь и охрану здоровья (Конституция РФ, гл. 2, ст.41).

В статье 41 Конституции Российской Федерации закреплено право каждого гражданина на охрану здоровья, зафиксирована обязанность государства финансировать программы охраны и укрепления здоровья, декларирована ответственность за сокрытие информации способной нанести ущерб жизни и здоровью граждан.

Многочисленными исследованиями показано, что в силу чрезвычайной сложности человеческого организма и ограниченности знаний о его функционировании, любая, даже самая развитая, система здравоохранения обречена на значительный (не менее 10% – данные ВОЗ) процент дефектов оказания медицинской помощи в общем числе оказанных медицинских услуг. В этой связи, особенное значение и актуальность имеют методы и системы, направленные на оперативное выявление дефектов оказания медицинской помощи и их нейтрализацию.

В докладе рассматривается дискретно-событийная модель формирования базы интегрированных электронных медицинских карт. Обосновано положение о необходимости достижения полноты интегрированной медицинской карты для организации облачных вычислений с целью раннего обнаружения дефектов оказания медицинской помощи.

Богданов А.В., Примакин А.И., Синещук М.Ю., Синещук Ю.И., Яковлева Н.А.
Россия, Санкт-Петербург, Государственный Эрмитаж,
Санкт-Петербургский университет МВД России

ПОСТРОЕНИЕ КОНЦЕПТУАЛЬНОЙ МОДЕЛИ НАРУШИТЕЛЯ С ЦЕЛЬЮ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Большинство информационно-управляющих систем функционируют с участием человека, а преступления, как известно, совершаются людьми. Следовательно, вопросы безопасности такого рода систем часто сводятся к вопросам человеческих отношений и человеческого поведения.

Нарушителем безопасности называют лицо, которое осуществляет попытку выполнения запрещенных операций, либо по ошибке, либо по незнанию, либо осознанно. Наиболее опасен – злоумышленник, как разновидность нарушителя, который намеренно идет на преступление из корыстных побуждений. В общем случае, нарушитель может быть внешним по отношению к защищаемой системе (посторонние лица) и внутренним (из числа персонала, пользователь – в широком смысле).

Особую сложность в раскрытии компьютерных преступлений представляют именно пользователи, с одной стороны, это есть ее необходимый элемент, а с другой стороны – источник нарушения или преступления. Поэтому целесообразно заблаговременно построить модель нарушителя безопасности, которая характеризует его теоретические и практические знания, навыки, время и место действия.

Построение концептуальной модели нарушителя целесообразно начинать с анализа социальных истоков компьютерной преступности. При этом надо учитывать, что между людьми часто возникают конфликты, которые могут сказаться на состоянии безопасности.

Анализ сути и содержания социально-психологических конфликтов позволяет выработать конкретные рекомендации, позволяющие воздействовать и даже управлять социально-психологической обстановкой в коллективе, способствуя тем самым повышению уровня защищенности объекта.

Выделяют три основные побудительные причины нарушений информационной безопасности со стороны пользователей – это безответственность, самоутверждение и корыстный интерес.

При разработке модели нарушителя необходимо дифференцировать всех пользователей по возможности доступа к системе и по потенциальному ущербу от каждой категории пользователей.

Способы предотвращения нарушений вытекают из природы побудительных мотивов. В качестве базовых профилактических мер можно назвать – подготовку пользователей, поддержание здорового климата в коллективе и подбор персонала.

Описание особенностей нарушителя следует рассматривать как его предрасположенность к совершению преступления. Однако, реализация этой предрасположенности зависит от личности пользователя, ее ценностных ориентации, складывающихся под влиянием социальных отношений, в которые он включен.

Модель нарушителя позволяет выявить условия, при которых может произойти формирование психологической готовности к противоправным действиям и произвести общую типизацию криминальности потенциального нарушителя. Для этого:

Каждый тип нарушителя должен быть охарактеризован значениями соответствующих характеристик. При этом необходимо помнить, что определение конкретных значений характеристик модели нарушителя в значительной степени субъективно и, следовательно, модель нарушителя может быть представлена перечислением нескольких вариантов его облика.

Исходя из рассмотренных положений, «модель нарушителя» адекватная реальным возможным типам нарушителей, включает описания его практических и теоретических возможностей, место и время реализации его действий, другие характеристики.

В процессе разработки модели нарушителя необходимо определить: категории лиц, к которым может принадлежать нарушитель; мотивы действий нарушителя (его цели); квалификацию нарушителя, его осведомленность о системе защиты и оснащённость; характер возможных действий нарушителя.

При этом необходимо учитывать следующие факторы:

– хорошо поставленная работа по подбору кадров и профилактические мероприятия препятствуют формированию коалиций нарушителей, их сговора;

– принцип «враждебного окружения» предполагает, что любой нарушитель, скрывает свои преступные действия от других сотрудников;

– деструктивные проявления в функционировании объекта защиты могут быть следствием элементарных ошибок сотрудников (пользователей, администраторов, эксплуатирующего и обслуживающего персонала), а также недостатков принятой технологии обработки информации и т.д.

Адекватная реальности модель нарушителя может служить основой прогнозного сценария реализации криминальных поступков по нарушению системы безопасности, позволяет проанализировать причины нарушений и дает возможность либо устранить их заблаговременно, либо обоснованно сформулировать требования к разрабатываемой системе защиты и эффективно проводить мероприятия по профилактике и расследованию компьютерных преступлений.

Борзенко Р.А., Вайчикаускас М.А., Молдовян Д.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербургский институт информатики и автоматизации РАН

ПРОТОКОЛЫ ЦИФРОВОЙ ПОДПИСИ НА ОСНОВЕ ГОСТ Р 34.10–2012

Новый стандарт электронной цифровой подписи (ЭЦП) ГОСТ Р 34.10–2012 специфицирует алгоритмы формирования и проверки ЭЦП в рамках протокола индивидуальной цифровой подписи. Однако практикой востребованы также протоколы коллективной ЭЦП, слепой ЭЦП и слепой коллективной ЭЦП. Реализация протоколов ЭЦП с расширенной функциональностью на основе алгоритмов, предписанных стандартами ЭЦП, представляет значительный интерес с прикладной точки зрения. Ранее было показано, что перечисленные типы протоколов ЭЦП могут быть реализованы на основе стандартов ЭЦП России ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001, Беларуси СТБ 1176.2–99 и Украины ДСТУ 4145–2002, в то время как такое расширение функциональности стандартов США DSA и ECDSA не представляется возможным. В связи с принятием нового стандарта ЭЦП ГОСТ Р 34.10–2012 представляет интерес вопрос о возможности расширения его функциональности.

В предлагаемом сообщении обсуждается вопрос о возможности использования алгоритмов генерации и верификации цифровой подписи, специфицированных стандартом ГОСТ Р 34.10–2012, в протоколах коллективной, слепой и слепой коллективной ЭЦП.

К протоколам коллективной ЭЦП предъявляется требование обеспечения целостности коллективной подписи. Это требование состоит в том, чтобы по данной коллективной подписи нельзя было бы сформировать какие-либо другие подписи (коллективные или индивидуальные), проходящие процедуру проверки как подлинные подписи. Для протоколов обычной (индивидуальной) ЭЦП ее целостность заключается в вычислительной невозможности формирования по имеющейся подлинной индивидуальной ЭЦП к электронному сообщению M некоторой другой подлинной подписи, относящейся к M или другому электронному сообщению и некоторому другому открытому ключу (ОК).

Для обеспечения свойств целостности используются следующие приемы: 1) проверка корректности генерации ОК, состоящей в том, что ОК, регистрируемые и распространяемые удостоверяющим центром, сформированы в строгом соответствии с процедурой, специфицированной используемой схемой ЭЦП; 2) вычисление значения хэш-функции от сообщения с присоединенным к нему коллективным ОК, относящимся к заданному набору пользователей, разделяющих коллективную цифровую подпись. Для удобства практического применения протоколов коллективной ЭЦП, последние строятся таким образом, чтобы использовать имеющуюся на практике инфраструктуру открытых ключей. При этом протокол коллективной ЭЦП строится как обобщение протокола индивидуальной ЭЦП, в котором цифровая подпись относится к произвольному числу подписывающих $m \geq 1$. Таким образом, протоколы коллективной ЭЦП при значении $m = 1$ реализуют протокол обычной индивидуальной ЭЦП.

Протоколы слепой подписи решают задачу обеспечения анонимности в системах электронной наличности и тайного электронного голосования. В протоколах такого типа используются случайные ослепляющие параметры, формируемые клиентом, т.е. пользователем, который готовит и предоставляет документ или его хэш-код для формирования подписывающим слепой подписи. По полученному значению слепой ЭЦП клиент формирует подлинную ЭЦП, устраняя маскирующий эффект внесенный ослепляющими параметрами.

Изучение стандарта ГОСТ Р 34.10–2012 показало, что он специфицирует проверочное уравнение, аналогичное проверочному уравнению стандарта ГОСТ Р 34.10–2001, поэтому способы расширения функциональности, применимые к стандарту 2001 г., могут быть также использованы и для построения протоколов расширенной функциональности, реализуемых на основе ГОСТ Р 34.10–2012. Разработано несколько вариантов протоколов коллективной и слепой ЭЦП, а так же проколов слепой коллективной ЭЦП.

Бориев З.В.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова

ЗАЩИТА ИНФОРМАЦИИ В БАЗАХ ДАННЫХ

В настоящее время объём информации в мире настолько велик, что самым оптимальным методом работы с ней является база данных (БД). База данных – это представленная в объективной форме совокупность материалов, систематизированных так, чтобы эти материалы могли быть найдены и обработаны с помощью компьютера. Её защита является одной из самых сложных задач на сегодняшний день.

Угрозы потери конфиденциальной информации стали обычным явлением,и если в системе защиты есть недостатки, то ценные данные могут оказаться в руках третьих лиц. Каждый сбой работы

БД может парализовать работу целых корпораций, фирм, что приведет к весомым материальным потерям.

Методы защиты баз данных в различных СУБД условно делятся на две группы (анализ современных фирм Borland и Microsoft):основные и дополнительные.

К основным средствам защиты относится:

– защита паролем;
– шифрование;
– разделение прав доступа к объектам БД;
– защита полей и записей таблиц БД.

Защита паролем – это самый простой способ защиты БД от несанкционированного доступа. Пароли устанавливаются пользователями или администраторами. Их учет и хранение выполняется системой управления базой данных (СУБД). Пароли хранятся в специальныхфайлах СУБД в шифрованном виде. После ввода пароля пользователю предоставляется доступ к требуемой информации.

Несмотря на простоту парольной защиты, у неё имеется ряд недостатков. Во-первых, пароль уязвим, особенно если он не шифруется при хранении в СУБД. Во-вторых, пользователю надо запоминать или записать пароль, а при небрежном отношении кзаписям пароль может стать достоянием других.

Более мощным средством защиты данных является шифрование. Шифрование – это процесс перевода информации по определенному алгоритму в вид непригодный для чтения, в целях защиты от несанкционированного просмотра или использования.Важной особенностью любого алгоритма шифрования является использование ключа, который утверждает выбор конкретного метода кодирования из всех возможных. В основном применяется для защиты уязвимых данных.

Шифрование обеспечивает три состояния безопасности информации:

– Конфиденциальность.
– Целостность.
– Идентифицируемость.

В целях контроля использования основных ресурсов СУБД во многих системах имеются средства установления прав доступа к объектам БД. Права доступа определяют возможные действия над объектами. Владелец объекта, а также администратор БД имеют все права. Остальные пользователи имеют те права и уровни доступа к объектам, которыми их наделили.

Разрешение на доступ к конкретным объектам базы данных сохраняется в файле рабочей группы.

Файл рабочей группы содержит данные о пользователях группы и считывается во время запуска. Файл содержит следующую информацию: имена учетных записей пользователей, пароли пользователей, имена групп, в которые входят пользователи.

К дополнительным средствам защиты БД можно отнести следующие средства:

– встроенные средства контроля значений данных в соответствии с типами:
– повышение достоверности вводимых данных:
– обеспечения целостности связей таблиц:
– организации совместного использования объектов БД в сети.

Описанные выше методы и способы являются основополагающими, однако их использование не гарантирует полной сохранности данных. Для повышения уровня безопасности информации в БД рекомендуется использование комплексных мер.

Бухарметов М.Р.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПЕРЕДАЧИ ДАННЫХ ПО ОТКРЫТЫМ КАНАЛАМ НА ВОДНОМ ТРАНСПОРТЕ

Эффективность работы водного транспорта напрямую зависит от наличия безопасных средств управления и связи. Процесс управления предполагает обработку большого количества разнородной информации. Некоторая часть может представлять собой данные различных уровней конфиденциальности, такие как персональные данные или коммерческая тайна. Задача защиты конфиденциальной информации может решаться путем создания собственной физической сети. Но данный способ может быть либо экономически неоправданным, либо технически невозможным. Поэтому для построения сети для обмена с удаленным пользователем конфиденциальной информацией приходится прибегать к услугам глобальной сети, что позволяет снизить эксплуатационные расходы. Но при передаче персональных данных по открытым каналам (сетям общего пользования) количество субъектов, имеющих доступ к сети, не ограничено, доступ может получить любой. Из за чего существует риск нарушения их безопасности и целостности, появляется вероятность искажений и считывание информации третьими лицами. В этом случае

организационными мерами безопасности не обойтись, нужны технические. Для этого передаваемая информация модифицируется таким образом, чтобы её невозможно было изменить (аутентификация) или просмотреть (криптография) на пути её следования. При совместном применении этих двух механизмов обеспечивается как сокрытие информации, так и невозможность ее подмены на всем пути ее следования.

Использование криптографии обеспечивает защиту данных от просмотра или изменения, а также создает защищенные каналы связи на основе незащищенных каналов. Например, данные могут быть зашифрованы с помощью некоторого криптографического алгоритма, переданы в зашифрованном виде, а затем расшифрованы лицом, которому они предназначались. В криптографии базовыми понятиями являются ключ и математический алгоритм. При помощи этого алгоритма и ключа, информация модифицируется таким образом, чтобы была гарантирована возможность обратного преобразования данных к первоначальному виду, только при условии, что известны алгоритм и ключ. Если хотя бы один из компонентов скрыт, как правило это ключ, то просмотр данных посторонним человеком будет невозможен, а расшифровать перехваченные данные будет достаточно трудно.

В аутентификации, так же как и в криптографии, основными понятиями являются ключ и алгоритм. Но в отличии от криптографии, математический алгоритм используется не для шифрования передаваемых данных по сети, а для создания электронной цифровой подписи (ЭЦП). ЭЦП является аналогом подписи, которую ставят на бумажных документах, либо печати. Но подпись на электронных документах формируется таким образом, чтобы вычислить её, не зная ключа и алгоритма было невозможно. Созданная таким образом электронная подпись передается по открытому каналу в пункт назначения. Но так как передаваемые данные не были зашифрованы, то существует вероятность перехвата информации третьими лицами и её дальнейшего изменения. Если это произойдет, то при помощи электронной подписи изменение документа сразу будет обнаружено. После сравнения полученной электронной подписи передаваемых данных с вычисленным значением цифровой подписи на хосте назначения искажение документа будет идентифицировано. Таким образом, ЭЦП предназначена для защиты от подделки электронных документов, а так же для идентификации лица, подписавшего данный документ.

Операция шифрования данных по сравнению с вычислением электронной подписи выполняется более длительное время. Но в отличие от криптографии, аутентификация не может защитить данные от чтения, а предназначена лишь для защиты от фальсификации передаваемых данных. Поэтому ЭЦП следует применять лишь в тех случаях, когда важна надежность доставки, а не конфиденциальность. Для усиленной защиты можно использовать аутентификацию совместно с криптографией, что позволит повысить надежность передаваемой конфиденциальной информации по открытым каналам.

Использование описанных средств может способствовать усилению защищенности корпоративной информации без использования лишних вложений во внутреннюю сеть, а так же снизить её расходы на эксплуатацию.

Бухарметов М.Р.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова

МЕТОДЫ ОБЕСПЕЧЕНИЯ ЗАЩИЩЕННОГО ДОКУМЕНТООБОРОТА В ТРАНСПОРТНОЙ СФЕРЕ

Развитие средств защиты информационного наполнения документа является актуальной задачей в различных сферах, в том числе и на водном транспорте. Так, например, одним из ключевых элементов достаточно большого числа документов являются медиа файлы. Защита авторских прав владельца на файл, противодействие копированию и подделкам, всё это далеко не полный перечень применения средств защиты информации.

С развитием информационных сетей мир постепенно превращается в единое информационное и коммуникационное пространство и проблемы, возникающие в связи с защитой авторских прав, прежде всего следуют из свойств самой всемирной сети: глобальность, общедоступность, анонимность. Именно сеть дает возможность бесконтрольного использования авторских прав, так например копия изображения может оказаться на другом сайте без указания имени автора или в искаженном виде. Для того, чтобы это не произошло можно задействовать ЭЦП (электронно-цифровую подпись), которая может быть использована физическими и юридическими лицами в качестве аналога собственноручной бумажной подписи, для придания документу юридической силы. Но ведь не обязательно скрывать информацию только об авторе файла. Что же ещё может быть зашифровано в небольшом медиа файле? Для этого разберем структуру одного из самых популярных на сегодняшний день формата файлов изображений JPEG.

Важнейшей особенностью формата JPEG является использование алгоритма сжатия информации с потерями. Это означает, что при сжатии файла часть информации уничтожается, но

изменения не сильно влияют на файл и они не мало заметны. Алгоритм изображения JPEG состоит из нескольких этапов, последовательно выполняемых друг за другом:

- Преобразования цветового пространства.
- Дискретизация.
- ДКП.
- Квантование.
- Кодирование.

На первом этапе происходит преобразование из цветового пространства RGB (широко используемое в компьютерной графике) в пространство YCbCr (основано на характеристиках яркости и цветности). Вся дальнейшая работа будет производится именно в этом цветовом пространстве. Применение данного пространства вместо привычного и легкого для понимания RGB объясняется физиологическим строением человеческого глаза, а именно нервной системой человеческого зрения, которая обладает гораздо большей чувствительностью к яркости нежели к цветоразностным составляющим.

Именно благодаря большей чувствительности глаза к яркости света чем к оттенку следует второй шаг алгоритма сжатия формата JPEG – это дискретизация. На данном этапе изображение ужимают вдвое, разбив всю сетку пикселей блоками 2x2, то есть по 4 пикселя, и взяв их усредненное значение цветоразности. Это необязательный шаг, но так как ведет к мало заметным потерям качества с точки зрения восприятия картины глазом человека, его почти всегда используют.

Далее идет один из самых важных моментов сжатия файла. Изображение делится на блоки размерами 8x8 точек и отдельно для каждого компонента цветового пространства Y, Cb, Cr осуществляется прямое дискретно косинусное преобразование. Цель этого преобразования заключается в переходе от пространственного представления изображения к спектральному (пространству частот изменения яркости и оттенка).

Получив частоты каждого компонента можно приступать к квантованию полученной информации. Именно на этом этапе мы терпим практически все потери. Известно, что зрение человека мало восприимчиво к высоким частотам, особенно высоким частотам цветоразностных компонент. Поэтому эти частоты с помощью специальных таблиц квантования обнуляются, что приводит при деквантовании к потерям информации.

Кодирование является заключительным этапом сжатия, во время которого блоки изображения преобразуются в векторную форму (как правило, в начале вектора будут записываться ненулевые коэффициенты, а в конце цепочки из нулей). При помощи модифицированного алгоритма RLE убираем последовательности из нулей, заменяя вектор парами типа (пропустить, число), где «пропустить» означает то количество нулей, которое нужно пропустить, а «число» – значение, которое необходимо поставить в следующую ячейку. Остается только завершить данный алгоритм сжатия, свернув получившиеся пары с помощью неравномерных кодов Хаффмана с фиксированной таблицей.

Вайчикаускас М.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ПРЕОБРАЗОВАНИЕ ОТКРЫТЫХ ТЕКСТОВ, ШИФРОТЕКСТОВ И РЕЗУЛЬТАТОВ ШИФРОВАНИЯ ДЛЯ ОПРЕДЕЛЕНИЯ КРИПТОГРАФИЧЕСКОЙ СТОЙКОСТИ АЛГОРИТМОВ ГЕНЕРАЦИИ КЛЮЧЕВОЙ ИНФОРМАЦИИ

Несмотря на существование ряда общеизвестных способов генерации ключей, например, по стандарту ANSI X 9.17 существует алгоритм DES в режиме выходной обратной связи, формирование ключей с помощью генераторов псевдослучайных чисел, зачастую производители смарт-карт используют собственные, разработанные внутри компании алгоритмы. Поскольку ключ не генерируется случайным образом и сформирован по некому математическому алгоритму, он обладает определенными свойствами, делающими его более стойким против известного ряда атак, таких, как, например, способ полного перебора. Такой метод генерации позволяет отсеивать потенциально слабые ключи, не отвечающие этим свойствам, сокращая область выбора ключевого значения. В связи с вышесказанным, возникает вопрос, возможно ли смоделировать алгоритм, позволяющий существенным образом сократить область поиска, делая задачу нахождения ключа вычислительно осуществимой. Для решения данной задачи могут использоваться следующие методы криптоанализа: атака на основе шифротекста, атака на основе окрытых текстов и соответствующих шифротекстов, атака на основе подобранного открытого текста и атака на основе адаптивно подобранного открытого текста. В нашем случае актуальными являются два последних способа. Атака на основе адаптивно подобранного открытого текста является более удобным частным случаем атаки на основе подобранного открытого текста, поэтому использование данного типа атаки является, в данном случае, наиболее целесообразным. Поскольку ключ генерируется машиной по определенному алгоритму, логично сделать вывод о том, что ключи, формируемые таким

образом, описываются некоторыми критериями, предполагающими исключение слабых ключей. Такой механизм генерации сужает область подбора от первоначальных *N* вариантов, исключая так называемые слабые ключи. Слабый ключ определим как ключ, не обеспечивающий достаточного уровня защиты или использующий в шифровании закономерности, которые могут быть выявлены. Для имитации действий алгоритма формирования будем руководствоваться следующей идеей: наименее сложную задачу составляет нахождение ключа с простейшим внутренним строением. Под внутренним строением будем понимать совокупность символов в шестнадцатеричном представление Мастер-ключа. Сложным внутренним строением будем считать такое устройство ключа, при котором не существует закономерностей между символами, составляющими шестнадцатеричное представление, то есть данные символы образуют случайную последовательность.

Таким образом, можно сделать вывод, что для определения криптографической стойкости алгоритма генерации ключа необходимо выявить ключи, внутреннее устройство которых можно описать определенными способом. Описание такого внутреннего устройства будет являться критерием принадлежности ключа к множеству слабых значений.

Вайчикаускас М.А., Мондикова Я.А., Фахрутдинов Р.Ш.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербургский институт информатики и автоматизации РАН

АЛГОРИТМ ОТКРЫТОГО ШИФРОВАНИЯ НАД ДВОИЧНЫМ ПОЛЕМ

Алгоритмы открытого шифрования (АОШ) относятся к двухключевым шифрам и решают задачу защиты конфиденциальной информации, передаваемой по открытым каналам, без необходимости предварительного распределения секретных ключей. Эта возможность реализуется за счет использования открытых ключей (ОК) при выполнении процедуры зашифрования сообщения. Расшифровать криптограмму может только владелец ОК, по которому было выполнено зашифрование сообщения. Открытое шифрование можно использовать также и для выполнения процедуры распределения секретных ключей с последующим шифрованием передаваемых сообщений с использованием симметричных криптосистем, которые обладают существенно более высокой производительностью. Последний вариант соответствует реализации гибридной криптосистемы.

В основе АОШ лежат некоторые вычислительно трудные задачи, например задача факторизации целых чисел специального вида и задача дискретного логарифмирования (ЗДЛ) в конечном поле. Примером построения АОШ на основе ЗДЛ конечном простом поле *GF*(*p*) является алгоритм Эль-Гамаля. Для предотвращения различных атак на данный шифр требуется выбрать его параметры соответствующим образом. В известной литературе обычно указывается требование делимости числа $p - 1$ на достаточно большое простое число *q*. Однако для некоторых специальных видов атак этого недостаточно. В настоящем сообщении рассматривается сценарий такой атаки и предлагаются варианты выбора параметров АОШ для обеспечения стойкости к ней. Показывается, что задание АОШ с использованием ЗДЛ в конечных двоичных полях *GF*(2^*s*), степень расширения которых равна одному из следующих простых чисел: 1279, 2203, 2281, 3217, 4253 и 4423 и представляет собой наиболее привлекательный вариант для нейтрализации указанной атаки.

Полная нейтрализация рассмотренной атаки может быть достигнута построением АОШ с использованием ЗДЛ, заданной над конечным двоичным полем *GF*(2^*s*) с таким значением степени расширения поля, для которого число $2^s - 1$ является простым (числа такого вида называются числами Мерсенна).

Двоичные многочлены – это многочлены, заданные над полем *GF*(2). Все такие многочлены, имеющие степень, не превышающую значение $s - 1$, образуют конечное поле, называемое полем двоичных многочленов *GF*(2^*s*), при задании операции умножения многочленов по модулю некоторого неприводимого двоичного многочлена $\eta(x)$ степени *s*. Известно, что мультипликативная группа любого конечного поля является циклической и включает все элементы поля, кроме нулевого элемента (нуля). В случае поля двоичных многочленов $GF(2^s)$ порядок мультипликативной группы равен $q = 2^s - 1$. Если выбрать такое значение *s*, что число *q* окажется простым, то все двоичные многочлены поля $GF(2^s)$ будут иметь порядок *q*, т.е. будут являться образующими мультипликативной группы поля.

Предложенный АОШ представляет практический интерес благодаря тому, что нейтрализуется атака на основе известного сообщения, восстановленного из криптограммы и появляется возможность использования секретных ключей размером 160–256 бит, за счет чего может быть существенно снижена вычислительная сложность процедуры расшифрования. При этом может быть получен дополнительный выигрыш в производительности путем применения двоичных трехчленов и пятичленов в качестве неприводимого многочлена $\eta(x)$, используемого в качестве модуля операции умножения, что позволяет выполнить модульное умножение без выполнения операции деления многочленов.

В настоящее время представляют интерес для практической реализации предложенного АОШ следующие шесть значений *s*: 1279, 2203, 2281, 3217, 4253 и 4423. Для будущих приложений представляют интерес еще шесть других значений *s*: 9689, 9941, 11213, 19937, 21701 и 23209. Для указанных двенадцати значений степени Мерсенна известны неприводимые двоичные многочлены с достаточно малым числом (три или пять) ненулевых коэффициентов. Операции умножения по модулю таких многочленов имеют сравнительно низкую вычислительную сложность, т.е. их использование позволяет существенно повысить производительность АОШ.

Воробьев В.И., Евневич Е.Л., Шкиртиль В.И.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
МОДЕЛИРОВАНИЕ ЗАЩИЩЕННОСТИ СЕРВИСОВ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ

Новые парадигмы, такие как сервис-ориентированные архитектуры и облачные вычисления, превратили IT-технологии в решающий фактор развития индустрии . Жизненные циклы программ и сервисов становятся все короче за счет использования интероперабельных продуктов. Современные SaaS, PaaS и IaaS архитектуры часто оказываются недостаточно защищенными в условиях повышенных требований потребителя, касающихся композиции и качества сервисов.

Важным сервисом является обработка Больших Данных, интегрированная с облачными системами. Здесь необходимо решать задачи защищенного программно-конфигурируемого распределенного хранения; унифицированной аналитики в реальном времени; аналитики в виде сервиса по требованию; прозрачного встраивания результатов обработки в бизнес-процессы и документооборот предприятия.

Структура нахождения данных и сервисов в облачных вычислениях неопределенна и может меняться. Для облачных вычислений необходим Интернет поиск данных и соответствующих сервисов. Учитывая вышесказанное, представляется целесообразным построить онтологическое описание данных и сервисов, что при использовании языков онтологии позволит автоматически построить структуру местоположения данных и сервисов.

Предлагается онтологическая модель, позволяющая провайдерам и потребителям подбирать оптимальные композиции ресурсов, основываясь на пользовательском запросе. Онтология на OWL для описания ресурсов аппаратного и программного обеспечения, включающая ограничения интероперабельности, мета информацию, некоторые критерии поиска, граф композиций ресурсов, основывающиеся на абстрактном запросе, позволяет найти приемлемое решение. Онтология содержит набор понятий предметной области и связей между ними, способствуя тем самым обмену информацией между компьютерной средой и пользователем, и применяется для извлечения запрашиваемых пользователем ресурсов.

Описание функциональных требований поступает на вход онтологической модели, которую можно рассматривать в качестве базы знаний. Для представления знаний используется онтология Semantic Web и управляющие языки OWL и SWRL в комбинации с возможностями SPARQL-запросов.

Деменева А.А.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова
ЗАЩИТА МНФОРМАЦИИ В MICROSOFTOFFICE

Любая информация, хранимая в электронном виде, уязвима. Сюда можно отнести различные виды данных – от корпоративных записок до военных оборонных стратегий и другой секретной правительственной информации. С развитиемтехнологий структура угроз непрерывно эволюционирует. Если в начале 90-х годов атаки злоумышленников были в основном направлены на серверы и клиентские машины, то в последнее время всё чаше приходится сталкиваться с попытками получения информации непосредственно из пользовательских приложений.

Одним из лидеров в области разработки систем безопасности для приложений на протяжении многих лет является компания Microsoft. В каждой новой версии пакета MicrosoftOffice появляются более совершенные элементы защиты, которые позволяют предотвратить атаки с использованием известных слабостей системы.

Ключевым компонентом архитектуры безопасностиофисных программ является механизм многоуровневой защиты.Эта стратегия позволяет устранить угрозы безопасности посредством нескольких элементов, тесно взаимодействующих друг с другом**.** Компонент предотвращения выполнения данных можно назвать первым уровнем защиты. Он позволяет предотвратить проблемы, которые могут возникнуть при попытке выполнения кода из той части памяти, которая не помечена как исполняемая. На следующем уровне для того чтобы снизить вероятность атак введены ограничения типов файлов доступных для открытия, а также происходит предотвращение выполнения определенных типов кода. Компонент проверки файлов может остановить их запуск, если будет обнаружено, что формат является недопустимым. Также с помощью параметров

блокировки можно ограничить или полностью запретить открывать и сохранять определенные типы файлов. Защита от вредоносных программ происходит путем открытия потенциально опасных документов в изолированной среде, которая называется защищённым просмотром. При помощи этой функции пользователи могут предварительно просматривать файлы перед их фактическим открытием и редактированием.

Помимо выше перечисленных уровней защиты приложения MicrosoftOffice обладают еще рядом эффективных средств. Самым распространенным методом является установка пароля. С его помощью пользователь может защитить файл от нежелательного просмотра. Программы MSOffice содержат параметры, которые позволяют управлять способом шифрования данных, выбирать наиболее подходящие алгоритмы. В общем виде схема шифрования достаточно стандартна – из пароля с помощью хеширования получается ключ, на этом ключе шифруется документ.

Еще один способ защиты это цифровая подпись. По сути это примерно то же самое, что и обычная подпись, заверенная нотариусом. Отличие лишь в том, что она выдается специальной организацией – Центром сертификации. Добавление ее в документ может быть как явным, так и срытым. Также в более поздних версиях офисных программ в цифровых подписях поддерживаются надежные отметки времени.

Что касается средств защиты от компьютерных вирусов, то в приложениях MicrosoftOffice предприняты некоторые профилактические меры, но они явно недостаточны, ибо не позволяют обнаружить вирусы и излечить от них. Для этого понадобятся системные антивирусные утилиты. Аналогичная ситуация характерна для средств защиты от несанкционированного копирования и удаления данных, средств восстановления утерянных и испорченных данных.

Программы MicrosoftOffice содержит различные средства, которые помогут защитить документы и обезопасить рабочие станции, но обеспечить полную сохранность данных очень сложно. И только комплексное использование всех мер позволит максимально полно защитить данные.

Десницкий В.А., Котенко И.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

КОНФИГУРИРОВАНИЕ ВСТРОЕННЫХ СИСТЕМ ЗАЩИТЫ В РАМКАХ СЕРВИСОВ МНОГОУРОВНЕВОЙ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Современные системы поддержки процессов на железнодорожном транспорте (ЖТ) представляют собой сложные информационно-телекоммуникационные сетевые и распределенные архитектуры, включающие взаимодействующие между собой различные стационарные и мобильные встроенные устройства. В рамках бизнес-процессов ЖТ встроенные устройства предоставляют специализированные функции коммуникации, ввода информации, контроля, информирования, обработки и хранения данных и событий безопасности автоматизированных систем ЖТ. Такие системы характеризуются динамически изменяемой топологией сети и отличающимися типами коммуникаций между ее отдельными узлами, а также заранее не фиксированным набором функционирующих агентов и задействованных устройств.

Специфика встроенных устройств включает их меньшую по сравнению с другими видами вычислительных систем производительность и ограниченность доступных программно-аппаратных ресурсов, что обуславливает применение компонентного подхода к их разработке, при котором устройство интегрируется в виде некоторого множества программных и программно-аппаратных компонентов, каждый из которых отвечает за реализацию определенной целевой функции. Как следствие, задача поддержки защиты таких систем требует принципиально новых путей решения, которые помимо реализации защиты от заданного вида угроз учитывали бы также нефункциональные («ресурсные») требования к механизму защиты.

Подход к нахождению оптимальной конфигурации компонентов защиты, предлагаемый в работе, базируется на получении серии численных нефункциональных показателей защиты, и − путем постановки и решения оптимизационной экстремальной задачи при ограничениях на значения этих показателей и заданной целевой функции − позволяет построить наиболее эффективную конфигурацию компонентов защиты для обеспечения безопасности информационно-телекоммуникационной системы. Особенностью такого подхода является большая гибкость процесса построения встроенного устройства, в том числе его направленность на возникающие изменения в требованиях, вносимые на различных этапах процесса проектирования и влекущие пересмотр ранее проведенных этапов.

Разработка встроенных систем защиты в рамках сервисов многоуровневой интеллектуальной системы комплексной безопасности железнодорожного транспорта включает: (1) анализ существующих моделей нарушителя, определение функциональных свойств защиты и свойств программно-аппаратной совместимости; (2) определение ограничений ресурсопотребления платформы устройства; (3) поиск и формирование репозитория имеющихся компонентов защиты встроенных устройств, определение их свойств; (4) проведение анализа несовместимостей

компонентов защиты на основе экспертных знаний в области безопасности встроенных устройств процессов управления железнодорожного транспорта; (5) проведение оценки ресурсопотребления компонентов защиты на основе автоматизированного модуля тестирования с использованием эмулятора встроенного устройства; (6) многокритериальный выбор компонентов защиты на основе учета показателей ресурсопотребления с использованием эвристик по выбору порядка учета критериев ресурсопотребления.

Анализ эффективности конфигурирования проводится путем его сравнения с альтернативными стратегиями комбинирования компонентов, алгоритмов и принципов защиты встроенных устройств. За счет применение экспертных знаний в области защиты встроенных устройств, а также знаний в предметной области автоматизированных систем управления железнодорожным транспортом методы оптимизации, моделирования, системного и объектно-ориентированного анализа, теории принятия решений позволят повысить уровень защищенности и эффективность ресурсопотребления встроенных устройств и сервисов, которые они предоставляют.

Программный прототип механизма конфигурирования, разработанный в рамках кросс-платформенной среды Java 2 с использованием принципов объектно-ориентированного проектирования и универсального языка моделирования UML, демонстрирует особенности процесса конфигурирования, включая возможность задания определенных критериев ресурсопотребления с учетом известных видов функциональных несовместимостей отдельных компонентов защиты.

Работа выполняется при поддержке РФФИ (проекты 13159-офи_м_РЖД, 13-01-00843-а и 11-07-00435-а) и программы фундаментальных исследований ОНИТ РАН.

Десницкий В.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ВЕРИФИКАЦИЯ ИНФОРМАЦИОННЫХ ПОТОКОВ В СИСТЕМАХ СО ВСТРОЕННЫМИ УСТРОЙСТВАМИ

Наличие существенных ограничений на системные ресурсы встроенных устройств обуславливает сложность использования традиционных криптографических алгоритмов и других программно-аппаратных средств защиты, которые применяются для обеспечения безопасности в централизованных, сетевых и распределенных архитектурах. Поэтому для защиты информационных систем со встроенными устройствами требуются специализированные подходы к проектированию механизмов защиты, которые могли бы обеспечить стойкость системы к атакам не только за счет дополнительных средств защиты, но и за счет особенностей архитектуры системы. Анализ информационной системы со встроенными устройствами на всех этапах проектирования, как один из путей достижения этой цели, позволяет избежать архитектурных недоработок, которые, в свою очередь, снижают уровень защищенности системы.

Важнейшим результатом работы является методика верификации сетевых информационных потоков. Методика включает оценку защищенности разрабатываемой информационной системы со встроенными устройствами, проверку корректности политики безопасности этой системы и определение уровня соответствия информационных потоков в реальной системе заданной политике.

Применяется метод «проверки на модели» для верификации правил политик безопасности, описывающих информационные потоки с использованием программного инструмента SPIN. Данный тип верификации относится к методам статического анализа системы и ее проведение на начальных этапах проектирования обеспечивает раннее выявление противоречий в рамках политики безопасности, а также несоответствий топологии сети информационной системы. В противоположность динамическому анализу, включающему тестирование готовых устройств на основе тестовых векторов атак, предлагаемый подход к верификации позволяет сократить количество и объем действий, которые необходимо провести повторно после исправления обнаруженных ошибок проектирования.

Сущность метода «проверки на модели» заключается в переборе состояний, в которые может перейти система в зависимости от появляющихся информационных потоков и ответов компонента, принимающего решения о разрешении или отклонении таких запросов на основе политик. Последовательность действий при переборе зависит от условий, которые сформулированы на языке линейной темпоральной логики и выражают корректные состояния системы. Состояние системы определяется набором значений переменных, а изменение состояния вызывается выполняющимися в ней параллельными процессами. Процесс, который должен выполняться в очередной момент времени, выбирается случайно. Система рассматривает все возможные последовательности шагов для заданных процессов и сигнализирует о потенциальном некорректном состоянии. После этого пользователю выдается «трасса», т.е. последовательность шагов, ведущая к некорректному состоянию системы относительно заданных условий. Перебор правил политики осуществляется в порядке уменьшения их приоритета до момента первого срабатывания. В целом приоритезация позволяет организовать более сложное управление взаимосвязанными правилами политики с возможностью задания правил по умолчанию.

В общем случае, по сравнению с классическими сетевыми структурами, особенностью информационных систем со встроенными устройствами в рамках задачи верификации политик контроля информационных потоков является наличие более разветвленной топологии сети с учетом разнообразных встроенных устройств с различными видами программно-аппаратных интерфейсов, являющимися точками входа и выхода информационных потоков, а также изменчивость таких систем (узлов, топологии, типов коммуникаций, сетевых протоколов) на всем протяжении работы системы.

В работе выделяется один из наиболее важных типов аномалий, на выявление которых направлена верификация, аномалия «затемнения». Наличие такой аномалии определяет, что некоторое правило никогда не срабатывает из-за того, что имеется одно или несколько правил, его «перекрывающих». Аномалия свидетельствует о вероятной ошибке в политике, которую необходимо пересмотреть.

Преимущество предложенной методики верификации – возможность гарантировать безопасность системы при условии совпадения поведения модели и реальной системы. К недостаткам методики можно отнести: большой объем вычислительных ресурсов, необходимый для анализа сложных моделей; «ложные срабатывания», то есть предупреждения о потенциальных информационных потоках, которых в реальной системе не будет; неполноту, так как проверяется не реальная система, а ее модель.

Работа выполняется при поддержке РФФИ (проекты 13159-офи_м_РЖД, 13-01-00843-а и 11-07-00435-а) и программы фундаментальных исследований ОНИТ РАН.

Десницкий В.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

МЕТОДИКА КОНФИГУРИРОВАНИЯ БЕЗОПАСНОГО ВСТРОЕННОГО УСТРОЙСТВА

Методика конфигурирования безопасного встроенного устройства определяет действия, которые должен выполнить разработчик встроенного устройства при конфигурировании его компонентов защиты. Предварительная стадия методики охватывает действия по анализу спецификации встроенного устройства и моделей нарушителей. Результатом стадии являются списки потенциальных атак на устройство и перечисление свойств программно-аппаратной совместимости.

Стадия формирования требований и ограничений включает определение функциональных требований защиты и задание необходимых типовых шаблонов защиты для каждого требования. Типовой шаблон представляет собой обобщенный алгоритм, реализуемый в виде комплексного компонента защиты и параметризуемый одним или несколькими базовыми компонентами – используемыми криптографическими примитивами.

Применение существующих нормативов и стандартов позволяет среди имеющихся базовых компонентов защиты выбрать те из них, которые отвечают требованиям стойкости и надежности в соответствии с моделью атак и актуальными видами нарушителей встроенного устройства. В соответствии с принятыми регламентами при отборе допустимых компонентов защиты могут учитываться, также, некоторые внутренние решения организации разработчика относительно предпочтительности тех или иных разновидностей аппаратных средств защиты.

Помимо учета требуемого уровня защиты проводится фильтрация базовых компонентов защиты на основе анализа свойств программно-аппаратной совместимости. Ресурсные ограничения устройства определяются, исходя из спецификации устройства и потребностей в аппаратных ресурсах со стороны программного приложения устройства на выполнение его целевых функций. Выходом стадии является формирование списка потенциально возможных конфигураций защиты устройства.

Стадия проведения многокритериального выбора включает определение показателей ресурсопотребления конфигураций защиты с использованием разработанного модуля оценки ресурсопотребления, уточнение эвристики многокритериального выбора, анализ несовместимостей компонентов защиты и осуществление выбора наиболее эффективной конфигурации защиты с использованием программного модуля поддержки принятия решений для выбора конфигураций.

Выбор искомых конфигураций производится с использованием метода лексикографического упорядочения заданных критериев ресурсопотребления. Упорядочивание критериев осуществляется на основе эвристики, определяющей важность аппаратных ресурсов устройства. Использование критериев ресурсопотребления направлено на осуществление наиболее экономного расхода критически важных ресурсов устройства в процессе его функционирования.

Уточнение эвристики производится при необходимости экспертом в области информационной безопасности, и такое уточнение включает добавление в используемую таблицу признаков эвристики каких-либо дополнительных признаков, имеющих существенное значение в контексте ресурсопотребления устройства, а также их ранжирование. Использование эвристики разработчиком устройства включает: выявление релевантных признаков, определение на их основе порядка аппаратных ресурсов устройства и, собственно, осуществление процедуры выбора конфигураций на множестве допустимых конфигураций.

Модуль поддержки принятия решений для выбора конфигураций представляет собой программное средство, запускаемое разработчиком устройства. Данное средство предоставляет пользовательский интерфейс для задания информации об имеющихся компонентах защиты, их свойствах, требованиях со стороны устройства в терминах свойств и ограничений, критериях ресурсопотребления. Результатами работы данного модуля является информация о конфигурации, признанной в качестве эффективной в соответствии с заданными критериями.

Особенностями методики являются выделение ролей эксперта по информационной безопасности и разработчика встроенного устройства в процессе конфигурирования безопасного встроенного устройства и определение согласованных действий для каждой из них, разработка и реализация автоматизированных процедур оценки ресурсопотребления и поддержки принятия решений выбора конфигураций.

Работа выполняется при поддержке РФФИ (проекты 13159-офи_м_РЖД, 13-01-00843-а и 11-07-00435-а) и программы фундаментальных исследований ОНИТ РАН.

Дойникова Е.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ПОДХОД К АНАЛИЗУ ЗАЩИЩЕННОСТИ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ СИСТЕМЫ ПОКАЗАТЕЛЕЙ ЗАЩИЩЕННОСТИ

В настоящее время распределенные информационные системы получают все большее распространение и приобретают все больший масштаб. Сложность таких систем, огромное количество взаимосвязанных сервисов, множество различных событий безопасности, усложняют процесс отслеживания ситуации по безопасности и принятия соответствующих решений по реагированию на инциденты информационной безопасности. Ввиду этого важной задачей информационной безопасности является предоставление лицу, принимающему решения, актуальной и адекватной информации. Такую информацию может предоставить комплексная система показателей защищенности, характеризующих текущее состояние распределенной информационной системы на различных уровнях детализации и с учетом разнообразных воздействующих факторов и возможных мер по реагированию на инциденты информационной безопасности (контрмер).

В данной работе предлагается подход, которыйвключает разработку комплексной системы показателей и соответствующих методик их вычисления, которые позволят учитывать различные характеристики компьютерных атак, а также различные аспекты функционирования защищаемой системы. Такой подход подразумевает использование более сложных алгоритмов вычисления показателей при статическом режиме работы, учет информации о событиях безопасности в режиме, близком к реальному времени, а также быстрый перерасчет показателей на основе новой поступающей информации, что позволит отслеживать направление и уровень сложности атаки, ее цели и характеристики атакующего.

В рамках данной работы были детально проанализированы существующие исследования в области показателей защищенности и выделены следующие основные группы показателей: показатели топологического уровня, вычисляемые на основе данных о топологии и характеристиках элементов системы (в том числе, Уязвимость Хоста, Критичность Хоста, Слабость Хоста и т.п.); показатели уровня графа атак (в том числе, Потенциал Атаки, Ущерб от Атаки и т.п.); показатели уровня атакующего (в том числе, Уровень Навыков Атакующего, Профильный Потенциал Атаки и т.п.); показатели уровня событий (в том числе, Динамический Потенциал Атаки, Динамический Уровень Навыков Атакующего и т.п.); показатели уровня системы (в том числе Уровень Защищенности Системы, Поверхность Атаки и т.п.).

Данная классификация основывается на общем подходе к анализу защищенности, использующем в качестве входных данных: модель защищаемой системы (включающей информацию о топологии системы, информацию о хостах и уязвимостях системы, информацию о сервисах системы и их взаимосвязях), модель атакующего (включающую информацию об уровне навыков атакующего иего положении в системе) и модель атак (представляющую собой множество возможных атакующих действий в виде графа атак).Таким образом, формируются первые три уровня предложенной классификации показателей, соответствующие статическому режиму работы системы анализа защищенности. Однако, в рамках современных систем управления информацией и событиями безопасности (SIEM-систем) важно учитывать развитие ситуации со временем на основе поступающих событий безопасности. Учет данной информации отражается на следующем уровне классификации – уровне событий.Данный уровень соответствует динамическому режиму работы системы.

В зависимости от режима работы системы и уровней вычисления показателей (а значит, и учитываемой при расчетах информации), корректируются методики вычисления показателей.Требующие больших затрат вычисления проводятся в статическом режиме (на первых трех уровнях).

В дальнейшем, в рамках динамического режима, эти данные пересчитываются на основе поступающих событий безопасности.Так, например, в рамках уровня топологических показателей рассчитывается критичность ресурса системы с учетом зависимостей сервисов системы. Это позволяет избежать сложных вычислений на этапе определения ущерба от атаки. Значение вероятности атаки также изначально рассчитывается на основе статических данных о топологии и уязвимостях системы, и затем корректируется в зависимости от знаний об уже осуществленных атакующим действиях и изменении знаний о его навыках.

Данный подход был реализован и протестирован на примере сценария “Олимпийские Игры”.

Работа выполняется при поддержке РФФИ (проекты 11-07-00435-а, 13-01-00843-а) и программы фундаментальных исследований ОНИТ РАН.

Дубенецкий В.А., Цехановский В.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ЗАЩИТА ИНФОРМАЦИИ В КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ УПРАВЛЕНИЯ «РЕСУРС»

Проектирование корпоративной информационной системы (КИС) на современном этапе осуществляется на основе управления жизненным циклом изделия (Product Lifecycle Management – PLM). PLM – это стратегический бизнес-подход и интегрированное решение для коллективной разработки, управления, распространения и использования информации в рамках предприятия и между партнерами от момента формирования концепции до вывода продукции с рынка, объединяющее людей, процессы, бизнес-системы и интеллектуальные активы.

Идеология, методология и информационные технологии поддержки жизненного цикла продукции базирующаяся на представлениях о единой (интегрированной) информационной среде предприятия (отрасли), реализованы в информационной системе управления ресурсами предприятия «РЕСУРС». Наличие единой информационной среды предъявляет повышенные требования к информационной безопасности КИС.

Обязательно должна быть обеспечена система разграничения доступа, которая предполагает определение для всех пользователей автоматизированной информационной системы информационных и программных ресурсов, доступных им для конкретных операций (чтение, запись, модификация, удаление, выполнение) с помощью заданных программно-технических средств доступа.

Уровень полномочий каждого пользователя определяется индивидуально, соблюдая следующие требования:

– открытая, конфиденциальная информация размещаются по возможности на различных серверах (это упрощает обеспечение защиты);

– каждый сотрудник пользуется только предписанными ему правами по отношению к информации, с которой ему необходима работа в соответствии с должностными обязанностями;

– начальник имеет права на просмотр информации своих подчиненных только в установленных пределах в соответствии со своими должностными обязанностями;

– наиболее ответственные технологические операции должны производиться по правилу «в две руки» – правильность введенной информации подтверждается другим должностным лицом, не имеющим права ввода информации.

Аппаратно-программная конфигурация автоматизированных рабочих мест, на которых обрабатывается защищаемая информация (с которых возможен доступ к защищаемым ресурсам), должна соответствовать кругу возложенных на пользователей данного АРМ функциональных обязанностей.

Указанные мероприятия реализованы в принятой архитектуре КИС «РЕСУРС», что позволяет гибко перестраивать конкретные варианты модели предприятия силами группы сопровождения.

Зыков В.М.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

АНАЛИЗ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

В общем случае защита информации техническими средствами обеспечивается в следующих вариантах:

1. Источник и носитель информации локализованы в пределах границ объекта;
2. Соотношение энергии носителя и помех на выходе приемника канале утечки такое, что злоумышленнику не удается снять информацию с носителя с необходимым для ее использования качеством;
3. Злоумышленник не может обнаружить источник или носитель информации;
4. Вместо истинной информации злоумышленник получает ложную.

Эти варианты реализуют следующие методы защиты:

1. Воспрепятствование непосредственному проникновению злоумышленника к источнику информации с помощью инженерных конструкций, технических средств охраны;
2. Скрытие достоверной информации;
3. «Подсовывание» злоумышленнику ложной информации.

Скрытие информации предусматривает такие изменения структуры и энергии носителей, при которых злоумышленник не может непосредственно или с помощью технических средств выделить информацию с качеством, достаточным для использования ее в собственных интересах.

Различают информационное и энергетическое скрытие. Информационное скрытие достигается изменением или созданием ложного информационного портрета семантического сообщения, физического объекта или сигнала.

Возможны следующие способы изменения информационного портрета:

1. Удаление части элементов и связен, образующих информационный узел;
2. Изменение части элементов информационного портрета при сохранении неизменности связей между оставшимися элементами;
3. Удаление или изменение связей между элементами информационного портрета при сохранении их количества.

Метод защиты дезинформированием.

Заключается в трансформации исходного информационного портрета в новый, соответствующий ложной семантической информации.

Различают следующие способы дезинформирования:

1. Замена реквизитов защищаемых информационных;
2. Поддержание версии с признаками, заимствованными из разных информационных портретов реальных объектов;
3. Сочетание истинных и ложных признаков;
4. Изменение только информационных узлов с сохранением неизменной остальной части информационного портрета.

Как правило, используются различные комбинации этих вариантов. Другим эффективным методом скрытия информации является энергетическое скрытие.

Энергетическое скрытие достигается уменьшением отношения энергии (мощности) сигналов, т.е. носителей (электромагнитного или акустического полей и электрического тока) с информацией, и помех. Уменьшение отношения сигнал/помеха возможно двумя методами: снижением мощности сигнала или увеличением мощности помехи на входе приемника.

Воздействие помех приводит к изменению информационных параметров носителей: амплитуды, частоты, фазы. Чем меньше отношение мощностей, а, следовательно, амплитуд, сигнала и помехи, тем значительнее значения амплитуды суммарного сигнала будут отличаться от исходных (устанавливаемых при модуляции) и тем больше будет искажаться информация.

Характер зависимости качества принимаемой информации от отношения сигнал/помеха отличается для различных видов информации (аналоговой, дискретной), носителей и помех, параметров средств приема и обработки сигналов.

В общем случае при уменьшении отношения сигнал/помеха до единицы и менее качество информации настолько ухудшается, что она не может практически использоваться. Для конкретных видов информации и модуляции сигнала существуют граничные значения отношения сигнал/помеха, ниже которых обеспечивается энергетическое скрытие информации.

Так как разведывательный приемник в принципе может быть приближен к границам контролируемой зоны организации, то значения отношения сигнал/помеха измеряются, прежде всего, на границе этой зоны. Обеспечение на границе зоны значений отношения сигнал/помеха ниже минимально допустимой величины гарантирует безопасность защищаемой информации от утечки за пределами контролируемой зоны.

Игнатьев М.Б., Шейнин Ю.Е., Литовкин А.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

НА ПУТИ К ЭКАФЛОПОВСКИМ МАШИНАМ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ – ОТ ЦИФРОВЫХ АНАЛОГОВ ЧЕРЕЗ РЕКУРСИВНЫЕ СТРУКТУРЫ К КВАНТОВЫМ КОМПЬЮТЕРАМ

В период с 1974 по 1979 гг. коллективом ученых Ленинградского института авиационного приборостроения была разработана оригинальная архитектура рекурсивной вычислительной системы, изготовлены многие блоки машины и осенью 1979 г экспериментальный образец рекурсивной машины был предъявлен государственной комиссии во главе с академиком А.А. Дородницыным. В специальном Постановлении ГКНТ СССР и Комиссии Президиума Совета Министров СССР от 14.09.1979 г за №472/276 отмечалось, что запуск первого в мире экспериментального образца многопроцессорной рекурсивной машины высокой производительности

и надежности является достижением мирового уровня. Были предприняты попытки использовать эту вычислительную структуру для решения задач обеспечения информационной безопасности, о чем рассказывается в докладе.

В математике существует большой раздел – рекурсивные функции. Долгое время термин «рекурсия» употреблялся математиками, не будучи четко определенным. Его приблизительный интуитивный смысл можно описать следующим образом. Значение искомой функции Ф в произвольной точке X (под точкой подразумевается набор значений аргументов) определяется, вообще говоря, через значения этой же функции в других точках H, которые в каком-то смысле предшествуют X. Само слово «рекурсия» означает возвращение. Рекурсивные функции – это вычислимые функции. По сути дела все вычислимые на компьютерах функции – это рекурсивные функции, но разные компьютерные архитектуры по-разному ведут вычислительные процессы. Чем лучше соответствует структура компьютера структуре задач, тем меньше затраты памяти и времени. Так что когда мы говорим о рекурсивных машинах, мы говорим о соответствии структур машины и задач, а так как задачи бывают разные, то структура машин должна гибко подстраиваться к структурам задач. Математика в настоящее время погружена в программирование, и в программировании рекурсивные операции распространены.

ЭВМ выступает как средство материализации логико-математических преобразований. ЭВМ являет собой иллюстрацию концепции потенциальной осуществимости, поскольку при отсутствии ограничений на время работы и емкость памяти любая ЭВМ в состоянии провести любые вычисления. Конкретное же протекание процессов вычисления проявляется лишь на уровне организации преобразований информации (задействуются конкретные регистры, коммутаторы, процессоры, линии передачи данных в определенном порядке и сочетании и т.д.).

Когда мы формулировали принципы организации рекурсивных машин, мы исходили из потребностей развития вычислительных машин и систем, получили множество авторских свидетельств. Концепция рекурсивных машин была отражена в докладе на конгрессе ИФИП в Стокгольме в 1974 г. Этот доклад содержал анализ недостатков машин традиционной архитектуры, ревизию принципов фон Неймана, принципы архитектуры рекурсивных машин, основные особенности языка рекурсивных машин, фрагментарное описание рекурсивной машины. В качестве иллюстрации рекурсивной структуры можно привести систему ЗМ – модульную микропроцессорную систему. Система ЗМ строится из модулей трех типов – операционных, коммуникационных и интерфейсных. Операционные модули выполняют основную работу по обработке данных, реализации объектов математической памяти, процессов определения готовности и выполнения операторов программы на внутреннем языке. Коммуникационный модуль предназначен для реализации коммуникационной системы – установления логического соединения между модулями, обмена информацией между модулями, поиска в системе ресурсов запрошенного типа. Интерфейсные модули подключаются к внешним устройствам своими блоками ввода-вывода. Вопросы организации обмена информацией с внешним миром имеют большое значение для существенно многопроцессорных систем, оказывают значительное влияние на их фактические характеристики. Различные классы задач требуют различной интенсивности обмена с внешними устройствами. Вычислительная система должна обеспечивать построение таких ее конфигураций для каждого конкретного применения, которые бы обладали оптимальными для этого применения характеристиками по вводу-выводу. Система ЗМ обеспечивает инкрементное наращивание вычислительной мощности до любого необходимого значения путем подключения дополнительных блоков без внесения изменений в имеющуюся систему и ее программное обеспечение, как на этапе разработки системы, так и в ходе ее эксплуатации. Методология проектирования и реализации системы ЗМ базируется на рассмотрении вычислительной системы как иерархии виртуальных машин. Система ЗМ имеет рекурсивно-организованную многоуровневую структуры. Рекурсивность структуры состоит в том, что структура всякой модификации системы задается рекурсивным определением. Динамически меняющиеся в ходе вычислений виртуальные процессы требуют постоянной динамической реконфигурации связей между модулями. Сейчас реализуются системы, содержащие тысячи и миллионы процессоров.

Интересное направление в развитии элементной базы – квантовый компьютер — гипотетическое вычислительное устройство, которое путём выполнения квантовых алгоритмов существенно использует при работе квантовомеханические эффекты, такие как квантовый параллелизм и квантовая запутанность. Квантовый параллелизм можно реализовать с помощью метода избыточных переменных, а квантовая запутанность реализуется с помощью структуры произвольных коэффициентов. Лингво-комбинаторное моделирование позволяет строить такие системы, базируясь на использовании ключевых слов, основных понятий, сложившихся в предметной области. Модель состоит из трех групп переменных – характеристик основных понятий, изменения этих характеристик и структурированной неопределенности в эквивалентных уравнениях, которая может быть использована для адаптации и управления. Можно построить лингво-комбинаторных модели атомов, которые следует использовать в качестве квантовых вычислителей.

Аналогичным образом возможно построение лингво-комбинаторных моделей всех известных элементов таблицы Менделеева и их изотопов и возможных новых элементов. Это еще один путь для

построения квантовых компьютеров, позволяющий построить экзафлоповские машины, которые будут определять новый уровень информационной безопасности. При этом необходимо решать задачу привязки таких моделей применительно к конкретным системам.

Базовые характеристики квантовых компьютеров в теории позволяют им преодолеть некоторые ограничения, возникающие при работе классических компьютеров. Квантовый компьютер – это разновидность цифрового аналога, цифровое устройство аналоговой природы. Цифровые аналоги активно разрабатывались в 60-е годы в Институте электромеханики АН СССР в Ленинграде под руководством А.А. Воронова.

Игнатьев М.Б., Герасимов Г.М., Липинский Я.А., Макин П.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

АВТОНОМНЫЙ АДАПТИВНЫЙ ШАГАЮЩИЙ РОБОТ ДЛЯ ДИАГНОСТИКИ ГАЗОПРОВОДОВ

Самые различные трубы являются основой современной цивилизации – это и водопроводы, и канализация, и нефтепроводы, и газопроводы и химические производства и энергетика. Трубы изнашиваются, подвергаются коррозии и деформациям и нуждаются в контроле и диагностике для предотвращения аварий. Существует большой арсенал средств для решения этой проблемы, который нуждается в улучшении. Решение этой проблемы возможно лишь в условиях обеспечения информационной безопасности. Предлагаемый и запатентованный нами автономный адаптивный шагающий робот (далее – робот) создан с целью диагностики газопроводов без отключения подачи газа, робот перемещается внутри трубы в потоке газа, откуда и черпает энергию. Робот может перемещаться внутри трубы на многие километры, он не связан проводами с оператором, результаты диагностики сообщаются оператору по беспроводной системе связи.

При создании этого робота были решены следующие проблемы. Во-первых, это проблема энергообеспечения. Все известные нам устройства для контроля и диагностики получают энергию по проводам, что существенно ограничивает их возможности. Мы предложили использовать поток газа для получения необходимой электроэнергии с помощью оригинальной ветротурбины, а в качестве исполнительных устройств использовать оригинальные электромагниты на основе сильных постоянных магнитов, что и позволило нам обеспечить необходимый энергетический баланс. Большинство различных трубопроводов заполнено различными жидкостями, но на период ремонта они освобождаются от жидкостей и туда в качестве энергоносителя может подаваться сжатый воздух, из потока которого наш робот может черпать энергию.

Во-вторых, это проблема адаптации робота при перемещении робота внутри трубы к различным выступам, изгибам и деформациям. Это проблема решена нами путем использования принципа адаптивного шагания. У робота девять ног, башмачки которых поочередно втягиваются или вытягиваются вплоть до соприкосновения со стенками трубы. Активизированные электромагниты ног играют роль магнитных пружин, что и обеспечивает адаптацию к различным выступам, деформациям и изгибам.

В-третьих, это проблема диагностики состояния трубы. На теле робота имеется возможность закреплять различные диагностические устройства, закреплены вэб-камеры с полупроводниковыми светодиодами для освещения внутренней поверхности трубы. Возможно закрепление шесть таких вэб-камер для полного осмотра внутренней поверхности трубы. Вместо вэб-камер можно установить ультразвуковые генераторы и приемники для диагностики тела трубы.

В-четвертых, это проблема передачи информации человеку-оператору. Она решена с помощью использования беспроводной передачи, ведь труба – это хороший волновод.

Таким образом был создан наш робот как оригинальный программно-аппаратный комплекс, позволяющий перемещаться внутри трубы газопровода и взаимодействовать с объектами. Он обеспечивает информационное погружение человека-оператора в среду внутри газопровода с целью его диагностики.

Проведен анализ целей и задач использования робота в индивидуальном и групповом режимах, на основе которого должны быть разработаны сценарии использования робота для диагностики газопроводов различных типов.

Разработана архитектура, состав и режимы работы типового класса роботов, требования к аппаратному, информационному, телекоммуникационному и программному обеспечению, а также к объемно-пространственным характеристикам роботов.

Определен состав стандартных и специализированных программных и аппаратных модулей типового класса роботов с возможностью индивидуального и группового режимов работы. Изготовлен экспериментальный образец робота, испытания которого подтвердили его работоспособность. Робот демонстрировался на Всемирной выставке в Ганновере в апреле 2013 года. Автономный адаптивный шагающий робот существенно пополняет арсенал средств для диагностики газопроводов и повышает их безопасность.

Игнатьев М.Б., Катермина Т.С., Ненашев В.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения*, Нижневартовский государственный университет

ПРОБЛЕМА ПРОГНОЗИРОВАНИЯ ЗЕМЛЕТРЯСЕНИЙ ПУТЕМ МОДЕЛИРОВАНИЯ ДВИЖЕНИЯ КОНТИНЕНТАЛЬНЫХ ПЛИТ

Прогнозирование землетрясений старая, но очень актуальная проблема. На нашей планете во время землетрясений гибнут многие тысячи людей. Прогнозирование землетрясений позволяет уменьшить количество пострадавших. Существует множество гипотез о природе землетрясений, одна из распространенных гипотез связывает источник землетрясений с местами столкновений континентальных плит, которые как бы плавают на поверхности магмы. Сейчас тектоника плит подтверждена прямыми измерениями скорости плит методами интерферометрии и с помощью спутниковых навигационных систем. В докладе рассматривается проблема моделирования движения континентальных плит. Система прогнозирования землетрясений должна состоять из блока моделирования движений континентальных плит, блока измерения реального положения плит и блока учета дополнительных факторов, влияющих на возникновение землетрясений, при условии обеспечения информационной безопасности. Создание реально действующей системы прогнозирования землетрясений требует широкого международного сотрудничества.

Как показывают геологические исследования, расположение материков в прошлом было совсем не такое как в наше время. Континентальные плиты продолжаю двигаться, вызывая землетрясения. Вокруг Тихого океана сформировалось огненное кольцо – зона повышенной сейсмической активности. В докладе рассматривается лингво-комбинаторное моделирование движения континентальных плит (см. М.Б. Игнатьев «Кибернетическая картина мира» Санкт-Петербург, 2010).

Геологи выделяют 8 крупнейших плит, которые покрывают 90% поверхности Земли, среди них плиты – Австралийская, Антарктическая, Африканская, Евразийская, Индостанская, Северо-Американская, Тихоокеанская, Южно-Американская. Имеются еще плиты среднего размера, их значительно больше.

Каждую из плит мы можем рассматривать как отдельное слово и методом лингво-комбинаторного моделирования определить структуру уравнений с произвольными коэффициентами. Эти уравнения задают всю структуру взаимодействий между плитами, всю комбинаторику взаимодействий. Очевидно, что при большом числе плит структура эквивалентных уравнений будет содержать большое количество произвольных коэффициентов, что и определяет трудность прогнозирования землетрясений. Моделирование движения плит является важным направлением исследований.

Каждая из плит имеет свои очертания. Для моделирования движения плит и наглядного представления этих движений в ускоренном масштабе времени каждая из плит представляется как пересечение конуса, прямые образующие которого исходят из центра земли и проходят через границы плиты на поверхности геоида. Так мы можем разместить эти плиты на модели земного шара, и задать движение плит, назначая соответствующие значения произвольным коэффициентам, не задумываясь пока о тех силах, которые влияют на движение плит.

Общая схема прогнозирования землетрясений должна включать блоки моделирования движения плит и блоки измерений положения и скорости реальных плит с помощью спутниковой навигации. Параметры модели должны корректировать по результатам измерений. Чем будет больше точек измерения этих параметров, тем точнее будет прогнозирование землетрясений.

Карпина А.С.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова

ОРГАНИЗАЦИОННОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ НА ПРИМЕРЕ ТРАНСПОРТНО-ЛОГИСТИЧЕСКИХ КЛАСТЕРОВ

В экономической теории под понятием кластера понимают группу взаимосвязанных организаций или компаний, объединенных общностью интересов участников и расположенных на общей территории. Таким образом, они находятся между собой как в отношениях кооперации, так и в отношениях конкуренции. Главной целью такого объединения является повышение конкурентоспособности и экономической эффективности.

Транспортно-логистические кластеры (ТЛК) – отраслевые кластеры, конечным продуктом деятельности которых являются транспортно-логистические услуги в грузовом и (или) пассажирском секторах. ТЛК представляют наземный, воздушный и водный виды транспорта. В состав кластера может входить множество предприятий, специализирующихся на выполнении конкретных рыночных функций. Территория ТЛК определяется как административно-территориальная единица или совокупность сопредельных административно-территориальных единиц.

Организации, находящиеся в составе кластера, постоянно взаимодействуют между собой, грубо говоря, производят обмен информацией. Таким образом, безопасность информации на ТЛК должна осуществляться на внешнем и внутреннем уровнях. Внешний уровень – это защита ИБ самого кластера, внутренний – защита информации каждой организации отдельно.

Говоря об обеспечении информационной безопасности данной экономической структуры, мы должны четко понимать, какая информация является конфиденциальной в рамках конкретной компании, а какая – в рамках самого ТЛК.

Идеализируя модель ТЛК, основываясь на главной идеи кластеров – достижение максимальной эффективности, мы можем составить перечень конфиденциальной информации (КИ) кластера. Например, технические сведения одной организации (используемое оборудование и технологии), в идеальной системе, не должны являться конфиденциальной информацией для другой, потому как, объединение усилий компаний в этой области приведет к развитию и распространению инновационных технологий на территории всего кластера. Однако, нотариальная, налоговая тайны – КИ каждой фирмы.

Еще один аспект, касаемо КИ – это информационная база (база клиентов, поставщиков). На вопрос, нужно ли формировать единую базу ТЛК, нельзя дать однозначного ответа. Такое решение принимают сами организации. Возможно, оптимальным вариантом был бы вариант частично объединенной базы. Когда клиентская база является открытой для всех организаций, в составе кластера, а базы поставщиков – индивидуальны.

Таким образом, говоря об организационных мероприятиях по созданию и функционированию комплексной системы защиты, мы можем упомянуть главные направления деятельности.

Внешние: составление структуры кластера, выявление характера связей между компаниями, организация контрольно-пропускного режима (КПР).

Внутренние: организация КПР, организация ЗИ при проведении совещаний и переговоров, организационные мероприятия по работе с персоналом, порядок приема на работу сотрудников для работы с информацией ограниченного доступа.

Кетов Д.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

ПРОГРАММНЫЕ СРЕДСТВА КОНТРОЛЯ ДИНАМИЧЕСКОЙ ЦЕЛОСТНОСТИ ПРИКЛАДНЫХ ПРОЦЕССОВ В ОПЕРАЦИОННЫХ СИСТЕМАХ ВЫСОКОПРОИЗВОДИТЕЛЬНЫХ МЕЖСЕТЕВЫХ ЭКРАНОВ

Функции современных межсетевых экранов (МСЭ) реализуются в большинстве случаев при помощи программно-аппаратных комплексов на основе встраиваемых операционных систем (ОС) общего назначения, где в силу требований высокой производительности выполняются откомпилированные в код процессора (native) специализированные программы, обычно написанные на достаточно низкоуровневом языке программирования Си. Эти программы исполняется как совокупность ядерных и прикладных процессов под управлением ОС, поэтому необходимость удовлетворения требований руководящих документов (РД) ФСТЭК и ФСБ (по обеспечению целостности программ и процессов МСЭ) приводит к задаче контроля статической целостности программ и динамической целостности ядерных и прикладных процессов ОС.

Согласно ГОСТам целостность информации (ресурсов автоматизированной информационной системы) - состояние информации (ресурсов автоматизированной информационной системы), при котором ее (их) изменение осуществляется только преднамеренно субъектами, имеющими на него право, при этом сохраняются их состав, содержание и организация взаимодействия.

Прикладной процесс многозадачной операционной системы - последовательная смена состояний виртуальной среды исполнения (виртуальная память, регистровый контекст процесса и пр.), происходящих в результате выполнения процессором команд прикладной программы. Таким образом, будем считать программу, выполняемую процессором - единственным субъектом, имеющим право на преднамеренную смену состояний своей виртуальной среды исполнения, а динамическую целостность прикладного процесса предлагается понимать как свойство, при выполнении которого сохраняется порядок выполнения команд, изначально предписанный управляющим графом программы.

При нарушении динамической целостности в смысле нарушения порядка выполнения команд программы, изначально предписанного управляющим графом программы, в большинстве случаев нарушаются естественные правила вызова/возврата подпрограмм. Таким образом, обнаружение нарушения целостности процессов предлагается свести к проверкам соответствия естественным правилам вызова/возврата подпрограмм на графе вызовов подпрограмм (Call Graph, CG).

В качестве программных средств, реализующих механизмы контроля целостности на основе проверок соответствия естественным правилам вызова/возврата подпрограмм предлагается

использовать встраиваемые мониторы (IRM, Inline Reference Monitor), внедряющиеся в текст программы на стадии компиляции.

Внедрение встраиваемых мониторов было реализовано для набора инструментов разработчика программ на языке Си, основанного на GCC версии 4.6 и выше, за счет использования в этом компиляторе многостадийной компиляции, где после стадий препроцессирования и компиляции, и перед стадией ассемблирования обрабатывался полученный ассемблерный текст программы (для архитектуры x86) с целью внедрения встраиваемых мониторов. Обработчик реализован на языке программирования Python, а в число подвергавшихся пересборке программ входили архиваторы gzip и zip, веб-сервер apache и над'ядерная часть FreeBSD 9.1.

В результате исследования снижения производительности программ, подвергшихся внедрению встраиваемых мониторов, обеспечивающих динамическую целостность своих процессов путем проверки правил вызова/возврата из подпрограмм, было выявлено увеличение времени выполнения операций разными программами:

Таблица 1

Увеличение времени операций, при использовании встраиваемых мониторов

Программа	Сжатие	Зашифровка	Пересылка	Увеличение времени
	512Mb случайных данных			
GZIP	+	-	-	менее чем на 1%
ZIP	+	-	-	менее чем на 3%
ZIP	+	+	-	менее чем на 8%
ZIP	-	+	-	менее чем на 15%
APACHE	-	-	+	менее чем на 3%

Полученные количественные оценки накладных расходов, вызванные использованием программных средств обеспечения динамической целостности были признаны удовлетворительными, в результате чего было принято решение о их применении в программном обеспечении межсетевых экранов.

Козина Г.Л., Никулищев Г.И.
Украина, Запорожье, Запорожский национальный технический университет

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ЭЛЛИПТИЧЕСКИХ КРИВЫХ НАД КОНЕЧНЫМ ВЕКТОРНЫМ ПОЛЕМ В СХЕМАХ СЛЕПОЙ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Актуальной проблемой современных цифровых взаимоотношений является выбор надежного механизма проведения электронного голосования. Подобный механизм должен обеспечивать учет и верификацию каждого отданного голоса, а также анонимность голосующего. Поставленная задача может быть решена с использованием схем слепой электронной цифровой подписи (ЭЦП).

В протоколе слепой ЭЦП принимают участие три стороны – подписант, который владеет закрытым ключом; эмитент, которому необходимо подписать документ; верификатор, который использует открытый ключ для проверки подписи под документом. Взаимодействие сторон организуется таким образом, что подписант не имеет доступа ни к содержимому документа, предоставленного эмитентом на подпись, ни к окончательному виду подписи под ним, а верификатор может проверить лишь подлинность подписи под документом, но не принадлежность его эмитенту. При использовании протокола слепой подписи в системе электронного голосования в роли подписанта выступает избирательная комиссия, эмитента – избиратель, верификатора – центральная избирательная комиссия.

В схемах слепой ЭЦП становится возможным особенный тип атаки – нарушение анонимности эмитента со стороны подписанта. Реализация такой атаки в системе электронного голосования позволит избирательной комиссии узнать, за кого отдал голос тот или иной избиратель. Существующие протоколы слепой подписи, предлагаемые различными авторами, на данный момент не стандартизированы, а лишь основываются на принятых стандартах и популярных схемах ЭЦП. Поскольку стандартами гарантируется стойкость подписи только к традиционным для единичной ЭЦП атакам, необходима проверка подобных протоколов на анонимность.

В основе национальных стандартов ЭЦП многих стран мира (например, российского ГОСТ Р 34.10-2012 или украинского ДСТУ 4145-2002) лежит математический аппарат эллиптических кривых (ЭК) над простым или расширенным полем Галуа. Соответственно, операции в группе точек ЭК используются и в большинстве предлагаемых протоколов слепой подписи. Основными недостатками подобных операций являются невозможность распараллеливания и необходимость выполнения трудоемкого деления в поле.

Поскольку ЭК может быть задана над полями Галуа различного вида, то авторами в качестве способа устранения указанных недостатков предлагается использование конечных векторных полей (КВП). КВП представляет собой расширение поля Галуа, элементами которого являются вектора некоторой длины. Основные особенности КВП состоят в использовании меньших чисел в качестве координат вектора с сохранением величины порядка группы точек ЭК и возможности распараллеливания операций над точками ЭК – сложения точек и умножения точки на число.

Криптостойкость протоколов слепой ЭЦП, как и схем, на которых они основаны, обеспечивается вычислительно сложной задачей дискретного логарифмирования в группе точек ЭК. Она не снижается при использовании ЭК над КВП с достаточно большим порядком группы точек.

Исследования авторов показывают, что использование ЭК над КВП в протоколах слепой ЭЦП не нарушает их анонимности. В частности, авторами было предложено и реализовано использование математического аппарата КВП в одной из слепой модификаций российского стандарта ЭЦП. В дальнейшем авторами планируется разработка схем слепой подписи на ЭК над КВП на основе других национальных стандартов.

Козьмовский Д.В., Куватов В.И., Примакин А.И.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

МЕТОДЫ АНАЛИЗА ТРАФИКА В ИНТЕРЕСАХ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И КОНТРОЛЯ СЕТЕВОЙ ДЕЯТЕЛЬНОСТИ ПОЛЬЗОВАТЕЛЕЙ РАСПРЕДЕЛЕННЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

В работе проведена оценка современных методов анализа трафика распределенных вычислительных сетей, направленных на выявления нарушений функционирования сетей и обеспечения безопасности. Показано, что современные методы, в основном, решают задачи технического обслуживания, мониторинга и ошибок функционирования сетей. Предложен метод, позволяющий вести контроль деятельности пользователей сети на основе статического анализа информации в заголовках сетевых пакетов.

Создание автоматизированной системы с возможностями контроля сетевой деятельности распределенных вычислительных сетей является перспективным решением в интересах надежного, безопасного и эффективного функционирования и снижения рисков, связанных опасностями, определяемыми несанкционированной и нештатной деятельностью отдельных элементов системы.

Контроль сетевой деятельности предполагает реализацию систем, задачей которых является анализ и классификацию трафика распределенных вычислительных сетей.

В рамках указанного подхода применяется анализ среднечасовых и среднесуточных показателей трафика. Эти показатели, с одной стороны, довольно полно отражают состояние работы сети, а с другой – более устойчивы, чем исходные данные, съем которых обычно осуществляется с частотой один раз в несколько минут.

Следует отметить большое количество разработанного программного обеспечения, которое позволяет перехватывать и анализировать трафик сети. Их возможности, как правило, позволяют провести сетевой мониторинг, предназначенный для перехвата, хранения, анализа и восстановления различных сетевых событий: сообщений электронной почты, веб-страниц, загруженных файлов, сообщений коммуникационных программ (ICQ/AIM, MSN) и разговоров по IP-телефонии (VoIP). В целом, с помощью таких программ можно определить, какие из приложений выполняются в данный момент, какие пользователи зарегистрировались в сети и кто из них генерирует основной объем трафика.

Кроме того, существуют системы защиты информации (СЗИ), в которых реализован анализ трафика. В данных СЗИ применяется контекстный и сигнатурный анализ, что накладывает ограничения на их использование. Первые – обладают невысоким качеством из-за сложности технической и программной реализации, непросты во внедрении, ресурсоемки и пока их эффективность невысока. Вторые – являются наиболее известными методами классификации и применяются практически во всех современных СЗИ. Однако они не лишены некоторых недостатков, связанных с необходимостью постоянного обновления сигнатур, невозможностью учета данных, сигнатуры которых отсутствуют, отсутствием контроля сетевой деятельности пользователей.

Сводный анализ возможностей СЗИ показал, что большая часть этих систем не имеет возможностей для защиты от утечек информации, инициированных легальным пользователем ИС. Те из них, которые ориентированы на решение подобных задач, находятся на начальной стадии развития, обладают большими требованиями к ресурсам системы и характеризуются высокой сложностью внедрения и использования. Кроме того, отсутствуют реализованные способы контроля сетевой деятельности объектов распределенных вычислительных сетей, несмотря на возможности существующих методов. Предлагается метод анализа данных, содержащихся в заголовках сетевых пакетов в целях классификации по видам сетевой деятельности в интересах задач контроля деятельности пользователей в распределительных информационных системах.

Объединение сетевых пакетов в сеансы происходит по алгоритму формирования сеансов в результате временного анализа сетевого обмена двух узлов вычислительной сети.

Анализ информации, содержащейся в заголовках сетевых пакетов, позволил определить параметры, которые будут участвовать в классификации сетевых сеансов по видам деятельности. Критерием выбора были проверка наличия связи между статистическими параметрами и видами деятельности и проверка взаимонезависимости параметров между собой.

Таким образом, метод классификации трафика по видам деятельности позволяет ввести функцию контроля за сетевой деятельностью объектов распределенных вычислительных сетей,

повышая возможности существующих систем безопасности. Простая реализация метода позволяет произвести легкое внедрение разработок в инструментарий специалиста безопасности при анализе и классификации деятельности абонентов вычислительной сети распределенных информационных систем.

Коноплев А.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

ЗАЩИТА ВЫСОКОПРОИЗВОДИТЕЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ НА ОСНОВЕ АВТОМАТИЧЕСКОГО УПРАВЛЕНИЯ ДОСТУПОМ ЗАДАНИЙ К ВЫЧИСЛИТЕЛЬНЫМ УЗЛАМ

Информационная безопасность в современных высокопроизводительных распределенных вычислительных сетях (РВС) обеспечивается на уровне узлов, образующих такие сети. Однако специфика таких систем, в том числе основополагающий принцип совместного доступа к вычислительным ресурсам и данным пользователей, требует наличия механизмов безопасности, которые бы на сетевом уровне обеспечивали защиту от несанкционированного доступа (НСД) к ресурсам РВС.

Для решения указанной проблемы автором предложен комплексный подход, позволяющий обеспечить защиту ресурсов РВС от НСД путем решения следующих задач:

1. Безопасное распределение запросов пользователей на предоставление ресурсов РВС. Решение данной задачи предусматривает формализацию функции перехода и ее последующую интеграцию в состав провайдеров ресурсов РВС, выполняющих поиск узлов, подходящих для выполнения запросов пользователей. Таким образом, перемещение запросов пользователей происходит только в рамках легитимных узлов РВС и с учетом требований политик информационной безопасности (ПИБ).
2. Верификация требований ПИБ. Позволяет выявлять отношения доступа, приводящие к отклонениям от требований ПИБ. Данная задача решается путем построения модели контроля и управления доступом пользователей в РВС с помощью математического аппарата раскрашенных функциональных сетей Петри и последующего решения задачи достижимости.

Предложенный автором способ безопасного распределения запросов пользователей РВС предполагает, что для выполнения запроса пользователя на предоставление доступа к ресурсам РВС (расположенным на провайдерах ресурсов), необходимо прохождение процедуры взаимной аутентификации и отображение пользователя РВС в предварительно определенный на узлах РВС локальные учетные записи при условии, что такое отображение не создаст отношений доступа, противоречащих требованиям ПИБ. Для этого выполняется учет предустановленных отношений доступа на узлах РВС. Множество предустановленных отношений доступа представляет собой совокупность записей о том, какой тип доступа, каким пользователем РВС и на каком провайдере ресурсов уже предоставлен.

Данное условие формализовано в виде функции перехода в сети Петри, моделирующей исходную РВС. Однако моделирование таких высокораспределенных систем как РВС приводит к проблеме «взрыва» числа состояний, поскольку их количество возрастает экспоненциально с ростом числа узлов РВС. Например, среднестатистические реализации РВС, выполняющих расчет трудоемких задач в научной сфере, содержат более 1000 узлов. Начальная маркировка сети Петри, описывающей такую систему, представляется следующим образом: $M_0 = ([Q_A]_1, \ldots, [Q_A]_Q)$, где $Q_A \subseteq Q$ — количество активных узлов РВС, которые могут инициировать запрос на предоставление ресурсов. Каждый маркер маркировки построенной сети может принимать значение в интервале от 0 до Q_A, при условии, что пользователь РВС не может отправить запрос, не получив результата исполнения предыдущего. Тогда общее число состояний, описывающих такую РВС, — Q_A^Q, что эквивалентно значению 103000. Для решения данной проблемы в работе применяется теория методов частичного порядка и декомпозиции сетей Петри, что позволяет уменьшить пространство состояний модели, описывающей произвольную РВС, до значения $2\sqrt{Q}$.

Задачу поиска узлов, подходящих для выполнения пользовательских запросов, выполняет специальная служба РВС, функционирующая на провайдерах ресурсов. Следовательно, для решения рассмотренной задачи функция перехода должна быть интегрирована в ее состав. Таким образом, при выборе подходящего узла будет учитываться не только их доступность и тип ресурсов РВС, которыми располагает данный узел, но и требования ПИБ, разрешающие или запрещающие использование ресурсов на указанном узле пользователем, инициировавшим запрос.

Предложенный автором способ безопасного распределения запросов пользователей в РВС, реализация указанного программного модуля и его интеграция в составе провайдеров ресурсов позволят реализовать априорный подход к обеспечению защиты ресурсов РВС от НСД, автоматизировать процедуру анализа безопасности РВС, и тем самым обеспечить высокий уровень надежности и безопасности РВС, используемых для построения доверенных информационно-телекоммуникационных систем.

Копыльцов А.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

СОХРАНЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ ДАННЫХ ПРИ ПОДДЕРЖКЕ ПРИНЯТИЯ РЕШЕНИЙ НА ОСНОВЕ ИЗВЛЕКАЕМОЙ СПЕЦИАЛЬНЫМ ОБРАЗОМ ИНФОРМАЦИИ

При поддержке принятия решений важно сохранение конфиденциальности данных, поскольку при утрате важной информации решение может измениться. Построена система моделей и алгоритмов обработки слабо формализованной специальным образом извлекаемой информации, в которой учитывается конфиденциальность данных, поступающих от технических систем и позволяющих осуществлять поддержку принятия решений. Система моделей обработки формализованной информации включает целевые модули: 1. Информация, 2. Распознавание, 3. Классификация, 4. Свертка, 5. Оценивание достоверности полученной информации, 6. Оценивание безопасности полученной информации, 7. Установление связей вновь полученной информации с ранее полученной, 8. Оценивание вероятности, с которой можно доверять вновь полученной информации, 9. Поддержка принятия решения (по каждому классу), 10. Поддержка принятия решения (обобщенная), 11. Число связей, подтверждающих правильность принятого решения, 12. Выработка устойчивой реакции на поступающую информацию и запоминание, 13. Руководство к действию, 14. Хранилище данных. Система работает следующим образом. Информация собирается (модуль 1), распознается (модуль 2) и классифицируется (модуль 3). Информация обрабатывается в каждом классе по определенному алгоритму (модуль 4). Достоверность информации оценивается путем сравнения ее с ранее полученной информацией (модуль 5), производится проверка безопасности информации (модуль 6), устанавливаются связи между вновь полученной информацией в каждом классе и ранее полученной информацией, находящейся в хранилище в модуле 14 (модуль 7), оценивается вероятность, с которой можно доверять полученной информации в каждом классе (модуль 8). Поддержка принятия решений в каждом классе (модуль 9), сбор сгенерированных решений из всех классов и генерация новой совокупности решений в поддержку принятия решения (модуль 10), сравнение принятого решения с решениями, принятыми ранее (модуль 11), выработка устойчивой реакции на многократно поступающую повторяющуюся информацию (модуль 12), генерирование рекомендаций (модуль 13). Модуль 14 включает в себя хранилище информации, поступившей ранее, в модуле путем сравнения вновь записанной информации с ранее записанной в хранилище генерируется новая информация, которая поступает в модуль 1. Таким образом, построена система моделей и алгоритмов обработки специальным образом извлекаемой информации, поступающей от технических систем.

Важными элементом предложенной системы являются модули, ответственные за сохранение конфиденциальности данных, в частности, оценивание достоверности полученной информации о нарушении конфиденциальности данных (модуль 5), оценивание безопасности полученной информации (модуль 6), оценивание вероятности, с которой можно доверять вновь полученной информации о нарушении конфиденциальности (модуль 8). Результат обработки информации в модулях 5, 6 и 8 оказывает существенное влияние на поддержку принятия решений и дальнейшую работу всей системы (модули 9,12,13).

Копыльцов А.В., Сорокин И.В.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена

МОДЕЛИ РАСПОЗНАВАНИЯ ВРЕДОНОСНЫХ ПРОГРАММ НА ОСНОВЕ ЭНТРОПИЙНЫХ ХАРАКТЕРИСТИК

В настоящее время имеется большое количество различных вредоносных программ. Для их обезвреживания разработаны различные подходы. В последние годы существенно увеличилось количество вредоносных программ, в которых используются методы упаковки и запутывания программного кода. Применение известных методов обезвреживания не позволяет эффективно бороться с такими вредоносными программами. Поэтому актуальным является разработка таких подходов (моделей, численных методов и программного обеспечения), которые позволяют это осуществить. Предлагаются математические модели и алгоритмы распознавания упакованных вредоносных программ, на основе анализа энтропийных характеристик файлов, в частности, алгоритм сегментации вредоносной программы, учитывающий энтропийные характеристики файла и алгоритмы распознавания упакованных вредоносных программ, позволяющие оценивать степень похожести файлов на основе их энтропийных характеристик. Апробация предложенных моделей и алгоритмов осуществлялась на упакованных вредоносных программах, представленных в формате Portable Executable для операционной системы Microsoft Windows. Предложена новая классификация методов анализа и распознавания вредоносных программ, использующих энтропийный подход. Предложенная классификация позволила выявить недостатки предлагаемых ранее подходов и найти новые пути решения проблем, возникающих при анализе и распознавании упакованных вредоносных

программ. Разработан новый алгоритм сегментации бинарных файлов, основанный на вейвлет-преобразовании с дискретным изменением параметров масштаба и сдвига базисного вейвлета. Выбор соответствующего типа преобразования обоснован с точки зрения эффективности использования при анализе вредоносных программ. Предлагаемый алгоритм сегментации позволяет проводить поиск границ итоговых сегментов, при минимальных вычислительных ресурсах. Разработано и обосновано новое использование трех способов описания сегментированных участков файлов. Во-первых, учет размера сегмента и его информационной энтропии. Во-вторых, учет частоты появления различных байтов в сегменте. В-третьих, использование нейросетевой модели «неокогнитрон» для запоминания уникального расположения байтов в рассматриваемом сегменте. Каждый из трех подходов позволяет выявлять уникальные характеристики присущие вредоносным программам. Предложен подход, позволяющий представлять файл в векторной форме на основе использования трех способов описания сегментированных участков файлов, что позволяет сравнивать файлы между собой. Разработан новый алгоритм распознавания упакованных вредоносных программ, основанный на взвешенном расстоянии редактирования для последовательностей, состоящих из элементов с двумя числовыми характеристиками: размер сегмента и его информационная энтропия.

Корниенко А.А., Глухов А.П.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения, Москва, ОАО «РЖД»

СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ЖЕЛЕЗНОДОРОЖНОМ ТРАНСПОРТЕ: СОВРЕМЕННОЕ СОСТОЯНИЕ И ЗАДАЧИ СОВЕРШЕНСТВОВАНИЯ

В середине 90-х годов прошлого века началась масштабная информатизация железнодорожного транспорта, в результате чего в отрасли был создан и продолжает разрабатываться и развиваться до сих пор комплекс основополагающих документов и программ, включающих, в том числе, решение проблем информационной безопасности и защиты информации.

Основные тенденции корпоративной информатизации ОАО «РЖД» заключаются в следующем:

1. Переход от информационных и автоматизированных систем к информационно-управляющим системам.
2. Консолидация информационных ресурсов в 3 центрах обработки данных.
3. Интеллектуализация: создание интеллектуального поезда и «умных» объектов инфраструктуры ж.д. транспорта.

Продолжает развиваться и совершенствоваться также и корпоративная система обеспечения информационной безопасности (СОИБ ОАО «РЖД»). Можно выделить следующие этапы и задачи создания и развития СОИБ:

I этап – создание СОИБ (1996 – 2003 гг.) заключается в формировании организационной структуры обеспечения информационной безопасности и защиты информации; разработке концепций обеспечения информационной безопасности корпоративных сетей, защиты информационных ресурсов; разработке профилей защиты и политик информационной безопасности, внедрении средств защиты информации и создании подсистем обеспечения информационной безопасности корпоративных систем и сетей; создании СОИБ ОАО «РЖД».

II этап – создание системы управления информационной безопасностью (2004 – 2008 гг.) заключается в разработке и совершенствовании корпоративной нормативной базы в области информационной безопасности и защиты информации, методического аппарата и системы оценки защищенности (СОЗ), проведении мероприятий по защите персональных данных, разработке корпоративного стандарта по системе управления информационной безопасностью (СУИБ) и типовой политики информационной безопасности дорожного уровня.

III этап – развитие СОИБ и СУИБ (с 2009 г.).

Целями создания системы обеспечения информационной безопасности (СОИБ) российских железных дорог являются:

– Поддержание и обеспечение требуемого уровня безопасности движения, грузовых и пассажирских перевозок, информационной безопасности железнодорожного транспорта в условиях динамичной информатизации отрасли.

– Минимизация или поддержание приемлемого уровня информационных рисков, экономического и других видов ущерба при нарушении безопасности информации.

– Своевременное предоставление пользователям полной и достоверной информации, а также информационных услуг, в том числе по защите информации, не относящейся к категории «государственная тайна».

В целом СОИБ ОАО «РЖД» представляет собой сложную организационно-техническую систему, предназначенную для обеспечения защиты информации и информационной инфраструктуры от воздействий, которые могут нанести неприемлемый ущерб ОАО «РЖД» за счет утраты конфиденциальности, целостности и доступности информации.

Основными задачами, решаемыми в рамках системы обеспечения информационной безопасности российских железных дорог, являются:

– защита информации, не относящейся к категории «государственная тайна»;
– внедрение и эксплуатация технических подсистем, комплексов и средств обеспечения информационной безопасности;
– обеспечение доступности соответствующих категорий информации для пользователей;
– недопущение непроизводственного и непроизводительного использования ресурсов;
– управление, аудит и анализ информационной безопасности ОАО «РЖД».

Корт С.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

АНАЛИЗ ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ GPU ДЛЯ ПОСТРОЕНИЯ СИГНАТУРНЫХ СИСТЕМ ОБНАРУЖЕНИЯ АТАК

Алгоритмы поиска подстроки в строке очень популярны и используются во многих систем обнаружения атак. К примеру, в сигнатурной СОА Snort. Из всех методов обнаружения вторжений, которые проводит Snort, примерно 31% относится к поиску подстроки в строке. У всех подобных систем существуют проблемы с обработкой трафика – недостаточно высокая производительность. С недавних пор GPU стало возможно использовать не только для графических задач, как раньше, но и для решения задач неграфического общего назначения. Основой для эффективного использования мощи GPU в научных и иных неграфических расчётах является распараллеливание алгоритмов на сотни исполнительных блоков, имеющихся в видеочипах. По производительности GPU стал не только не уступать CPU, но и даже показывать значительно лучшие результаты.

В докладе рассматривается использование технологии GPU для построения сигнатурных систем обнаружения атак.

В докладе представлены проведены тесты на производительность центрального и графического процессоров, а также сравнительный анализ полученных результатов. В итоге, поиск на GPU оказался медленнее, чем аналогичный поиск на CPU при малом размере поисковой строки. При большом же размере поисковой строки GPU в несколько раз превосходит CPU. Это происходит вследствие серьезных накладных расходов на операцию копирования из общей памяти в память графической карты.

Как следствие этого положения, для использования в сигнатурных СОА вычислений на GPU у программы должна быть альтернативная архитектура. Возможный подход связан с тем, что, для того чтобы поиск шаблона был равнозначен поиску в большом тексте, необходимо будет «склеивать» пакеты, в одну большую поисковую строку и искать подстроку на GPU уже именно в ней. Если подстрока найдена, то её принадлежность к конкретному пакету будет определяться по индексу. В этом варианте существует проблема со временем – может понадобиться некоторый интервал времени ожидания, пока не наберутся пакеты с нужным общим размером, и вопрос ещё в том, наберутся ли они вообще. Данный подход требует дополнительного исследования.

Котенко И.В., Новикова Е.С.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ПОДХОД К ПОСТРОЕНИЮ СИСТЕМЫ ВИЗУАЛЬНОГО АНАЛИЗА ДЛЯ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ ИНТЕЛЛЕКТУАЛЬНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ЖЕЛЕЗНОДОРОЖНОГО КОМПЛЕКСА РОССИИ

Интенсивное развитие интеллектуальных систем управления перевозочным процессом в железнодорожном комплексе на базе современных цифровых телекоммуникационных и спутниковых технологий приводит к необходимости прилагать значительные усилия по обеспечению необходимого уровня информационной безопасности этих автоматизированных систем.

Эффективность управления безопасностью интеллектуальной системы (ИС) железнодорожного комплекса России может быть повышена путем применения методик визуального анализа данных, которые эффективно сочетают особенности зрительного восприятия человеком графической информации и мощность автоматических методов обработки информации. Большинство существующих инструментов, предназначенных для визуализации данных о защищенности информационной системы, являются узко специализированными, предназначенными для решения конкретных задач обеспечения безопасности. В основном они используют данные определенного формата, полученные от датчика безопасности одного типа (межсетевые экраны, системы обнаружения/предотвращения вторжений и т.д.) и не всегда не всегда учитывают последние достижения в области обнаружения сетевых атак, внутреннего нарушителя и т.д. Из-за этих ограничений и проблем масштабируемости применение этих инструментов в реальном мире для решения оперативных задач часто не представляется возможным. Этот факт обуславливает

необходимость создания расширяемой и масштабируемой платформы для визуального анализа защищенности интеллектуальной системы железнодорожного комплекса России.

В докладе представляется новый подход к построению компонента визуализации системы управления информационной безопасностью ИС, позволяющего выполнять визуальную корреляцию событий, постановку и подтверждение гипотез, а также интерактивное исследование графического представления данных. Основными его отличиями являются: 1) многоуровневый принцип представления информации; 2) адекватное представление большого объема поступающей информации с учетом возможностей человека по ее восприятию; 3) обобщенно-ситуационное отображение параметрических изменений режима процесса; 4) активное привлечение внимания к выявляемым отклонениям в контролируемых данных. При проектировании графических элементов предлагается использовать последние достижения как в области обнаружения сетевых атак, внутреннего нарушения, так и в теории восприятия информации, что позволит повысить скорость понимания и оценки текущего уровня защищенности информационной системе и, в конечном счете, эффективность управления информационной безопасностью.

Масштабируемость и гибкость разрабатываемого компонента визуализации обеспечивается использованием сервис-ориентированного подхода при его проектировании. Кроме того, он позволяет использовать различные графические технологии для реализации графических элементов, и хорошо согласуется моделью графических систем “данные - отображение - вид - управление”.

Предложенная архитектура компонента визуализации состоит из трех уровней: уровень графического интерфейса пользователя, уровень управляющих сервисов, уровень графических элементов и функциональных сервисов, осуществляющих обработку данных. Графические элементы реализуют отображение входных данных и механизмы взаимодействия пользователя с их графическим представлением. Функциональные сервисы выполняют обработку исходных данных, например, осуществляют построение графа атак исходя из заданной конфигурации компьютерной сети и ее хостов. Уровень управляющих сервисов осуществляет взаимодействие между графическими сервисами и функциональными. Он предоставляет стандартный интерфейс по работе с потоками визуализации: создание и остановка графического потока, который реализуется на уровне графических элементов.

Работа выполняется при поддержке РФФИ (проекты 11-07-00435-а, 13-01-00843-а и 13-07-13159-офи_м_РЖД) и программы фундаментальных исследований ОНИТ РАН.

Котенко И.В., Саенко И.Б.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

О ПОСТРОЕНИИ МНОГОУРОВНЕВОЙ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ НА ЖЕЛЕЗНОДОРОЖНОМ ТРАНСПОРТЕ

Автоматизированные информационные и аналитические системы инфраструктуры железнодорожного транспорта образуют многоуровневое информационное пространство и играют важнейшую роль не только для управления железнодорожным движением, но и для обеспечения транспортной безопасности. Однако интенсивное развитие информационных технологий приводит к необходимости прилагать значительные усилия по обеспечению необходимого уровня информационной безопасности этих автоматизированных систем (АС). Наиболее острой проблемой в этой области становится гарантированное обеспечение информационной безопасности АС железнодорожного транспорта (ЖТ) в условиях реализации попыток несанкционированного доступа к ним со стороны как внутренних нарушителей (инсайдеров), так и внешних. На ЖТ данная проблема приобретает особое значение по ряду причин. С одной стороны, реализация угроз информационной безопасности АС транспортной инфраструктуры способна привести к катастрофическим последствиям. С другой стороны, объекты железнодорожной инфраструктуры все интенсивнее оснащаются техническими средствами выхода в глобальные сети (Интернет). Поэтому проблема обеспечения информационной безопасности АС на ЖТ приобретает особую актуальность.

Для ее решения предлагается построение и внедрение в АС на ЖТ многоуровневой интеллектуальной системы обеспечения информационной безопасности. Данная система должна реализовывать принципы не только априорной защиты, которые обеспечиваются криптографическими средствами, средствами аппаратной защиты, межсетевыми экранами, антивирусными средствам и т.д., но и принципы апостериорной защиты, связанной со сбором информации о безопасности и выработкой контрмер на основе ее анализа. Поэтому в качестве основных подсистем многоуровневой интеллектуальной системы обеспечения информационной безопасности предлагается реализовать следующие подсистемы: 1) сбора, предварительной обработки и хранения данных о событиях информационной безопасности; 2) моделирования атак и поведения защищаемой системы; 3) поддержки принятия решений в области обеспечения безопасности; 4) визуального анализа информации о событиях безопасности.

Основными функциями, которые реализуются в подсистеме сбора, предварительной обработки и хранения данных, являются преобразование входных данных во внутренний универсальный формат, их корреляция и хранение. Сбор данных может инициироваться как центром управления, так и оконечными источниками данных. Предварительная обработка информации включает в себя нормализацию, фильтрацию, корреляцию, агрегацию и классификацию данных. Отфильтрованные данные в нормализованном виде хранятся в репозитории (информационном хранилище), являющимся средством кросс-платформенной интеграции различных компонентов. В качестве основы для его реализации предлагается сервисно-ориентированная архитектура. Репозиторий является гибридным онтологическим хранилищем, в котором объединены реляционные, XML- и триплетные базы данных. Последние два вида баз данных используются для поддержания онтологических моделей представления данных об информационной безопасности, что обеспечивает возможность логического вывода и существенно повышает возможности системы по своевременному обнаружению вторжений в АС на ЖТ и выработке адекватных контрмер обеспечения безопасности.

В подсистеме моделирования атак и поведения защищаемой системы осуществляется: моделирование объекта защиты и поведения злоумышленника; генерация (обобщение) общего графа атак; вычисление различных показателей (метрик) безопасности; предоставление всеобъемлющих процедур анализа риска. Основными результатами работы данной подсистемы являются «узкие места» автоматизированной системы и предложения по повышению уровня безопасности, основанные на метриках, политиках и инструментарии безопасности.

В качестве основы для построения подсистемы поддержки принятия решений предлагается использовать модель «контроля доступа, ориентированного на организацию» (Organization-Based Access Control, OrBAC), которая позволяет объединять политики безопасности через различные структурные компоненты организации и автоматически их конфигурировать. Тем самым обеспечивается возможность централизованного управления политиками безопасности, основанного на запросах.

Подсистема визуализации данных призвана обобщать множество отдельных деталей, делая смысл того или иного события и совокупности событий более понятным, и позволяет, используя различные формы, цвета, размеры и взаимное расположение элементов, существенно повысить оперативность восприятия больших объемов воспринимаемой информации.

Работа выполняется при поддержке РФФИ (проекты 13159-офи_м_РЖД, 13-01-00843-а и 11-07-00435-а) и программы фундаментальных исследований ОНИТ РАН.

Котенко И.В., Саенко И.Б., Полубелова О.В., Дойникова Е.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ОНТОЛОГИЯ ПОКАЗАТЕЛЕЙ ЗАЩИЩЕННОСТИ КОМПЬЮТЕРНОЙ СЕТИ КАК ОСНОВА ВЫРАБОТКИ КОНТРМЕР

Анализ защищенности компьютерных сетей является актуальной на сегодняшний день задачей. Его целью является поддержка принятия решений о необходимости повышения уровня защищенности путем реализации защитных мер. Принятие таких решений основывается на показателях защищенности, отражающих такие аспекты как вероятность успешной реализации компьютерных угроз, возможный ущерб для компьютерной сети в случае успешной реализации угроз, уровень риска для отдельных ресурсов сети или сети в целом и т.д.

В области показателей защищенности существует большое количество исследований. Важной задачей является создание комплексной системы показателей, которая позволит принимать адекватные и своевременные решения по реагированию на компьютерные угрозы. В данной работе предлагается решение этой задачи на основе использования механизма онтологий, сформирована онтология показателей защищенности и разработан подход к выработке контрмер на основе логического вывода в рамках предложенной онтологии.

Разработанная онтология показателей защищенности содержит следующие основные элементы: классы, описывающие показатели защищенности; классы, которые характеризуют компьютерную сеть и ее окружение; классы, которые определяют возможные контрмеры и события безопасности.

Основным элементом предлагаемой онтологии являются показатели защищенности, определяемые суперклассом Показатели. В рамках суперкласса Показатели определен ряд подклассов, соответствующих отдельным группам показателей защищенности. Группы показателей защищенности были выделены на основе детального анализа исследований в области и включают: топологические показатели, которые оценивают структурные элементы компьютерной сети (например, Критичность Хоста, Уязвимость Хоста и т.п.), показатели, характеризующие злоумышленника (например, Уровень Навыков Злоумышленника), показатели, характеризующие атаку (например, Потенциал Атаки, Ущерб от Атаки и т.п.), показатели, характеризующие уровень защищенности системы в целом (например. Уровень Защищенности Системы, Поверхность Атаки и т.п.), стоимостные показатели (например, Среднегодовое Ожидание Потерь, Выигрыш при

Реагировании и т.п.) и показатели нулевого дня (например, Вероятностная Мера Уязвимости и т.п.). Связи между суперклассом Показатели и подклассами определяются отношением “класс-подкласс”.

Параметры, характеризующие защищаемую систему (это могут быть хосты, приложения, уязвимости и т.п.) и ее окружение (атаки, злоумышленники и т.п.), являются входными данными для вычисления показателей защищенности. Они определяются классом Система и соответствующими подклассами. Между классом Система и подклассами определены связи “часть-целое”. Кроме того, введены связи между классами показателей и классами, относящимися к системе и ее окружению: связи “характеризует” (означает, что показатель характеризует систему или ее элемент) и связи “оценивается на основе” (означает, что показатель вычисляется на основе данных характеристик системы).

Класс Реагирование также определяет входные данные для вычисления показателей и делится на два подкласса – события безопасности и контрмеры. Отношение между данным классом и классом Показатели определяется связью “оценивается на основе ”.

Кроме того, в работе описывается применение данной онтологии в рамках систем управления информацией и событиями безопасности (SIEM-систем). Она является частью компонента анализа защищенности и выбора контрмер. Отношения между понятиями показателей защищенности и поддержки выбора контрмер определяются исходя из того, что на основе показателей защищенности проводится анализ защищенности, оценка угроз и выбор контрмер. Основные понятия онтологии: Ресурс, Атака, Показатель и Контрмера. Понятие Ресурс определяет защищаемые ресурсы системы. Понятие Атака описывает различные типы атак. Между понятиями Атака и Ресурс введено отношение “атакует”, которое описывает возможное воздействие атаки на ресурсы. Понятие Показатель основано на описанной выше онтологии показателей защищенности. Между понятиями Атака и Показатель введено отношение “влияет”, таким образом, что значения понятия Показатель определяют знания о ходе проведения атаки. Между понятиями Ресурс и Показатель введено отношение “описывает”. Понятие Контрмера описывает различные возможные контрмеры и их характеристики (включая стоимость). Между понятиями Атака и Контрмера введено отношение “применяется”. Далее, на основе правил логического вывода, делаются заключения об атаке (на основе экземпляров показателей атаки); о вовлечении ресурсов в атаку (на основе показателей); о внутренней корреляции показателей; о возможных контрмерах.

Работа выполняется при поддержке РФФИ (проекты 11-07-00435-а, 13-01-00843-а и 13-07-13159-офи_м_РЖД) и программы фундаментальных исследований ОНИТ РАН.

Култышев Е.И., Полонский А.М., Степанов А.Г.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

КЛАССИФИКАЦИЯ СИСТЕМЫ УПРАВЛЕНИЯ ОБУЧЕНИЕМ MOODLE С ПОЗИЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Система управления обучением Moodle представляет собой информационную систему содержащую сведения о персональных данных студентов и учащихся. Поэтому на эту систему распространяются требования федерального закона 152-ФЗ от 27.06.2006 г. «О персональных данных». Проведем классификацию системы управления обучением с позиций требований по информационной безопасности.

Поскольку система Moodle уже разработана и много лет эксплуатируется, на нее распространяются требования совместного приказа ФСТЭК №55, ФСБ №86, Минсвязи №20 от 13 февраля 2008 г. В соответствии с упомянутым приказом система Moodle может быть отнесена к категории 3, поскольку она содержит персональные данные, позволяющие идентифицировать субъекта персональных данных. Хотя в ГУАП система обслуживает более 30000 пользователей, классификация по объему персональных данных относит систему к 3-й группе, поскольку все персональные данные сосредоточены в пределах одной организации.

Система Moodle ГУАП в своей работе предусматривает сбор информации, ее анализ и поддержку принятия решения администрации вуза, порождающего определенные юридические последствия для студента. Однако система не принимает окончательных решений (их принимает преподаватель, кафедра, деканат, ректор) и по этому признаку она может быть классифицирована как типовая. Рассматриваемая информационная система имеет подключения к сетям международного информационного обмена и, следовательно, является распределенной. По режиму обработки персональных данных система управления обучением — многопользовательская. По разграничению прав доступа пользователей — с разграничением прав. Тогда система Moodle в соответствии с упомянутым приказом классифицируется как система класса К3.

Фактически Moodle является автоматизированной системой и, с точки зрения информационной безопасности, к ней могут быть применены требования Руководящего документа (РД) Гостехкомиссии «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». Являясь

многопользовательской автоматизированной системой, Moodle может быть отнесена к группе 1 к классу «1Г» в соответствии с РД. Для полного выполнения требований РД дополнительно требуется очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Поэтому на компьютере – рабочей станции должны быть установлены так называемые «наложенные средства защиты».

ГОСТ Р 50739-95 и Руководящий документ Гостехкомиссии «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации» устанавливают классификацию средств вычислительной техники (СВТ) по уровню защищенности от несанкционированного доступа (НСД) к информации. Анализ показывает, что система управления обучением ГУАП функционирует на СВТ 2-й группы 6 класса. В документации Moodle подчеркивается, что требуется обращать особое внимание на безопасность на любом уровне. Формы и данные проверяются, данные проверяются на достоверность, cookies шифруются и т.д. Однако сколь либо серьезных исследований системы Moodle на безопасность авторам не известны.

Для минимизации последствий угроз, связанных с несанкционированным доступом (НСД) важно иметь в учебном заведении продуманную политику безопасности, и четко ей следовать. Общеизвестно, что в её отсутствие проявляются тенденции к неуправляемому накоплению и расширению полномочий всеми пользователями, в результате если все пользователи будут администраторами, то и система управления обучением будет практически неработоспособна.

Для предотвращения несанкционированного доступа в информационной системе в Moodle определены следующие группы пользователей: Главный администратор; Teacher; Non-editing teacher; Student. Данные группы пользователей необходимо соотнести с категориями реальных пользователей в высшем учебном заведении. Например, Лектор соответствует пользователю группы «Teacher». Ассистент – пользователю группы «Non-editing teacher» В то же время для пользователей Заведующий кафедрой, Методист соответствующая группа пользователей Moodle отсутствует. К функциям пользователя «главный администратор» относится администрирование исключительно программной платформы. Предлагается создать дополнительный механизм администрирования в системе Moodle вуза в виде групп пользователей Выпускающая кафедра, Обеспечивающая кафедра и т.д.

Купреенко С.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

МОДЕЛИ И МЕТОДЫ ОРГАНИЗАЦИИ ПАРАЛЛЕЛЬНЫХ ВЫЧИСЛЕНИЙ ПРИ РЕШЕНИИ ЗАДАЧИ УПРАВЛЕНИЯ ДОСТУПОМ К ИНФОРМАЦИОННЫМ РЕСУРСАМ

В докладе рассматриваются особенности организации параллельных вычислительных процессов, использующих механизмы многопотоковой обработки данных. Для формализации модели вычислений предлагается использовать абстракцию “виртуальное соединение” (ВС), которая используется для формирования характеристической функции доступа к информационным ресурсам. Для вычисления характеристической функции предложен алгоритм, включающий в себя стадии идентификации, буферизации и параллельной обработки данных с использованием высокопроизводительных многоядерных вычислительных систем. В рамках предложенного подхода появляется возможность локализации данных и контекста обрабатываемых виртуальных соединений. На примере межсетевого экрана (МСЭ), работающего в режиме скрытной фильтрации, показана эффективность предложенных решений и возможность повышения производительности и снижения латентности обработки пакетного трафика в нагруженных высокоскоростных компьютерных сетях.

Виртуальное соединение, как некоторая абстракция, существует параллельно и независимо от других виртуальных соединений. Вместе с тем, предлагаемая трактовка термина “виртуальное соединение” для устройств сетевой безопасности имеет смысл только в контексте выполнения процедуры обработки и контроля виртуальных соединений, известной под общим термином “stateful inspection”. В этом случае обработка виртуального соединения есть вычислительный процесс, для выполнения которого требуются такие ресурсы, как ЦПУ и оперативная память.

При переходе к вычислительным системам на основе многоядерных процессоров появляется возможность параллельного выполнения процессов обработки ВС

В предлагаемой модели сочетается как последовательная, так и параллельная обработка сетевого трафика:

– последовательно в отдельном потоке выполняются процедуры идентификации пакетного трафика и балансировки обработки виртуальных соединений (Б);

– параллельно в нескольких потоках выполняется обработка виртуальных соединений, заключающаяся в вычислении соответствующей характеристической функции.

Также следует отметить, что во встроенных многопотоковых приложениях для защиты информации имеют место жесткие ограничения на латентность алгоритмов вычисления

характеристических функций виртуальных соединений, что связано с необходимостью обработки сетевого трафика в темпе работы компьютерной сети.

Предлагаемый метод организации параллельных вычислений основан на использовании характеристической функции булева типа, структура которой представляется конечным автоматом, узлы которого соответствуют структуре обрабатываемого протокола, а переходы определяются обрабатываемыми данными, содержащимися в заголовке обрабатываемого пакета и предикатными соотношениями, описывающими заданную политику безопасности. Структура конечного автомата виртуального соединения представляется гиперграфом, что позволяет учесть контекст вычисления характеристической функции.

Все виртуальные соединения, разбиваются на классы, каждому из которых соответствует своя структура характеристической функции. Класс виртуального соединения определяется структурой протокола прикладного уровня, формирующего виртуального соединения, а структура характеристической функции задается как структурой протокола прикладного уровня, так и выбранной политикой безопасности.

Предложенный подход позволяет в полной мере использовать возможности оценки эффективности организации параллельной обработки виртуальных соединении в соответствии с законами Амдала и Густавсона-Барриса.

Предложенный подход был реализован в прототипе МСЭ, предназначенного для использования на базе высокопроизводительных многоядерных вычислительных систем. Помимо многопотоковой параллельной обработки виртуальных соединений, в данном прототипе также были реализованы все необходимые сервисные функции, присущие МСЭ, такие, как регистрация трафика, авторизация пользователей, контроль целостности программного обеспечения и др.

Проведенные сравнительные тесты производительности МСЭ, использующего многопотоковую параллельную обработку ВС и МСЭ, выполняющего последовательную обработку ВС в однопоточном режиме, позволяют сделать выводы о том, что эффективность параллельной обработки ВС возрастает с ростом нагрузки в защищаемых сегментах компьютерной сети (рост интенсивности сетевого трафика и количества виртуальных соединений) и может достигать 100-150% по сравнению с последовательной обработкой ВС.

Мальцев В.А
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова

АППАРАТНЫЕ СРЕДСТВА, ИСПОЛЬЗУЮЩИЕСЯ ПРИ ПОСТРОЕНИИ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННО-ЗАЩИЩЕННЫЕ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

Современные тенденции развития рыночной экономики и межгосударственных отношений, интеграция Российской Федерации во всемирную торговую организацию требуют от компаний, желающих стабильно оставаться на рынке, создания территориально распределенной структуры бизнеса с учетом региональных и офшорных филиалов (представительств).

Таким образом, при планировании передачи информации в рамках одной кампании следует учитывать трансграничную передачу данных между внутренними и внешними ресурсами. С точки зрения информационной безопасности, следует говорить о совокупности контролируемых зон, соединенных между собой открытыми каналами передачи данных. В случае передачи по этим каналам информации, отнесенной к категории ограниченного доступа, необходимо создавать распределенную вычислительную сеть с дополнительной защитой указанных каналов передачи данных.

Такую защиту возможно осуществить только с использованием сертифицированных ФСБ и ФСТЭК средств защиты. Условно их можно разделить на две группы: аппаратные и программные. Условность деления связана с тем фактом, что аппаратные средства уже содержат в себе программную составляющую, тем самым правильнее их будет называть аппаратно-программными средствами. К таким средствам относятся ViPNet Coordinator HW 100, ViPNet Coordinator HW 1000, ViPNet Coordinator HW 2000, ViPNet Координатор-КВ2, ViPNet Coordinator HW-VPNM, ViPNet Terminal.

Наиболее дешевым в линейке аппаратно-программных средств является ViPNet Coordinator HW 100. Это компактный криптошлюз и межсетевой экран, позволяющий безопасно включить любое сетевое оборудование в виртуальную частную сеть, построенную с использованием продуктов ViPNet, и надежно защитить передаваемую информацию от несанкционированного доступа и подмены.

ViPNet Coordinator HW 100 построен на базе ПО ViPNet Coordinator Linux и выполняет в ViPNet-сети функции ПО ViPNet Coordinator, включая функцию VPN-сервера для доступа удаленных VPN-клиентов, оснащенных ПО ViPNet Client . Помимо относительно невысокой стоимости, это устройство обладает рядом других преимуществ, таких как:

– Алюминиевый корпус с безвентиляторной схемой исполнения и flash-диск вместо обычного жесткого диска, дающий высокие механические показатели надежности.

– Возможность питания от низковольтного источника тока, позволяющую использовать ViPNet Coordinator HW100 в полевых условиях и на подвижных объектах.

– Поддержка работы в современных мультисервисных сетях связи с динамической адресацией и сложным каналообразующем оборудованием.

Следующим в линейке значится ViPNet Coordinator HW1000. Это криптошлюз и межсетевой экран, построенный на аппаратной платформе телекоммуникационных серверов компании «Аквариус». Он легко интегрируется в существующую инфраструктуру, надежно защищает передаваемую по каналам связи информацию от несанкционированного доступа и подмены. Использование адаптированной ОС Linux и надежной аппаратной платформы серверов AquaServer позволяет применять ViPNet Coordinator HW1000 в качестве корпоративного решения, к которому предъявляются самые жесткие требования по функциональности, удобству эксплуатации, надежности и отказоустойчивости:

– Высокая надежность в режиме 24/7/365.

– Количество одновременно установленных соединений через криптошлюз не ограничивается.

– Поддержка работы в современных мультисервисных сетях связи с серверами DHCP, WINS, DNS и преобразованием адресов (NAT, PAT).

– Возможность проведения СИиСП оборудования серверов.

При наличии в организации достаточного количества денежных средств, а так же при необходимости работы в современных мультисервисных сетях связи с динамической адресацией и сложным каналообразующем оборудованием, подключении к различным высокоскоростным каналам связи, наличии системы горячего резервирования используют старшие модели, такие как ViPNet Coordinator HW2000 и ViPNet Координатор-КВ2.

Мальцев В.А.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова

ПРОГРАММНЫЕ СРЕДСТВА, ИСПОЛЬЗУЮЩИЕСЯ ПРИ ПОСТРОЕНИИ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННО-ЗАЩИЩЕННЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

Современные тенденции развития рыночной экономики и межгосударственных отношений, интеграция Российской Федерации во всемирную торговую организацию требуют от компаний, желающих стабильно оставаться на рынке, создания территориально распределенной структуры бизнеса с учетом региональных и офшорных филиалов (представительств).

Таким образом, при планировании передачи информации в рамках одной кампании следует учитывать трансграничную передачу данных между внутренними и внешними ресурсами. С точки зрения информационной безопасности, следует говорить о совокупности контролируемых зон, соединенных между собой открытыми каналами передачи данных. В случае передачи по этим каналам информации, отнесенной к категории ограниченного доступа, необходимо создавать распределенную вычислительную сеть с дополнительной защитой указанных каналов передачи данных. Такую защиту возможно осуществить только с использованием сертифицированных ФСБ и ФСТЭК средств защиты. Условно их можно разделить на две группы: аппаратные и программные. Условность деления связана с тем фактом, что аппаратные средства уже содержат в себе программную составляющую, тем самым правильнее их будет называть аппаратно-программными средствами.

Наиболее распространёнными представителями программных комплексов являются ViPNet Coordinator (Linux) и ViPNet Coordinator (Windows).

В зависимости от настроек ViPNet Coordinator может выполнять следующие функции:

– Сервера IP-адресов;
– Прокси-сервера защищенных соединений;
– Туннелирующего сервера (криптошлюза);
– Межсетевого экрана;
– Сервера защищенной почты.

Отдельного внимания заслуживают программные средства для мобильных устройств. Ни для кого не секрет, что в настоящее время мобильные устройства оказывают все большее влияние на нашу повседневную жизнь. По прогнозу IDC, за 2014-й год будет продано 800 млн смартфонов — на 24% больше, чем в 2012-м, в результате в ближайшие полтора года по количеству выпущенных устройств смартфоны и планшеты почти вдвое превысят персональные компьютеры. В связи с резко возросшим спросом на устройства, растут и угрозы информационной безопасности.

Выходом из такой ситуации могут являться программные продукты ViPNet Client Android и ViPNet Client iOS.

ViPNet Client Android — это приложение, работающее под управлением операционной системы Android, предназначенное для обеспечения защиты устройства от сетевых атак, и позволяющее получить доступ посредством защищенного технологиями ViPNet VPN туннеля, к ресурсам

корпоративной сети. ViPNet Client Android после установки на устройство перехватывает любой IP трафик, обеспечивая его прозрачное шифрование. После активации защитных функций ViPNet Client Android доступ к открытым ресурсам Интернет возможен только с использованием защищенных корпоративных proxy-серверов, доступных через VPN-туннель. Обеспечивается эффективная многоуровневая защита мобильного устройства – антивирусная защита и контентная фильтрация, причем без установки дополнительного программного обеспечения на каждое, что немаловажно, учитывая ограниченные возможности автономной работы мобильных устройств. Для управления функциями ViPNet Client Android используется графический интерфейс, дизайн которого выполнен в стандартах операционной системы Android, существует возможность использовать виджеты на рабочий стол, отображающие текущий статус подключения.

ViPNet Client iOS — это приложение, работающее под управлением операционной системы Apple iOS, предназначенное для обеспечения защиты iPad и iPhone от сетевых атак и позволяющее обеспечить доступ посредством защищенного технологиями ViPNet VPN-туннеля к защищенным ресурсам корпоративной сети. ViPNet Client iOS после установки на устройства iPad и iPhone перехватывает любой IP-трафик, обеспечивая его прозрачное шифрование. После активации защитных функций ViPNet Client iOS доступ к открытым ресурсам Интернет возможен только с использованием защищенных корпоративных прокси-серверов, доступных через VPN-туннель. Этим обеспечивается эффективная многоуровневая защита мобильного устройства — антивирусная защита и фильтрация контента, причем без установки дополнительного программного обеспечения на каждое мобильное устройство, что немаловажно, учитывая ограниченные возможности автономной работы мобильных устройств.

Масюк А.А., Сараджишвили С.Э.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

МЕТОДЫ КАТЕГОРИЗАЦИИ ПОЛНОТЕКСТОВЫХ РЕСУРСОВ В СИСТЕМАХ КОНТЕНТНОЙ ФИЛЬТРАЦИИ

В настоящее время остро стоит вопрос защиты пользователей сети Интернет от нежелательной и вредной для морального здоровья информации. Старые методы цензуры плохо работают в постоянно меняющейся информационной среде, а так же являются недопустимыми с точки зрения законодательства и соблюдения прав и свобод граждан. Возможным решением проблемы является добровольное применение системы контентной фильтрации (СКФ).

Система контентной фильтрации (СКФ) – это технологическое решение, основной задачей которого является предоставление сервиса управления доступом пользователей к ресурсам Интернет. СКФ отвечает за управление доступом пользователей к ресурсам Интернет в зависимости от категории запрашиваемых ресурсов и принятой организационной политики безопасности.

Лидирующие СКФ основываются на принципе анализа и категоризации Интернет-ресурсов, что признано наиболее эффективным методом фильтрации нежелательных данных.

Под категорией понимается группа, к которой может быть отнесён сайт на основе некоторых признаков. Категории представлены иерархическим деревом, а в простейшем случае списком. Категоризация Интернет-ресурсов осуществляется подсистемой тематической категоризации, которая предоставляет данную информацию клиентам СКФ.

На данный момент можно выделить несколько основных методов категоризации ресурсов:

– категоризация данных «налету» в процессе обращения к ним со стороны пользователя;

– использование базы данных категоризированных ресурсов с регулярным обновлением информации о них. Базы данных могут размещаться как локально (на одной машине с фильтрующим модулем), так и на удалённом сервере. Второй вариант обеспечивает модульность и хорошую масштабируемость системы;

– получение информации о содержимом от самого ресурса.

К преимуществам применения предопределенных баз категорий можно отнести то, что предоставление или запрет доступа производится еще на этапе выдачи запроса клиентом, что может существенно снизить нагрузку на каналы передачи данных. А главный недостаток использования данного подхода – задержки в обновлении баз категорий сайтов, поскольку для анализа потребуется некоторое время. Кроме того, некоторые сайты достаточно часто меняют свое наполнение, из-за чего информация о категории, хранящаяся в базе адресов, становится неактуальной.

В ситуации с русскоязычными ресурсами существующие контентные фильтры имеют ряд существенных недостатков, это:

– некорректная работа с русскоязычными ресурсами по причине отсутствия специальных инструментов работы с информацией на русском языке;

– бедность базы данных категоризированных русскоязычных ресурсов.

Методы категоризации ресурсов в большинстве существующих СКФ имеют нелинейную сложность и чрезмерно требовательны к вычислительным ресурсам. По этой причине большинство СКФ не могут категоризировать ресурсы при первом обращении: пользователь получает доступ, а ресурс категоризируется позже.

Во многих случаях методы категоризации требуют участия человека в проверке результатов для обеспечения приемлемого качества. Обычно участие человека в таких системах сводится к исключению из списков ресурсов, положительно категоризированных из-за несовершенства метода категоризации.

Распространённой ошибкой является определение ресурса, как относящегося к категории, на основе единственного термина, встретившегося в тексте, несмотря на то, что ресурс имеет тематику, существенно отличающуюся от тематики категории. Таким же образом ресурс может быть отнесён к нескольким категориям одновременно. В подобных методах проблемой является отсутствие интегрального показателя значимости, который позволил бы правильно соотносить ресурсы и категории.

Модель категоризации, разрабатываемая для перспективных СКФ, должна быть инвариантна языку анализируемых ресурсов. Метод категоризации, лежащий в основе модели, должен иметь линейную сложность и минимизировать участие человека в оценке качества категоризации. Оценка должна быть формализована.

Изложенные основания предопределяют актуальность исследования и разработки СКФ, лишённой перечисленных недостатков.

Михайлов Н.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ВИЗУАЛИЗАЦИЯ КОНТРОЛИРУЕМЫХ ЗОН И ГРУПП ПОЛЬЗОВАТЕЛЕЙ ПРИ АНАЛИЗЕ СТЕПЕНИ ЗАЩИЩЕННОСТИ КРИТИЧНЫХ ДОКУМЕНТОВ ОТ СОЦИО-ИНЖЕНЕРНЫХ АТАК С УЧЁТОМ СТРУКТУРЫ СВЯЗЕЙ МЕЖДУ ПОЛЬЗОВАТЕЛЯМИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

В докладе речь пойдёт о способах визуализации структуры компьютерной сети компании с учётом связей между пользователями информационной системы и их прав доступа к информационным ресурсам. Представлены различные алгоритмы визуализации. Подробнее рассмотрен алгоритм визуализации на графах, внедрённый в программный комплекс для анализа степени защищенности критичных документов от социо-инженерных атак.

Молдовян Д.Н., Мондикова Я.А., Горячев А.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

АЛГОРИТМ КОММУТАТИВНОГО ОТРИЦАЕМОГО ШИФРОВАНИЯ

Алгоритмы отрицаемого шифрования (АОШ) с разделяемым секретом перспективны для использования в качестве специального механизма защиты информации от несанкционированного доступа при передаче сообщений по открытым каналам связи и в компьютерных системах. Данный механизм защиты использует то, что криптограмма может быть расшифрована на двух независимых ключах, приводящих к восстановлению двух независимых осмысленных текстов, которые задаются как входные данные процесса шифрования. При этом на каждом из ключей криптограмма расшифровывается единообразно с использованием одной и той же формулы преобразования, а сама криптограмма неотличима от шифротекста полученного в процедуре вероятностного шифрования. Указанное свойство неотличимости от вероятностного шифрования обеспечивается тем, что криптограмма связывается с так называемым ассоциированным алгоритмом шифрования, который по заданному ключу расшифрования мог преобразовать сообщение, соответствующее этому ключу, в данную криптограмму. Алгоритмы коммутативного шифрования используются для защиты передаваемых по открытым каналам сообщений в случаях, когда между отправителем и получателем сообщения не было произведено предварительное согласование ключа шифрования.

В настоящем сообщении предлагается реализация механизма защиты информации, основанного на объединении свойство отрицаемого и коммутативного шифрования. Данный механизм защиты информации реализуется коммутативными АОШ, которые неотличимы от вероятностного алгоритма коммутативного шифрования по криптограммам, генерируемых получателем и отправителем в процессе выполнения протокола бесключевого шифрования.

Термин отрицаемое шифрование получил свое название в связи с тем, что он относится к таким процедурам шифрования, которые предполагают обеспечение стойкости к так называемым вынуждающим атакам. С последними связывается ситуация, когда атакующий требует предоставить ему ключ расшифрования, а получатель и/или отправитель криптограммы не имеет возможности отказаться от предоставления ключа. Защита обеспечивается тем, что криптограмма

является результатом совместного шифрования двух различных сообщений (истинного и фиктивного) на двух различных ключах (истинном и фиктивном). Атакующему предоставляется фиктивный ключ, на котором он успешно раскрывает фиктивное сообщение. Доказательство наличия еще одного сообщения в криптограмме вычислительно неосуществимо, а сама криптограмма получена с помощью алгоритма вероятностного шифрования, который предоставляется атакующему. Рассматривается как это может быть сделано с помощью алгоритмов коммутативного шифрования.

В сравнении с АОШ, предложенным ранее коммутативный АОШ представляет собой альтернативный вариант реализации механизмов защиты информации, основанных на обманных ловушках. По аналогии с предложенным коммутативным АОШ можно разработать коммутативные АОШ, использующие вычисления над многочленами. Общий механизм, который сохраняется в рамках предложенного подхода является формирование криптограмм, передаваемых по открытому каналу, в виде решения системы двух линейных сравнений, модули в которых являются элементом секретного ключа.

В разработанном коммутативном АОШ используются секретные простые числа *p* и *r*, в качестве модулей, по которым ведутся вычисления. Однако в общем случае можно выбирать и составные секретные модули *p* и *r*, удовлетворяющие условию взаимной простоты. Аналогичное замечание можно сделать и при реализации коммутативных АОШ с использований вычислений над многочленами – секретные многочлены, выбираемые в качестве модулей систем сравнений, должны быть взаимно неприводимыми.

Разрядность модулей *p* и *r* может быть разной, например, модуль, являющийся элементом фиктивного секретного ключа может быть выбран меньшего размера, чтобы направить усилия потенциального нарушителя на раскрытие фиктивного сообщения, в которое можно включить ложные данные.

Для повышения стойкости коммутативных АОШ предлагается включить в них вероятностные механизмы, что приведет к построению вероятностных коммутативных АОШ.

Мондикова Я.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет ЛЭТИ им.В.И.Ульянова (Ленина)

ПОДХОД К СИНТЕЗУ КРИПТОСХЕМЫ С ЗАДАННЫМ УРОВНЕМ СТОЙКОСТИ

Подход к синтезу криптосхем с 80-битовой стойкостью состоит в реализации известных типов криптосхем с открытым ключом, основанных на сложности задачи дискретного логарифмирования (ЗДЛ), над конечным кольцом вычетов по составному модулю $n = rq$, где размер числа r равен 1024 бит, а размер числа q – 512 бит. При таком подходе используется принципиальное существенное отличие ЗДЛ по составному модулю от задачи факторизации (ЗФ) и ЗДЛ по простому модулю. Известные криптосхемы, основанные на ЗДЛ по простому модулю, используются как аналоги, по которым строятся криптосхемы, использующие трудность ЗДЛ по модулю n размером 1536 бит. Последняя задача принципиально отличается от ЗДЛ по простому модулю. Для решения задачи дискретного логарифмирования по составному модулю могут быть использованы общие методы дискретного логарифмирования, имеющие экспоненциальную сложность, и метод сведения к ЗДЛ по простому модулю (имеет субэкспоненциальную сложность) путем факторизации составного модуля и использования китайской теоремы об остатках. Однако в последнем методе требуется вычислить дискретный логарифм по простым модулям r и q. Это показывает, что появление прорывного метода решения ЗФ или ЗДЛ по простому модулю не приведет к взлому криптосистемы, основанной на ЗДЛ по модулю n, один из простых делителей которого имеет длину 1024 бит.

Действительно, если будут найдены прорывные решения задачи факторизации, то ЗДЛ по составному модулю n потребует решения ЗДЛ по простым модулям q и r. Так как размер числа r в два раза больше размера q, то основной вклад в трудоемкость дискретного логарифмирования, в рассматриваемом случае, будет вносить ЗДЛ по простому модулю r. При 1024-битовом размере числа r трудоемкость задачи дискретного логарифмирования по модулю r равна 2 в 80-й степени операций модульного умножения. Это обеспечит 80-битовую стойкость криптосхем, основанных на трудности ЗДЛ по модулю n, даже в случае появления прорывных алгоритмов факторизации. Если будут найдены прорывные решения ЗДЛ по простому модулю, то эти методы смогут быть применены для взлома предлагаемых криптосхем только после решения задачи факторизации по модулю n. Таким образом, для взлома предлагаемых криптосхем потребуется решить как задачу факторизации, так и задачу дискретного логарифмирования по большому простому модулю r. Следовательно, предложенный подход к синтезу криптосхемы с заданным уровнем стойкости обладает существенно более высоким уровнем безопасности в смысле существенного снижения (на многие порядки) вероятности их взлома за счет появления прорывных атак.

Муравьев А.В., Мондикова Я.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и информатизации РАН, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ СЛАБОЙ КРИПТОГРАФИИ

В целях защиты информации от несанкционированного доступа наиболее эффективным методом считается использование криптографических преобразований. Однако в целях предотвращения криминальных действий со стороны правонарушителей в российском законодательстве предусмотрено ограничение, накладываемое на длину ключа, в производящихся, распространяемых и применяемых средствах криптографической защиты информации (СКЗИ).

В настоящее время, разрешены к свободному использованию СКЗИ, реализующие симметричные алгоритмы шифрования, с длиной ключа менее 56 битов, в соответствии с постановлением правительства № 957 от 27 декабря 2007г.

Размер ключа выбран таким образом, чтобы в случае необходимости специальные организации при наличии мощных вычислительных ресурсов смогли получить законный доступ к защищаемой информации, с другой стороны преодоление защиты потенциальными нарушителями является задачей, требующей больших затрат, которая не реализуема с помощью тех вычислительных средств, которыми они обладают.

Слабая криптография предназначена для защиты конфиденциальной и секретной информации при ее порождении. Использование слабой криптографии позволяет повысить защищенность информационного ресурса в целом. На данный момент, использование ключа длиной до 55 бит исключает возможность атаки на основе известных текстов с использованием больших таблиц, которые составляются путем шифрования часто встречаемых значений блоков открытого текста, но развитие техники не стоит на месте. Необходимо учитывать скорые темпы технического прогресса, что позволит при прямолинейном использовании 55 битовой криптографии осуществить угрозу преодоления криптографического рубежа защиты злоумышленником.

Чтобы решить данную проблему, необходимо существенно повысить сложность раскрытия одного секретного ключа и добиться роста сложности раскрытия совокупности ключей пропорционально числу вскрываемых ключей.

В качестве решения данной задачи можно рассматривать применение в криптографической схеме несекретных векторов инициализации, которые передаются вместе с зашифрованным сообщением.

Очевидно, что алгоритм блочного шифрования на фиксированном ключе будет задавать множество подстановок, мощность которого равна 2^|V| , где |V| – битовая длина вектора V. В виду этого, генерация больших таблиц становиться нецелесообразной, поскольку при достаточно большой величине |V| (64 бита) вероятность повтора подстановки достаточно мала, следовательно, ей можно пренебречь на практике. Раскрытие секретного ключа возможно следующими способами:

а) выбор случайного значения ключа (вероятность угадывания ключа равна 2^(-55));

б) поочередный перебор (среднее количество переборов равно 2^55).

Можно предложить следующий механизм, существенно повышающий стойкость алгоритма к «силовым» атакам. Данный подход заключается в генерации расширенного ключа, находящегося в зависимости от короткого секретного ключа и вектора инициализации. После чего расширенный ключ используется для шифрования сообщений. Наличие предварительных вычислений, предваряющих каждый процесс шифрования с данным конкретным ключом, существенно затрудняет «силовую» атаку. Время, требуемое для осуществления атаки можно оценить по формуле T≈2^(k-1) t, где k – длина секретного ключа, t – время предвычислений.

Для проведения атаки за разумное время потребуется очень большие вычислительные мощности с применением большого числа ЭВМ. Для многих приложений значение t равное от 0,5 до 1 секунды, является вполне приемлемым, в виду того, что для законного пользователя данная задержка относиться только к однократно выполняемой инициализации системы. Однако, для нарушителя, даже при меньшей длине ключа, чем 55 бит, время силового взлома будет неприемлемым.

Данные подходы могут послужить основой решений, позволяющих существенно повысить сложность «силовых» атак, при этом контролировать уровень сложности процедуры раскрытия ключа. Решение данной задачи должно способствовать увеличению доверия пользователей к широкому использованию слабой криптографии.

Реализация вышеописанных механизмов позволит задействовать на практике ресурсы слабой криптографии при решении задач защиты информации.

Представляет интерес комбинирование слабой криптографии с алгоритмами отрицаемого шифрования, которое может быть выполнено различными способами и представляет собой интересный механизм защиты информации путем дезинформирования атакующего.

Муравьев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и информатизации РАН

ТЕХНОЛОГИЯ АВТОМАТИЗИРОВАННОЙ ПРОВЕРКИ НАЛИЧИЯ НЕЛЕГИТИМНЫХ ПОЛЬЗОВАТЕЛЕЙ В СИСТЕМЕ

Проверка актуальности сведений о правах пользователей в системе – одна из важных задач при проведении аудита информационной безопасности. Наличие в системе устаревших учетных записей пользователей, например, уже уволенных сотрудников, является потенциальной угрозой для безопасности системы в целом. Таким образом, появляется возможность осуществить несанкционированный доступ (НСД) к данным штатными средствами системы. Потенциальному нарушителю не придется даже выявлять какие-либо уязвимости или пользоваться специальными техническими средствами для осуществления НСД. В виду своей специфики данный вид НСД достаточно сложно детектировать. Во избежание возникновения подобных ситуаций необходимо принять ряд превентивных мер, в первую очередь – организационные меры, цель которых сократить вероятность существования в системе учетных записей пользователей, которые уже не являются сотрудниками организации. В реальных условиях в крупных компаниях дело не ограничивается только одной подконтрольной системой – обычно их несколько десятков, а число пользователей исчисляется тысячами. В виду большого объема обрабатываемой информации не стоит исключать из рассмотрения человеческий фактор, который может стать причиной подобных случаев, как непреднамеренно, так и умышленно.

В связи с этим предлагается использовать технологию автоматизированного аудита легитимных пользователей в системах, используемых внутри организации (под системами здесь подразумеваются системы ведения бухгалтерского учета, службы доступа к VPN, RDP, корпоративная почта и т.п.). Основой данной системы является реляционная база данных, хранящая информацию по каждому сотруднику, и фиксирующая всю историю этого работника в организации: переводы, повышения, увольнение и т.д., а, следовательно, и историю изменения его привилегий в системах, к которым он имел доступ в соответствии со своими служебными обязанностями. Сложность реализации подобной системы заключается в отсутствии у подконтрольных систем единого интерфейса взаимодействия со сторонними программными продуктами. Здесь цель заключается в том, чтобы реализовать модуль ввода данных, как совокупность нескольких подсистем для сбора и обработки данных по пользователям для каждой конкретной системы.

Ввиду данной сложности, ранние механизмы проверки, заключались в написании какого-либо средства сравнения информации в текстовом виде, и заключались в попарном сравнении элементов двух списков. Первый с перечнем всех пользователей, зарегистрированных в системе, и второй, с перечнем уволенных сотрудников. Проще всего программно реализовать подобный механизм с помощью одного из скриптовых языков программирования (php, perl и т.п.). Недостатками подобного метода является недостаточная гибкость к входным данным, слабая возможность масштабирования. Большой объем операций все равно осуществляется вручную – подготовка и форматирование входных данных под единый формат, а также обработка выходных данных. Основным недостатком является то, что такой подход статичен, и подобная реализация не позволяет динамически реагировать на потенциальные нарушения со стороны сотрудников.

Гибкость новому подходу обеспечивают широкие возможности по выборке и обработке данных языка запросов SQL. На ряду, с обширным функционалом систем управления базами данных (например, postgreSQL), появляется техническая возможность отслеживать нарушения в режиме постоянного наблюдения. Реализация интерактивного интерфейса с пользователем (администратором безопасности) позволит динамически создавать правила, которые призваны отслеживать события, потенциально носящие нелегитимный характер, для последующего разбирательства в данном конкретном случае. Такого класса система является не только информационно-советующей, но и системой управления правами пользователей. Например, при возникновении потенциальной угрозы со стороны конкретного служащего, до того как администрация успеет среагировать и разобраться в возникшей ситуации, основная задача системы выявить данного сотрудника и временно заблокировать все его доступы к тем системам, к которым он имеет доступ в соответствии с его прямыми должностными обязанностями.

Предлагаемая технология призвана побороть перечисленные выше недостатки, сократить временные затраты на проведение подобных мероприятий в рамках аудита информационной безопасности и автоматизировать формирование отчетности.

Нестерук Ф.Г.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ТЕНДЕНЦИИ РАЗВИТИЯ АДАПТИВНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Разработка адаптивных систем защиты информации актуальна в связи с прогнозами Gartner, SecurityLab, SmartGrid, и другой достоверной статистикой о растущем спросе крупнейших международных компаний, в том числе и в критически важных инфраструктурах, на современные

системы защиты информации (СЗИ), своевременно и адекватно реагирующие на полный спектр уязвимостей и атак или обладающие необходимой и достаточной новизной под конкретную цель, например, при введении в компоненты системы защиты информации свойств биосистемной аналогии и адаптивности. Прогнозируются следующие тенденции развития систем обеспечения информационной безопасности (ИБ):

– интеллектуализация средств обеспечения ИБ и их интеграция с иными средствами защиты с целью всестороннего анализа состояния защищенности информационных технологий (ИТ);

– переход на защищенные платформы, объединяющие защищенную операционную систему и предварительно настроенную системы обнаружения атак;

– рост числа организаций, занимающихся аутсорсингом средств защиты.

Основным направлением развития информационно безопасных ИТ можно считать создание адаптивных систем защиты информации, удобных для технической реализации с привлечением современных наноэлектронных технологий, ориентированных на высоконадежные механизмы жизнеобеспечения и информационной защиты биологических систем.

Наилучшим сочетанием свойств для достижения поставленной цели обладают нечеткие нейронные сети (НС), которые сочетают достоинства обычной НС и нечеткой логики, опирающейся на опыт экспертов информационной безопасности. Механизм нечеткого логического вывода позволяет использовать опыт экспертов, овеществленный в виде системы нечетких предикатных правил, для предварительного обучения нечеткой НС. Последующее обучение НС на поле известных угроз предоставляет возможность анализа процесса логического вывода для коррекции существующей или синтеза новой системы нечетких предикатных правил систем защиты информации.

Перечислим свойства нечетких НС, необходимые для адаптивных СЗИ:

1) функциональная устойчивость и защищенность элементной базы;

2) возможность классификации угроз;

3) описание соответствия «угрозы – механизмы защиты» в виде системы нечетких предикатных правил,

4) адаптивность нейро-нечетких СЗИ (системы нечетких правил);

5) «прозрачность» для анализа структуры связей нейро-нечетких СЗИ и системы нечетких правил;

6) распределенный параллелизм вычислений.

Фактор времени и управление им также видится как перспективное направление развития СЗИ, в плане разработки модулей синхронизации времени, с двух сторон: со стороны атаки (на входе) и со стороны компонентов адаптивной системы защиты.

Работа выполняется при финансовой поддержке РФФИ (проекты 11-07-00435-а, 13-01-00843-а) и программы фундаментальных исследований ОНИТ РАН.

Нечитайленко Р.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕЖИМЕ ФИЛЬТРАЦИИ ИНФОРМАЦИИ В ТЕРРИТОРИАЛЬНО-РАЗНЕСЕННОЙ СИСТЕМЕ

Для защиты информационных ресурсов и обеспечения оптимальной работы территориально-разнесенной системы необходимо применение комплексной системы информационной безопасности, которая позволит эффективно решать задачи доведения информации разнотипным адресатам в специально организуемом формате данных. В безопасную архитектонику сети закладываются решения конструирования сети и реализации выбранной политики безопасности. Территориально-разнесенная сеть (ТРС) формирует геофизическое пространство в целях сбора, передачи, обработки информации, мониторинга состояния всей сети, ее сегментов и отдельных объектов. Соединить современные технические возможности конструирования и безопасности удалось в среде межсетевых экранов, допускающих одновременное решение задач адресного доведения, организации заданной структуры данных, обеспечения различных степеней скрытности, предотвращения нарушений, потерь и ложных доведений.

Использование межсетевых экранов позволяет организовать внутреннюю политику безопасности ТРС, разделив всю сеть на сегменты (логически или физически обособленную часть системы, наделенную аналитическими и интерфейсными вхождениями в сеть или самоизоляции). Разбиение сети на сегменты осуществляется с целью оптимизации сетевого трафика и повышения безопасности сети в целом. Это позволяет сформулировать основные принципы организации безопасности ТРС (введение категорий скрытности и создание соответствующих им сетевых сегментов; выделение в отдельный сегмент всех внутренних элементов системы; выделение в отдельный сегмент всех элементов системы, которым будет предоставлен доступ к внешних ресурсам; создание выделенных сегментов административного управления и управления

безопасностью; возможность организации многослойности сети; поддержка трафика доведения адресной информации в заданном формате (пакете) данных).

Межсетевой экран пропускает через себя весь трафик, принимая относительно каждого проходящего пакета решение: о возможности его проводки. Решение о фильтрации конкретных форматов и адресов, зависит от принятой в сети политики безопасности. При использовании межсетевого экрана прикладного уровня все соединения проходят через него. Межсетевой экран анализирует содержимое пакета и сопровождающий протокол и определяет, соответствует ли данный трафик правилам безопасности. В случае положительного решения межсетевой экран инициирует новое соединение между своим внешним интерфейсом и системой серверов. Межсетевой экран может изолировать адреса реверсивно расположенных систем. Так как все соединения инициируются и завершаются на интерфейсах межсетевого экрана, внутренние системы сети скрывают схему внутренней адресации ТРС. Выбранная система конструирования ТРС в форме системы межсетевых экранов позволяет достичь должного соотношения технических решений построения трафиков адресного доведения информации разных категорий скрытности, форматирования и протоколирования данных, фильтрации и заданной степени информационной безопасности.

Никифоров О.Г., Стародубцев Ю.И.
Россия, Санкт-Петербург, ОАО «НИИ «Рубин»

О ПРИМЕНЕНИИ МЕТОДОВ МНОГОУРОВНЕВОЙ МНОГОПОЗИЦИОННОЙ ЗАЩИТЫ В ЗАДАЧАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Решение вопросов обеспечения информационной безопасности объектов различного назначения обычно осуществляется по двум направлениям: с одной стороны – это вопросы защиты информации, циркулирующей на этих объектах, а с другой – это вопросы защиты информационной инфраструктуры самих этих объектов. И в первом, и во втором случае на объекте создается система защиты, которая по своим функциональным задачам может быть декомпозирована на пять уровней: уровень непосредственной защиты, уровни обнаружения опасных событий, сбора и обработки информации и принятия решения, а также уровни оперативного реагирования и нейтрализации опасных событий. При этом система может содержать некоторое множество позиций, характеризующихся физическим или логическим размещением средств защиты. Проведенный анализ показал, что при организации информационной безопасности объекта на основе традиционного принципа, базирующегося на создании физических и логических контролируемых зон и контроле за состоянием их безопасности, рассмотренная система защиты может использоваться для решения некоторых задач защиты как инфраструктуры объекта, так и информации, циркулирующей на этом объекте.

Так, в задачах защиты объектов информационной инфраструктуры от физического несанкционированного доступа система защиты использует все пять уровней. На первом осуществляется защита территории и локальных элементов объекта инженерно-техническими средствами защиты. Второй уровень системы обеспечивает своевременное и достоверной обнаружение опасных событий, заключающихся в выходе из строй средств защиты или преодолении их нарушителем. На третьем уровне система идентифицирует опасное событие, после чего принимается решение на противодействие этому событию. Четвертый уровень обеспечивает своевременность действий сил реагирования, а пятый нейтрализацию опасного события путем блокирования нарушителя, либо восстановления отказавших средств защиты.

В задачах защиты информации система защиты может использовать не все уровни. Так, при обеспечении защиты информации от утечки по техническим каналам система может содержать только три уровня: уровень непосредственной защиты, уровень обнаружения опасных событий, заключающихся в спецотказе технических средств обработки информации или средств ее защиты, и уровень нейтрализации опасных событий.

Анализ показал, что построенные на многоуровневом многопозиционном принципе системы защиты могут быть использованы для решения задач защиты информации в средствах вычислительной техники и автоматизированных системах управления от несанкционированного доступа, в задачах защиты информации, передаваемой по каналам и линиям связи и других подобных задачах. При этом для рационального построения таких систем может применяться разработанный унифицированный научно-методический аппарат, позволяющий осуществлять как анализ качества данных систем защиты и оценивание эффективности их применения по назначению, так и оптимальный структурно-параметрический синтез таких систем защиты по критериям минимальных затрат на их построение при условии выполнения требований к их эффективности. Данный научно-методический аппарат позволяет учесть большинство основных параметров и характеристик средств защиты, использующихся для построения системы, таких как их техническая надежность, защищенность от вскрытия средствами разведки, что дает возможность прогнозирования реальных значений параметров вскрытых средств защиты при попытках их блокирования, обхода или других деструктивных воздействиях.

Новикова Е.С.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ВЫЯВЛЕНИЕ АНОМАЛЬНОЙ АКТИВНОСТИ В СИСТЕМЕ МОБИЛЬНЫХ ДЕНЕЖНЫХ ПЕРЕВОДОВ С ПОМОЩЬЮ МЕТОДОВ ВИЗУАЛЬНОГО АНАЛИЗА

Технологическое развитие устройств мобильной связи обусловило появление нового механизма реализации денежных переводов между физическими лицами. Системы мобильных денежных платежей (СМДП) позволяют пользователям совершать различные операции, включая международные и местные денежные переводы между физическими лицами, оформлять кредиты, пополнять депозиты и счета. Особенно востребованы такие системы в странах третьего мира, в которых оплаченное эфирное время стало альтернативным способом оплаты товаров и услуг.

СМДП свойственны риски как традиционных, так и электронных платежных систем: отмывание денег, компрометация персональных данных, мошенничество и т.д. Использование мобильных технологий привносит свои особенности в реализации атак на СМДП, что объясняет необходимость усовершенствования имеющихся методов управления рисками и разработки новых подходов к выявлению нарушений безопасности в системе. Так, например, большинство методик противодействия отмыванию денег ориентировано на обнаружение подозрительных переводов на большие суммы денег. С помощью СМДП злоумышленник может легко обойти существующие схемы, используя несколько мобильных телефонов и выполняя денежные переводы на небольшие суммы.

В докладе представляются методики визуального анализа данных для выявления аномальной активности пользователей.

Ключевыми объектами СМДП для исследования финансовых операций, совершаемых в системе, являются ее пользователи и транзакции. Данные о пользователях системы, включая дату их рождения, адрес проживания, номер мобильного телефона, ассоциированный с ним мобильный счет, а также его роль в СМДП (оператор мобильной связи, розничный продавец услуг мобильной связи, поставщик товаров, конечный пользователь и т.д.) хранятся в системе управления учетными записями. Логи сообщений СМДП содержат сведения о типе транзакции (пополнение мобильного счета или снятие наличных с него, перевод между физическими лицами и т.д.), сумме, статусе, отправителе, получателе, балансе отправителя/получателя до и после транзакции. Важными характеристиками пользователей системы, которые могут быть полезны при выявлении аномальной активности, являются число входящих/исходящих транзакций и их частота.

Денежные потоки в СМДП предлагается представлять в виде ориентированного графа, вершинами которого являются пользователи системы, а дуги – транзакции. Свойства объектов СМДП кодируются при помощи графических атрибутов элементов графа. Например, цвет вершины графа задается ролью пользователя, а ее размер определяется суммой полученных/отправленных денежных переводов за фиксированный интервал времени. Цвет дуги зависит от типа финансовой операции. Процесс исследования данных поддерживается следующими механизмами взаимодействия пользователя с их графическим представлением: 1) подсветка входящих и исходящих связей вершины и соседних с ней узлов при ее выборе; 2) механизм фильтрации данных, позволяющий задавать сложные логические выражения. Кроме того, предусмотрена возможность управлять компоновкой узлов графа на плоскости, что позволяет выделить группы пользователей, обладающих общими свойствами.

В докладе показано, как с помощью разработанного графического представления могут быть выявлены незаконные операции по отмыванию денег, а также пользователи СМДП, чьи мобильные телефоны заражены вредоносным программным обеспечением, осуществляющим денежные переводы на счета злоумышленников без ведома пользователя.

Работа выполняется при поддержке РФФИ (проекты 11-07-00435-а, 13-01-00843-а) и программы фундаментальных исследований ОНИТ РАН.

Парфенов Н.П.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ПОЛОЖЕНИЕ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКА – СОСТАВНОЕ ЗВЕНО СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ПРЕДПРИЯТИЯ

Положение о защите персональных данных работника – это основной документ, регламентирующий технологию защиты персональных данных работника на конкретном предприятии. Данный документ занимает основное место в системе защиты информации предприятия. Как правило, положением определяется порядок получения, обработки, хранения, передачи и любого другого использования персональных данных работника, а также ведения его личного дела в соответствии с трудовым законодательством Российской Федерации.

Положение о защите персональных данных работника - это внутренний (локальный) документ предприятия. Данный документ разрабатывает кадровая служба предприятия. В настоящее время закон не установил строгой формы этого документа, но он должен соответствовать требованиям, которые предъявляет к защите персональных данных работника Трудовой кодекс РФ. Чаще всего, в

положении указываются: цель и задачи предприятия в области защиты персональных данных; понятие и состав персональных данных; в каких структурных подразделениях и на каких носителях (бумажных, электронных) накапливаются и хранятся эти данные; как происходит сбор персональных данных; как они обрабатываются и используются; кто (по должностям) в пределах предприятия имеет к ним доступ; как персональные данные защищаются от несанкционированного доступа; права работника в целях обеспечения защиты своих персональных данных; ответственность за разглашение конфиденциальной информации, связанной с персональными данными работников.

Положение о защите персональных данных работника утверждает руководитель предприятия или уполномоченное им лицо. А вводится в действие этот документ приказом руководителя предприятия. Под персональными данными работника понимаются сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность и содержащиеся в личном деле работника либо подлежащие включению в его личное дело в соответствии с настоящим положением.

В положении персональные данные работника содержат ряд признаков, отличающих их от иных сведений о гражданине, человеке. В положении сосредоточена информация, необходимая именно работодателю и именно в связи с трудовым отношением с конкретным работником. Персональные данные работника, в первую очередь связанные с его трудовой деятельностью, служат основанием для определения его трудоправового статуса, его положения как стороны трудового договора с конкретным работодателем.

Сведения о личности работника, его трудовом пути, семейном положении имеют сугубо персональный характер, относятся только к нему, его жизни и деятельности. Под информацией о гражданах (персональные данные) понимаются сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность. Идентификация личности проводится по сведениям, содержащимся в паспорте. Кроме этого, идентифицировать личность позволяют и дактилоскопические данные. Данные сведения необходимы работодателю, чтобы заключить трудовой договор, заполнить личную карточку №Т_2, помочь работнику в обучении, продвижении по службе, обеспечить его личную безопасность, контролировать количество и качество выполняемой им работы. Персональные данные относятся к конфиденциальной информации, то есть, к которой нет свободного доступа. При этом необходимо иметь ввиду, что объявить персональные данные общедоступными только внутри предприятия даже с согласия субъектов персональных данных нельзя. Работодатель в лице руководителя организации либо его представитель обеспечивает защиту персональных данных работников, содержащихся в их личных делах, от неправомерного их использования или утраты.

До сих пор не решен вопрос, являются ли сведения о деловых и личных качествах работника персональными данными. Комментируя закон «О защите персональных данных» мы приходим к выводу, что деловые и личные качества работника не являются персональными данными, и в свою очередь данным законом не охраняются. Если бывший работодатель сообщает сведения, порочащие честь и достоинство бывшего работника, то работник может воспользоваться судебной защитой чести, достоинства и деловой репутации.

В заключение доклада хотелось бы отметить, что при разработке положения о защите персональных данных необходимо стремиться к тому, чтобы распространить данное положение на широкий спектр работников с учетом их персональных данных.

Перервенко А.В.
Россия, Санкт-Петербург, ЗАО «АСИС»

АДАПТАЦИЯ КОРПОРАТИВНОЙ МЕТОДИКИ ОЦЕНКИ РИСКОВ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РС БР ИББС-2.2-2009 ДЛЯ КРУПНЫХ КРЕДИТНЫХ ОРГАНИЗАЦИЙ

Действующим стандартом Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (СТО БР ИББС-1.0) с целью создания и поддержания на должном уровне системы обеспечения информационной безопасности (СОИБ) организаций банковской системы (БС) Российской Федерации определено требование проведения оценки рисков нарушения информационной безопасности (ИБ).

Методика РС БР ИББС-2.2-2009 устанавливает рекомендуемые способы и порядок проведения оценки рисков нарушения ИБ организации БС РФ, являющейся составной частью системы менеджмента ИБ (СМИБ) организации БС РФ.

В результате анализа рекомендаций РС БР ИББС-2.2-2009 можно выделить следующие особенности их применения:

1. Методика оценки рисков, предложенная в рекомендациях РС БР ИББС-2.2-2009, является двухфакторной, а, следовательно, наилучшим образом применима для организаций с низким уровнем зрелости в вопросах ИБ. В тоже время методика распространяется и на организации банковской системы, уровень зрелости которых достаточно высок. Следовательно, для повышения

качества, достоверности и повторяемости результатов оценки рисков в таких учреждениях целесообразно применять трехфакторную модель оценки рисков.

2. В соответствии с п. 5.6.2 и 5.7.2 рекомендаций РС БР ИББС-2.2-2009 при привлечении к оценке возможности реализации угрозы или степени тяжести последствий нескольких экспертов и получении разных экспертных оценок рекомендуется итоговую, обобщенную оценку принимать равной экспертной оценке, определяющей наибольшую величину. Такой подход не представляется оптимальным.

3. Для оценки рисков нарушения ИБ в количественной форме перевод качественных оценок степени возможности реализации угроз ИБ и степени тяжести последствий от потери свойств ИБ осуществляется с использованием рекомендуемых шкал. При этом для конкретного качественного значения указан диапазон количественных значений, но каким образом выбрать конкретное значение из этого диапазона не определено.

Следовательно, для более эффективного применения рекомендаций РС БР ИББС-2.2-2009 в условиях крупных кредитных организаций с высоким уровнем зрелости ИБ целесообразно решить следующие задачи:

– Рассмотреть возможность применения трехфакторной модели оценки рисков, то есть при расчете риска учитывать также оценку уязвимости. При этом для проведения качественной оценки уязвимостей должны быть разработаны специальные, адаптированные к условиям крупной, имеющей большую филиальную сеть, кредитной организации списки вопросов и соответствующая матрица оценки рисков. Предложения по оценке уязвимостей и оценке рисков подготовить на примере методики CRAMM.

– Подготовить предложения по проведению экспертных оценок – выбрать методы оценки субъективных вероятностей.

– Предложить методы агрегирования экспертных оценок.

Для оценки уязвимостей в настоящее время наиболее распространен подход, основанный на учете различных факторов, влияющих на уровни уязвимостей. Он позволяет абстрагироваться от малосущественных технических деталей, принять во внимание не только программно-технические, но и иные аспекты. По косвенным факторам предлагаются вопросы и несколько фиксированных вариантов ответов, которые «стоят» определенное количество баллов. Итоговая оценка угрозы и уязвимости данного класса определяется путем суммирования баллов. Такой подход используется в методе CRAMM.

В рамках работы подготовлены вопросы для оценки уязвимостей, связанных с угрозой несанкционированного копирования конфиденциальной информации, как сотрудниками организации, так и посторонними лицами.

Подготовлена матрица оценки рисков ИБ и получены практические результаты ее использования.

Для решения задачи по повышению объективности и качества экспертных оценок рассмотрены методы оценки субъективных вероятностей и методы агрегирования оценок.

В целом применение подходов и принципов, изложенных в докладе, позволит повысить аналитическую и системную эффективность решения задачи оценки рисков ИБ в крупных организациях БС РФ с высоким уровнем зрелости ИБ.

Пичугин Ю.А., Фаткиева Р.Р.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена, Санкт-Петербургский институт информатики и автоматизации РАН

КОСВЕННЫЕ ПРИЗНАКИ КОМПЬЮТЕРНОЙ АТАКИ НА ОСНОВЕ СПЕКТРАЛЬНОГО АНАЛИЗА СЕТЕВОГО ТРАФИКА В РАЗРАБОТКЕ СРЕДСТВ ИНФОРМАЦИОННОЙ ЗАЩИТЫ

Благодаря простоте и эффективности, сетевые атаки DDoS представляют собой одну из самых значимых угроз для Web-сервисов. Задача обнаружения несанкционированного доступа к информационным системам предполагает проведение исследований по определению косвенных признаков наличия или отсутствия атаки. Одним из наиболее перспективных направлений исследования представляется спектральный анализ сетевого трафика, который позволяет изучить структуру исходных данных и выявить скрытые поведенческие характеристики системы, что может быть полезно для построения систем проактивной защиты от атак.

Моделирование DDoS-атак различных видов с дальнейшим анализом спектральных характеристик входящего и исходящего трафика показало возможность использования наиболее информативных метрик, позволяющих идентифицировать атаку. Применение метода сингулярного спектрального разложения (анализа главных компонент) показывает, что появление DDoS-атаки любого вида сказывается на поведении главных компонент достаточно явно. Например, для SYN-flood первая главная компонента всех метрик (тренд) изменяется скачкообразно во время начала DDoS-атаки, а 4 следующие главные компоненты имеют всплески во время начала атаки с последующим снижением амплитуды и, соответственно, дисперсии. Компоненты, начиная с шестой,

представляют собой высокочастотные шумы. Для некоторых метрик они также характеризуются уменьшением дисперсии после начала атаки.

Исходя из результатов численных экспериментов, определены метрики, дающие реакцию на любой вид компьютерной атаки. Все анализируемые метрики разбиты на группы в зависимости о реакции на тип атаки. При этом установлено, что на атаку типа SYN flood реагируют все метрики без исключения.

На основании проведенных исследований можно сделать вывод, что спектральные характеристики входного трафика, несомненно, могут быть использованы в качестве индикаторов (косвенных признаков) для обнаружения компьютерной атаки и открывают перспективу разработки системы обнаружения несанкционированных вторжений. Система перехватывает IP-трафик с помощью библиотек операционной системы, в реальном времени рассчитывает значения приведённых выше метрик и выполняет разложение на главные компоненты. Принимать решение о наличии атаки можно, анализируя скорость изменения первой главной компоненты (тренда), анализируя дисперсию следующих главных компонент и фиксируя в них всплески амплитуды сигнала.

Примакин А.И.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ПОЛИТИКА БЕЗОПАСНОСТИ, КАК КЛЮЧЕВОЕ ЗВЕНО СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ХОЗЯЙСТВУЮЩЕГО СУБЪЕКТА

Политика безопасности – это формальные правила, по которым должны действовать лица, программы и технические устройства при действиях с информацией. Из практики известно, что правильная политика безопасности даже без выделенных средств защиты дает лучшие результаты, чем средства защиты без политики безопасности.

Политикой безопасности можно назвать и простые правила использования ресурсов (уровень руководителей), и описания всех соединений и их особенностей (уровень инженерно-технического состава). В докладе рассмотрена только зона ответственности руководителя хозяйствующего субъекта в формировании политики безопасности, прежде всего, планирование защиты информационной системы. Именно участие руководителя, а не только технических специалистов, в разработке политики безопасности позволяет учесть целесообразное и выверенное, с точки зрения конкретных функциональных обязанностей, распределение информации.

Действия по управлению сложными организационно-техническими системами должны быть спланированы. Планирование информационной безопасности начинается после проведения анализа рисков и выбора средств защиты информации в соответствии с их ранжированием. Планирование – это процесс разработки пакета руководящих документов по реализации избранной политики информационной безопасности.

Политика информационной безопасности определяет облик системы защиты информации – совокупности правовых норм, организационных (правовых) мер, комплекса программно-технических средств и процедурных решений по рациональному использованию вычислительных и коммуникационных ресурсов, направленных на противодействие угрозам с целью исключения (предотвращения) или минимизации возможных последствий проявления информационных воздействий.

Политика безопасности должна гарантировать, что для каждого вида проблем существует ответственный исполнитель. В связи с этим ключевым элементом политики безопасности является доведение до каждого сотрудника его обязанностей по поддержанию режима безопасности.

Другими словами, защита информации начинается с постановки и решения организационных вопросов. Те, кому уже приходилось на практике заниматься вопросами обеспечения информационной безопасности в автоматизированных системах, отмечают следующую особенность – реальный интерес к проблеме защиты информации, проявляемый менеджерами верхнего уровня, на уровне подразделений, отвечающих за работоспособность автоматизированной системы, сменяется на резкое неприятие.

Как правило, приводятся следующие аргументы против проведения работ и принятия мер по обеспечению информационной безопасности:

– появление дополнительных ограничений для пользователей, затрудняющие использование и эксплуатацию автоматизированной системы организации;

– необходимость дополнительных материальных затрат как на проведение таких работ, так и на расширение штата специалистов, занимающихся проблемой информационной безопасности.

Экономия на информационной безопасности может выражаться в различных формах, крайними из которых являются:

– принятие только организационных мер обеспечения безопасности информации;

– использование только дополнительных технических средств защиты информации.

В первом случае, как правило, разрабатываются многочисленные инструкции, приказы и положения, призванные в критическую минуту переложить ответственность с людей, издающих эти

документы на конкретных исполнителей. Естественно, что требования таких документов (при отсутствии соответствующей технической поддержки) затрудняют повседневную деятельность сотрудников организации и, как правило, не выполняются.

Во втором случае, приобретаются и устанавливаются дополнительные технические средства. Их применение без соответствующей организационной поддержки только усиливает существующий беспорядок.

В докладе рассматривается комплекс организационных мер (в рамках политики безопасности), необходимых для реализации защиты информации в компьютерных сетях. С одной стороны, эти меры должны быть направлены на обеспечение правильности функционирования механизмов защиты и выполняться администратором безопасности системы. С другой стороны, руководство организации, эксплуатирующей средства автоматизации, должно регламентировать правила автоматизированной обработки информации, включая и правила ее защиты, а также установить меру ответственности за нарушение этих правил.

Рудакова С.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ВЫБОР МЕТРИК ДЛЯ ПРОВЕДЕНИЯ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В основе аудита информационной безопасности (ИБ) лежит оценка метрик ИБ. Поэтому выбор метрик – важный этап оценки защищенности. Применяемые сегодня методы аудита ИБ различны: проверка соответствия требованиям стандартов, оценка рисков ИБ, оценка динамики развития системы ИБ и другие. Как правило, эти методы аудита работают с уже готовыми наборами метрик: они могут задаваться стандартами или составляться экспертами. В случае если набор метрик ИБ является неполным или избыточным, результаты аудита могут оказаться некорректными. В связи с этим разработка методики выбора метрик, обеспечивающей отсутствие избыточности и неполноты метрик, является актуальной на сегодня задачей.

Предлагается осуществлять выбор метрик ИБ не готовыми наборами, а по уровням, начиная от общего верхнего уровня «Безопасность информации» и разделяя каждую метрику текущего уровня на более детализированные метрики следующего уровня, причем количество детализированных метрик предлагается делать как можно более маленьким, 2–5 метрик. При появлении у аудитора возможности объективно оценить текущую метрику, детализацию текущей метрики предлагается прекратить.

При детализации метрик ставятся следующие задачи:

– минимизация неполноты набора метрик;
– минимизация избыточности набора метрик.

Выполнение второй задачи (минимизация избыточности) обуславливается выбором метрик непосредственно перед проведением аудита ИБ, т.е. для конкретного объекта информатизации, а не для широкого круга типичных объектов.

Для выполнения первой задачи (минимизация неполноты) в процессе детализации метрик предлагается руководствоваться следующим правилом: совокупность детализированных метрик должна быть составлена таким образом, чтобы:

– невозможно было удалить хотя бы одну детализированную метрику так, чтобы характеристика метрики более высокого уровня не изменилась;
– невозможно было добавить хотя бы одну детализированную метрику так, чтобы характеристика метрики более высокого уровня изменилась;

То есть, совокупность детализированных метрик должна быть необходима и достаточна, чтобы полностью характеризовать метрику более высокого уровня.

Таким образом, можно построить граф, корнем которого будет свойство информации «безопасность», а листьями – метрики, оцениваемые в ходе аудита ИБ.

Помимо поиска метрик ИБ такой граф также может быть полезен при составлении выводов о степени защищенности информации: при поиске метрик мы двигаемся по графу «сверху вниз» (от корня к листьям), а при наличии оцененных метрик – «снизу вверх» (от листьев к корню), что позволяет сделать вывод о безопасности в целом, основываясь на отдельных метриках.

Рыжков А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ПОДХОД К ВЕРОЯТНОСТНОМУ КОДИРОВАНИЮ СООБЩЕНИЙ ТОЧКАМИ ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

Использование вычислений на эллиптической кривой (ЭК) с целью выполнения процедур шифрования представляет интерес в связи с тем, что при правильном выборе ЭК обеспечивается экспоненциальная стойкость, что позволяет существенно уменьшить размер чисел, над которыми

выполняются операции умножения по модулю, за счет чего повышается производительность алгоритмов шифрования.

При шифровании обычно предполагается, что любое сообщение, размер которого не превосходит некоторое заданное значение, может быть корректно зашифровано и расшифровано, т.е. на входные значения не накладывается ограничений. Однако не все значения конечного поля, над которым задана ЭК, могут быть абсциссами точек ЭК. Распространенным подходом для разрешения данной сложности является выбор некой базовой точки ЭК и представление кодируемого сообщения точкой ЭК через умножение сообщения на выбранную базовую точку.

Эффект вероятностного шифрования (когда исходный текст при шифровании с использованием одного и того же ключа может преобразовываться в различные шифртексты) достигается, например, наложением случайно сгенерированной последовательности на результат шифрования и передачи информации для снятия этой последовательности вместе с зашифрованным сообщением.

В предлагаемом подходе размер кодируемого сообщения выбирается на h бит меньше размера поля ЭК и при кодировании к сообщению, интерпретируемому как часть абсциссы точки ЭК, присоединяются справа (или слева) h случайных битов. Полученное значение принимается за абсциссу и проверяется существование точки ЭК с данным значением абсциссы. Если такой точки на используемой ЭК не существует, присоединяются новые случайные h битов и проверка повторяется. Вероятностная составляющая достигается случайным выбором присоединяемой последовательности, соответственно одному кодируемому сообщению могут соответствовать различные точки ЭК.

Для определения оптимальной длины добавляемой случайной последовательности необходимо разрешить следующие два вопроса:

– вероятность, что некоторое заданное сообщение не удастся закодировать точкой ЭК;

– вероятность существования во всем множестве исходных сообщений сообщения, которое невозможно закодировать.

Первый вопрос рассматривает вероятность, что не существует такой комбинации h случайных битов, при присоединении которой к заданному сообщению, возможно получить абсциссу точки ЭК. Для оценки этой вероятности P можно использовать формулу $P = 0{,}5H$, где $H = 2h$. Второй вопрос связан с оценкой вероятности существования хотя бы одного сообщения длиной μ бит, которое невозможно закодировать точкой ЭК. Оценка сверху этой вероятности не превосходит значения произведения числа возможных μ-битовых сообщений и вероятности отсутствия кодирующей точки для одного сообщения.

При длине случайной добавляемой последовательности h в 9 бит и более значение обоих вероятностей пренебрежимо мало. С использованием представленного подхода вероятностного кодирования была разработан алгоритм коммутативного шифрования на ЭК. Получаемая криптограмма представляет собой точку ЭК, которая может быть представлена в сокращенном виде, когда указывается абсцисса этой точки и дополнительный бит, позволяющий однозначно вычислить ординату по известной абсциссе. Криптограмма в сокращенном виде имеет размер незначительно больший, чем размер исходного сообщения (не более 7%). По сравнению с известными АКШ обеспечивается повышение быстродействия при одновременном повышении стойкости, причем обеспечивается экспоненциальная стойкость.

Представляет интерес использования в рамках предложенного способа коммутативного шифрования ЭК, заданных над двоичными конечными полями, что позволит упростить используемую процедуру вероятностного кодирования. Детальное рассмотрение этого вопроса представляет собой тему дальнейшей работы.

Рыжков А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ВЫБОР ПАРАМЕТРОВ ДЛЯ ПОСТРОЕНИЯ «ИДЕЛЬНЫХ» АЛГОРИТМОВ КОММУТАТИВНОГО ШИФРОВАНИЯ

Алгоритмы коммутативного шифрования (АКШ) применяются для решения ряда специфических задач информационных технологий, таких как построение протоколов бесключевого шифрования, электронной жеребьевки и игры в покер по телефону.

В ряде важных для практики случаев АКШ используются в криптографических протоколах, в ходе которых возникают условия, когда потенциальный нарушитель знает исходное шифруемое значение и получаемую из него криптограмму и пытается вычислить секретный ключ. Стойкость АКШ обеспечивается вычислительной сложностью задачи дискретного логарифмирования (ЗДЛ) в используемой циклической конечной группе.

Для АКШ актуальным вопросом является обеспечение достаточно малой вероятности существования сообщений, имеющих малое значение порядка или имеющих порядок, не содержащий ни одного большого простого делителя. В алгоритмах коммутативного шифрования, основанных на трудности ЗДЛ в простом конечном поле GF(p), эта проблема решается соответствующим выбором простого числа p. Для практического использования таких алгоритмов коммутативного шифрования это является достаточным. Однако теоретически идеальным случаем синтеза алгоритмов коммутативного шифрования над ЗДЛ является получение значения большого простого порядка для всех возможных значений шифруемых сообщений. При построении АКШ с использованием вычислений в поле GF(p) принципиально невозможно получение большого значения порядка для всех возможных значений шифруемых сообщений. Это связано с тем, что в таких полях всегда присутствует элемент, имеющий порядок, равный двум.

В настоящей работе решается задача синтеза «идеального» коммутативного шифра, основанного на трудности ЗДЛ. Для этого используются вычисления в конечном двоичном поле и вычисления на идеальной эллиптической кривой (ЭК).

Под идеальным коммутативным шифром понимается такой АКШ, для которого все возможные сообщения имеют большой простой порядок, равный порядку используемой циклической группы. Использование групп с простым значением порядка связано с тем, что наличие сравнительно малых простых делителей порядка позволяет подобрать сообщения, по криптограмме которых можно получить существенную информацию о ключе, применяя для решения ЗДЛ способ, известный как метод больших и малых шагов

Двоичные многочлены, заданные над полем GF(2) и имеющие степень, не превышающую значение $s - 1$, образуют поле двоичных многочленов GF(2s) при задании операции умножения многочленов по модулю неприводимого двоичного многочлена $\eta(x)$ степени s. Известно, что мультипликативная группа любого конечного поля является циклической. В случае поля двоичных многочленов GF(2s) порядок мультипликативной группы равен $q = 2s - 1$. Если выбрать такое значение s, что число q окажется простым, то все двоичные многочлены поля GF(2s) будут иметь порядок q. Наиболее простая реализация протокола связана с использованием вычислений в поле двоичных многочленов GF(2s), порядок мультипликативной группы которых q равен простому числу вида $2s - 1$ (числа Мерсенна). Числа такого вида являются простыми, только при определенных простых значениях s.

В настоящее время представляют интерес для практической реализации разработанного алгоритма следующие шесть значений s: 1279, 2203, 2281, 3217, 4253, 4423, поскольку при их использовании достигается приемлемый компромисс между стойкостью и производительностью.

Другим способом реализации идеального коммутативного шифра является его построение с использованием вычислений на ЭК простого порядка. Данный способ также представляет большое разнообразие вариантов построения идеальных АКШ.

Соколов С.С., Карпина А.С.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова

УМЕНЬШЕНИЕ ВЕРОЯТНОСТИ РЕАЛИЗАЦИИ УГРОЗЫ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ТРАНСПОРТНО-ЛОГИСТИЧЕСКИХ КЛАСТЕРОВ МЕТОДОМ СТРУКТУРНОГО СИНТЕЗА ИНФОРМАЦИОННЫХ ПОТОКОВ

Транспортно-логистический кластер представляет собой административно-территориальную единицу или совокупность административно-территориальных единиц, представленных в виде организаций или компаний, объединенных общностью интересов участников, конечным продуктом деятельности которых являются транспортно-логистические услуги в грузовом и (или) пассажирском секторах.

В информационных системах транспортно-логистических кластеров обрабатываются различные виды информации: служебная тайна, коммерческая тайна, персональные данные сотрудников, поставщиков, покупателей.

Вся эта информация отличается необходимым уровнем защиты и, как следствие, может быть категорирована с учётом мероприятий, средств и методов применяемых для ее защиты. После проведения категорирования информации следует произвести ее технический анализ на предмет выявления общности подходов к защите по программно-техническим, организационным и другим аспектам. Основные цели анализа:

1. Снижение уровня издержек с сохранением требуемого уровня защищенности.
2. Минимизация вероятности реализации угрозы.

Под структурным синтезом информационных потоков будем понимать их техническую рекомбинацию, выполненную посредством использования программно-технических средств, с целью построения новой структуры потоков, отличающуюся большей общностью и группировкой по определенным заранее категориям.

На данном этапе развития средств автоматизации моделирования и проектирования задача структурного синтеза, как правило, решается вручную, в интерактивном режиме составляется модель технического объекта, по которой в дальнейшем производятся расчёты.

Уменьшение вероятности реализации угрозы методом структурного синтеза происходит за счет уменьшения степени вхождения максимальной величины рисков в числитель расчетной величины вероятности при постоянном (априорно определенном) значении знаменателя, который отражает полную группу событий.

Супрун А.Ф.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

МЕТОДИКА ОЦЕНКИ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ОТ УТЕЧКИ ИНФОРМАЦИИ ЗА СЧЕТ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ

Прогресс в области обработки информации связан с широким внедрением вычислительной техники и электронных устройств передачи информации. Эксплуатация систем обработки и передачи информации сопровождается значительным побочным электромагнитным излучением (ПЭМИ), содержащим сведения об обрабатываемой информации. Активные методы подавления таких излучений затрудняют проведение разведки информации и снижают вероятность ее получения на 40…50%.

Оценка эффективности таких систем обработки информации может определяться по различным методикам. Однако с достаточной для практики точностью, задача оценки эффективности защиты данного канала утечки может быть решена с использованием следующей методики.

Используя технические средства мониторинга побочных электромагнитных излучений и наводок (ПЭМИН), применительно к конфигурации определяются излучающие «точки» и радиусы распространения информативного сигнала. Полученные инструментальным методом зоны излучения наносятся на план выделенного помещения. Зона возможного распространения информативных сигналов аппроксимируется одной из фигур (квадрат, эллипс, круг).

Из состава номенклатуры средств защиты, приведенных в справочниках, или прайс-листах отечественных производителей выбираются (один или несколько) удовлетворяющих требованиям по техническим характеристикам (ТХ) и стоимости.

Определяются размеры зон подавления, а затем с использованием стандартных процедур или методом прямого перебора находятся рациональные точки установки источника ПП, при которых обеспечивается выполнение определенного условия.

Таким образом, могут быть определеныоптимальные места установки ПП и их количество для любых вариантов расположения ИП.

Чечулин А.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ПРИМЕНЕНИЕ АНАЛИТИЧЕСКОГО МОДЕЛИРОВАНИЯ ДЛЯ ПОВЫШЕНИЯ УРОВНЯ ЗАЩИЩЕННОСТИ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Одной из актуальных проблем является разработка методологических основ обеспечения безопасности информации в распределенных информационных системах. В настоящее время информационные системы используются во всех областях – от повседневной жизни до управления критически важными инфраструктурами, и поэтому решение этой проблемы является одной из приоритетных задач, решаемых органами государственного, регионального и местного управления во всех развитых государствах мира. В данном исследовании предполагается повысить уровень защищенности распределенных информационных систем за счет разработки нового подхода к аналитическому моделированию. Реализация предложенного подхода позволит производить анализ защищенности компьютерной сети и, как следствие, рекомендовать оператору способы изменения параметров системы защиты этой сети за ограниченное время. Кроме того, система, основанная на результатах данного исследования, должна учитывать события безопасности, происходящие в реальном времени. С помощью разрабатываемой методики предполагается достичь значительного повышения уровня защищенности компьютерных сетей, обеспечить возможность манипулировать информацией о безопасности и осуществлять проактивное управление инцидентами и событиями безопасности. Система защиты информации, основанная на предложенном подходе, должна обладать способностью успешно решать следующие задачи: получение информации о реальном уровне защищенности информационных, телекоммуникационных и других критически важных ресурсов; проведение обоснованного анализа и управление рисками безопасности защищаемой компьютерной сети (в том числе своевременное устранение или снижение рисков безопасности); обнаружение несоответствия реального уровня защищенности важных ресурсов требуемому уровню, определяемому внутренними политиками безопасности, и приведение их в соответствие друг с другом; принятие эффективных решений по защите информации.

Основная задача исследования заключается в разработке моделей, методик и алгоритмов, позволяющих осуществлять управление параметрами защиты компьютерной сети с точки зрения выполнения требований к защищенности. В настоящее время существует множество подходов к анализу защищенности компьютерных сетей, позволяющих скорректировать параметры системы защиты. Большая часть этих подходов основана на комплексном анализе текущего состояния элементов компьютерной сети и не учитывают их возможные изменения. В отличие от существующих решений, предлагаемый подход основан на аналитическом моделировании защищаемой системы и субъектов, стремящихся нарушить защиту. Он позволит учитывать не только текущий уровень защищенности, но и принимать во внимание возможные изменения этого уровня в случае появления в системе нарушителей, обладающих различными начальными правами, знаниями, опытом и т.д. Для обеспечения этого, предполагается использовать методы итеративного моделирования, то есть формировать модели защищаемой сети для различных последовательностей действий нарушителя. Кроме того, важной научной задачей является оптимизация процесса аналитического моделирования, так как время, необходимое для построения моделей в существующих решениях, является главным препятствием для использования подобного подхода для систем защиты, работающих в режиме, близком к реальному времени. Несмотря на то, что для компьютерных сетей небольшого размера анализ поведения системы защиты и субъектов, производящих атакующие действия, может быть произведен достаточно быстро и с незначительным объемом использованных ресурсов, построение и анализ моделей для увеличивающихся сетей может привести к существенному росту требуемого времени и ресурсов. Рост сложности моделей приводит и к увеличению количества ошибок в результатах анализа защищенности, в результате чего возникает необходимость разработки нового комплекса моделей, алгоритмов и методик оперативного построения и анализа аналитических моделей. Для решения этой задачи предложена методика, позволяющая формировать, модифицировать и анализировать аналитические модели за заданное время. Для этого использовались методы теории оптимизации, интеллектуального анализа данных, эволюционного моделирования, онтологического представления знаний и т.д. Данная методика должна лечь в основу разработки системы защиты от сетевых атак, которая: 1) базируется на анализе моделей атак; 2) использует большое количество разнородных входных данных для оперативного построения моделей атак; 3) позволяет обнаруживать слабые места и проверять эффективность контрмер.

Работа выполняется при поддержке РФФИ (проекты 11-07-00435-а, 13-01-00843-а) и программы фундаментальных исследований ОНИТ РАН.

Шерстюк М.Ю., Воронков К.Л.
Россия, Санкт-Петербург, ЗАО «Институт инфотелекоммуникаций»

ОСОБЕННОСТИ ВЕДЕНИЯ ЭЛЕКТРОННЫХ МЕДИЦИНСКИХ ПЕРСОНАЛЬНЫХ ЗАПИСЕЙ

С развитием информационных технологий все большее количество медицинских учреждений переходит на электронный документооборот. Полный переход на ведение электронной истории болезни и отказ от привычной бумажной карточной системы повышает качество оказаний медицинских услуг и увеличивает пропускную способность поликлиники, больницы или другого медицинского учреждения.

Система электронного ведения истории болезни должна базироваться на ряде нормативных документов, основным из которых является ГОСТ Р 52636-2006 «Общие положения о ведении истории болезни». В рамках этого документа даны рекомендации по созданию медицинской системы, в которой любые медицинские сведения, составляющие, по сути, электронную историю болезни пациента, введенные медицинским персоналом, – являются электронными персональными медицинскими записями (ЭПМЗ) в этой системе.

Любая созданная ЭПМЗ включает в себя небольшой набор необязательных и обязательных сведений, основными из которых являются сами формализованные медицинские сведения, отражающие один из этапов медицинского обследования пациента, а также сведения о лице, подписавшем ЭПМЗ. Подписание ЭПМЗ юридически эквивалентно традиционному подписанию заключения или диагноза на бумаге, поэтому за неправильность введенных медицинских сведений о пациенте сотрудники учреждения должны нести ответственность в рамках закона РФ в зависимости от тяжести повлекшихся за собою последствий.

Весь жизненный цикл ЭПМЗ включает в себя пять этапов: создание, ведение, подписание, хранение с возможностью доступа к ней заинтересованных лиц и, наконец, уничтожение по истечению срока хранения.

При использовании системы электронного ведения истории болезни должен выполняться ряд требований:

– сведения, составляющие ЭПМЗ, должны быть неизменны и достоверны на протяжении всего периода хранения;

– должен существовать механизм обеспечения конфиденциальности сведений;

– должен существовать механизм аутентификации пользователей, деление их на группы по признаку разделения прав и полномочий в системе;

– в любой момент времени для любой ЭПМЗ должен существовать механизм определения автора записи, даты подписания записи.

В отношении ЭПМЗ необходимо выработать нормативную базу, обеспечивающую их правовой статус и эффективное использование в медицине и здравоохранении, как это сделано в отношении традиционной медицинской документации.

В медицинском учреждении, использующем систему электронного ведения истории болезни, в отношении ЭПМЗ должен быть создан специальный документ «Политика безопасности» (ПБ). Этот документ должен состоять из двух частей – открытой и закрытой.

В открытой части ПБ должна содержаться следующая информация:

– сведения о мерах безопасности, использующихся для обеспечения сохранности, неизменности и достоверности ЭПМЗ;

– сведения о лицах, ответственных за обеспечение безопасности и прав доступа в системе;

– сведения о лицах, имеющих особые права в системе с указанием меры их ответственности.

Закрытая часть ПБ должна содержать описание технических методов и средств обеспечения безопасности и предоставляться только органам по сертификации или иным компетентным органам по решению суда.

Шоров А.В., Чечулин А.А., Котенко И.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

КАТЕГОРИРОВАНИЕ ВЕБ-САЙТОВ ДЛЯ СИСТЕМ БЛОКИРОВАНИЯ ВЕБ-САЙТОВ С НЕПРИЕМЛЕМЫМ СОДЕРЖИМЫМ НА ОСНОВЕ АНАЛИЗА ТЕКСТОВОЙ И ГРАФИЧЕСКОЙ ИНФОРМАЦИИ

Сегодня Интернет является одним из основных способов получения информации. Отсутствие механизмов, классифицирующих информацию и регулирующих доступ к ней в сети Интернет, создает проблему получения нежелательной информации определенным кругом лиц. В частности, здесь подразумевается ограничение доступа к определенным видам информации детей. Кроме того, существует проблема защиты пользователей от различного вида вредоносного и нежелательного программного обеспечения, распространяющихся с помощью веб-сайтов, принадлежащих к определенным категориям.

Современные веб-сайты имеют сложную структуру и состоят из множества элементов, которые могут содержать информацию, которая кардинальным образом может отличаться друг от друга. Это обуславливает ряд проблем для решения задачи категоризации веб-страниц, заключающихся в разнородности информации, ее огромных объемах и постоянной изменчивости. Для решения задачи категоризации веб-сайтов необходимо учитывать ряд особенностей, на которые необходимо обращать внимание при реализации системы, а именно: 1) огромный массив данных, хранимых в Интернете, снижает эффективность их обработки, и, кроме того, он постоянно увеличивается; 2) типичный веб-сайт имеет сложную многокомпонентную структуру, что обуславливает необходимость применения разнообразных методов анализа и объединения результатов.

Можно выделить несколько этапов, необходимых для категоризации веб-сайтов. На первом этапе выполняется непосредственная загрузка содержимого определенной веб-страницы с помощью ее URL, первичная обработка и хранение. Структура веб-страницы (здесь подразумевается страница, сформированная с помощью кода HTML) содержит теги, формирующие представление веб-страницы с помощью браузера. Некоторые теги могут использоваться для выделения особо важной информации, которую необходимо представить пользователям или роботам, обслуживающим поисковые системы. Одним из основных типов данных, использующихся для категоризации веб-сайтов, является текстовая информация. Использование текста для обучения классификаторов вносит ограничения на язык веб-сайтов, категоризацию которых предполагается выполнять. Поэтому для классификации сайтов на иностранных языках предлагается использовать перевод текстового содержимого сайта с языка оригинала на язык, использовавшийся для обучения классификаторов. Использование изображений для классификации веб-сайтов также создает определенные трудности, т.к. зачастую изображения могут содержать различный информационный шум в виде накладываемого текста, изобразительных эффектов или быть рекламного характера, не имея отношения к анализируемому веб-сайту.

На втором этапе используются методы машинного обучения для получения классификаторов, необходимых для формирования системы категоризации веб-страниц. Используя данные, полученные на предыдущем этапе, производится создание списков основных ключевых слов по определенным категориям на основе следующих структурных компонентов веб-страниц: текст веб-страницы, видимый пользователю; текст, содержащийся в тегах, наиболее часто использующихся для выделения основной тематики сайта; URL веб-сайта. Происходит выделение свойств графической информации, необходимых для формирования классификатора по изображениям.

Далее производится обучение атомарных классификаторов по заранее сформированному списку категорий. После этого производится объединение атомарных классификаторов с помощью верхнеуровнего классификатора, который принимает решение о принадлежности сайта к той или иной категории, основываясь на мнении классификаторов нижнего уровня. Результатом данного этапа является обученная модель, которую можно использовать для категоризации неизвестных веб-сайтов.

В настоящий момент авторами разработан инструментарий, позволяющий автоматизировать процесс формирования обученной модели на основе списка URL-идентификаторов сайтов с заранее определенными категориями, а также инструмент, позволяющий категорировать неизвестные веб-сайты с помощью обученной модели. Средняя точность классификации по таким категориям, как порнография, наркотики, алкоголь, табак, оружие, азартные игры, свидания, культы, насилие и ненависть, составляет около 84%.

Для работы с предложенными схемами принятия решения, проведения собственных экспериментов и расширения потенциально успешных паттернов классификации используются два основных внешних программных пакета: Jsoup 1.7.1 и Rapid Miner 5.3.

Работа выполняется при поддержке РФФИ (проекты 11-07-00435-а, 13-01-00843-а) и программы фундаментальных исследований ОНИТ РАН.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Аверьянов Е.Г.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПРОЦЕССОВ МАРШРУТИЗАЦИИ В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ

Одной из особенностей развития телекоммуникаций на современной этапе является широкое внедрение сетей передачи данных, развертываемых с применением различные проводных и беспроводных технологий. Наиболее привлекательной для клиентов и, следовательно, перспективной с точки зрения развития бизнеса является сеть, предоставляющая широкий спектр телематических услуг при высокой надежности и хороших вероятностно-временных характеристиках процесса обмена. Достижение таких характеристик вынуждает операторов связи объединять свои сети и заключать договора о пропуске трафика. В этой ситуации обеспечение безопасности сетевых взаимодействий является актуальной задачей. В настоящее время практически невозможно говорить об абсолютной защищенности телекоммуникационных сетей, речь может идти о требуемом достаточном уровне. Под достаточным уровнем защищенности можно понимать такое состояние сети, при котором вероятность деструктивных воздействий уже мала, а применение средств защиты ещё не ухудшает качество предоставляемых сетью услуг. При дальнейшем увеличении уровня защищенности произойдет снижение вероятностно-временных характеристик процесса доставки сообщений, а часть из них вообще могут не доставляться получателю.

Применение средств обеспечения безопасности телекоммуникационных взаимодействий должно применяться на всех уровнях ЭМВОС. Одним из примеров таких взаимодействий на сетевом уровне ЭМВОС является решение задачи маршрутизации в сетях передачи данных. Основными протоколами динамической маршрутизации, широко используемыми в сетях, являются протоколы OSPF и BGP различных версий. Особенностью алгоритмов, лежащих в основе их работы, является обмен служебной информацией со всеми доступными маршрутизаторами и последующий расчет оптимальных маршрутов. В этих условиях не всегда есть возможность проверить надежность маршрутизаторов, участвующих в обмене. Таким образом возникает потенциальная возможность осуществления деструктивных воздействий. Для исключения возможности ввода ложной информации в таблицы маршрутов целесообразно доработать маршрутизаторы, оснастив их индивидуальными электронными подписями. В этом случае каждое устройство будет принимать и обрабатывать маршрутную информацию только от «разрешённых» устройств, чьи образцы подписей есть в памяти устройства. Кроме того, передача маршрутной информации может передаваться в зашифрованном виде, что исключит возможность перехвата информации злоумышленниками.

Другим элементов обеспечения безопасности телекоммуникационных взаимодействий является организация виртуальных туннелей между сетевыми устройствами. В настоящее время для этого используются различные протоколы, например, PPPoE (Point to Point Protocol over Ethernet – протокол двухточечного соединения через Ethernet). Такие протоколы имеют возможность выполнять шифрование данных с применением механизмов коммерческого шифрования. Для повышения безопасности обмена целесообразна замена существующих алгоритмов шифрования на алгоритм ГОСТ.

Применение указанных средств совместно с другими механизмами, позволит существенно повысить безопасность телекоммуникационных взаимодействий.

Авраменко В.С.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного

СТРАТЕГИИ УПРЕЖДАЮЩЕЙ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

Под стратегией защиты информации от несанкционированного доступа (НСД) понимается общая, рассчитанная на определенный период времени руководящая установка на организацию и выполнение мероприятий по защите информации от НСД, определяемая в зависимости от предстоящих (складывающихся) условий функционирования (ситуации).

В качестве основных стратегий защиты информации от НСД в современных телекоммуникационных сетях можно выделить оборонительную, наступательную и упреждающую. В критических телекоммуникационных сетях (с высокими требованиями по защите информации), функционирующих в условиях высокой степени неопределенности угроз безопасности информации и

динамики их реализации, целесообразно использовать стратегию упреждающей защиты, направленную на предотвращение нарушения защищенного состояния информации. Мероприятия по упреждению нарушений должны проводиться в сроки, учитывающие как временные характеристики возможных нарушений, так и процесса защиты (время, необходимое на выбор (разработку), доведение и реализацию упреждающих мероприятий по защите). В зависимости от возможностей системы защиты могут использоваться следующие варианты стратегии упреждающей защиты.

1. Стратегия быстрого реагирования. Заключается в немедленном выполнении заранее подготовленного комплекса упреждающих мероприятий при обнаружении направленного на НСД инцидента информационной безопасности (получении от системы контроля (прогнозирования) сигналов (сообщений) о возможном или уже реализуемом нарушении) независимо от ожидаемого времени завершения реализации нарушения или времени наступления негативных последствий. Основным недостатком данной стратегии является высокая ресурсоемкость, обусловленная возможностью проведения избыточных мероприятий для получения приемлемых результатов.

2. Стратегия выверенного реагирования (максимального выжидания). Мероприятия по реагированию проводятся с максимально допустимой задержкой с целью накопления максимального количества информации об обнаруженном или возможном инциденте безопасности. Под максимально допустимой задержкой понимается такой временной интервал после момента времени обнаружения инцидента безопасности, проведение упреждающих мероприятий после которого не приносит эффекта. Данная стратегия характеризуется сложным и ресурсоемким контролем, повышенным риском «промедления» упреждающих мероприятий, при ее реализации обеспечивается максимальная обоснованность решения на реагирование и, соответственно, максимальная результативность.

3. Стратегия достаточно обоснованного реагирования. В рамках данной стратегии реагирование начинается при накоплении достаточного для принятия обоснованного решения на реагирование количества информации о возможных (реализуемых) нарушениях независимо от оставшегося запаса времени на продолжение анализа нарушения и ситуации в целом.

4. Стратегия адаптивного (гибкого, динамического) реагирования. Характеризуется тем, что мероприятия по реагированию начинают сразу после накопления минимально достаточного количества информации о нарушениях, далее мероприятия могут оперативно уточняться (полностью изменяться, прекращаться) в зависимости от промежуточных результатов и складывающейся ситуации.

Авраменко В.С., Маликов А.В.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного

ПРОБЛЕМА ДИАГНОСТИРОВАНИЯ НАРУШЕНИЙ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

Одной из актуальных проблем защиты информации в телекоммуникационных сетях различного назначения является диагностирование нарушений безопасности информации.

Нарушение безопасности информации (НБИ) – событие, заключающееся в появлении или реализации угрозы безопасности информации. Событие, заключающееся в появлении (создании) угрозы безопасности информации и (или) попытке ее реализации, относится к нарушениям безопасности первого типа, а заключающееся в реализации угрозы безопасности – к нарушениям второго типа. В литературе и в нормативных документах термину нарушение безопасности первого типа в наибольшей степени соответствует термин «инцидент информационной безопасности» (ГОСТ 18044-2007), под которым понимается появление одного или нескольких нежелательных или неожиданных событий информационной безопасности, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы информационной безопасности.

Диагностирование НБИ представляет собой процесс сбора и анализа информации о НБИ, состоянии системы защиты информации в целом с целью идентификации характеристик нарушений безопасности, таких как цель (объект атаки), тип, местоположение, источник атаки, идентификаторы и др.

В процессе диагностирования НБИ значения одних характеристик могут быть исходными данными для других. Например, данные о местоположении нарушителя безопасности способствуют выяснению причин нарушения безопасности, участников и их ролей. Характеристики НБИ могут быть как однозначными, так и иметь множество признаков. Наиболее сложной является задача диагностирования нарушений по многозначным признакам.

В настоящее время в литературе, руководящих и нормативных документах по защите информации практически отсутствуют научно-обоснованные рекомендации и методики диагностирования НБИ. Диагностирование попыток и фактов реализации угроз безопасности информации в основном реализуется вручную и напрямую зависит от личного опыта, компетентности должностного лица по защите информации, что не позволяет выполнить современные требования к диагностированию нарушений безопасности информации, в первую очередь по оперативности.

Перспективным путём решения проблемы диагностирования нарушений безопасности является автоматизация основных функций диагностирования.

В первую очередь автоматизации подлежат функции сбора и анализа информации о нарушении безопасности. Также необходимо автоматизировать функцию выработки вариантов реагирования на НБИ, выполняемую на основе результатов анализа нарушений безопасности. Все функции диагностирования могут выполняться в автоматическом режиме, в критических системах (обеспечения жизнедеятельности, военных системах) принятие решение на реагирование должно выполняться человеком.

При разработке математического обеспечения системы автоматизированного диагностирования нарушений безопасности информации (методов, моделей алгоритмов) могут использоваться методы и математический аппарат теории вероятностей и математической статистики, распознавания образов, нечетких множеств, биоинспирированные методы.

Агеев С.А.
Россия, Санкт-Петербург, ЗАО «ПКБ «РИО»

ИНТЕЛЛЕКТУАЛЬНОЕ ИЕРАРХИЧЕСКОЕ УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЗАЩИЩЕННЫХ МУЛЬТИСЕРВИСНЫХ СЕТЯХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Подходы к построению инфокоммуникационных сетей связи (ИКСС) определяются концепцией построения сетей связи следующего поколения (Next Generation Network, NGN). Системообразующей основой ведомственной ИКСС является защищенная мультисервисная сеть специального назначения (ЗМС СН), которая создается на основе единой сетевой инфраструктуры и представляет собой цифровую телекоммуникационную сеть интегрального обслуживания с набором служб, обеспечивающих перенос разнородного трафика с заданными количественными и качественными характеристиками предоставления пользователям инфокоммуникационных услуг.

Важнейшей проблемой при создании и эксплуатации ЗМС СН является проблема обеспечения её безопасного функционирования и безопасности циркулирующей в ней информации.

В данной работе рассматривается иерархия оптимизационных задач управления ЗМС СН. Показано, что иерархия представляет собой как вертикальные связи, так и горизонтальные связи в рамках одного уровня управления пирамиды TMN. Показано также, что оперативное оптимальное управление затрудняется вследствие больших размерностей совокупности решаемых оптимизационных задач, которые обеспечивают решение управленческих задач. Обосновывается, что многообразие, разнородность, неполнота и нечеткость исходных данных, учитываемых в задачах управления ЗМС СН, включая управление безопасностью, предопределяют необходимость использовать средства и методы искусственного интеллекта при их решении. В результате чего можно говорить о том, что управление ЗМС СН, являясь по своей природе иерархическим, приобретает свойство «интеллектуального».

Для решения вышеуказанной проблемы предлагается уровни модели TMN дополнить функциональными интеллектуальными слоями управления, задачами которых являются:

– оперативная координация взаимодействия задач управления как на одном абстрактном уровне управления, так и между уровнями;

– повышение оперативности получения объективной количественной и качественной информации о состоянии ЗМС СН и ее элементов;

– повышение оперативности распределения телекоммуникационных ресурсов для обеспечения предоставления пользователям телематических услуг связи с требуемым качеством;

– уменьшение времени реакции на угрозы сетевой безопасности;

– своевременное реагирование на изменение целевых сетевых задач.

Интеллектуализацию предполагается реализовать на основе методов нечетких когнитивных карт, а также на основе методов нечетких логических выводов.

Предлагаемый подход не отрицает применение классических методов оптимизации сетевого управления, а дополняет их в условиях лимита времени на обработку информации в условиях неполной и нечеткой информации о состоянии сетевых элементов и ЗМС СН в целом, позволяет снизить размерность оптимизационных задач и, как следствие, улучшить оперативность выработки управленческих решений по управлению ЗМС СН.

Буренин А.Н.
Россия, Санкт-Петербург, ОАО «НИИ «Рубин»

МОДЕЛИ МОНИТОРИНГА СОВРЕМЕННЫХ ЗАЩИЩЕННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Функционирование современных защищенных телекоммуникационных сетей с высокими показателями по эффективности в условиях интенсивного информационного противодействия и достаточно жестких требований, предъявляемых к ним со стороны различных спецпользователей,

возможно только при решении целого комплекса задач управления сетью, одной из которых является обеспечение эффективного мониторинга.

Имеется определенное число объектов контроля. Каждый объект контроля (объект мониторинга и управления или ОМУ) характеризуется множеством случайных параметров, каждый элемент которого представляет собой случайную величину, задаваемую либо рядом распределения (если параметр представляет собой дискретную величину), либо плотностью распределения (если параметр представляет собой непрерывную величину).

Коллектор производит опрос каждого объекта либо циклически в определенной очередности, опрашивая все параметры, либо асинхронно – когда следующий запрос на последующий параметр посылается только после получения предыдущего.

Каждый запрос обрабатывается ОМУ за время в общем случае случайное, после чего данные значения параметра направляются в коллектор для обработки с целью его оценки.

Как правило, каждый запрос имеет практически фиксированный объем и загружает ресурсы сети обмена на определенное время, которое допустимо считать постоянным и равным среднему значению (математическому ожиданию) времени занятия.

Данные, получаемые по запросу, передаются по сети обмена за время, зависимое от того изменился параметр или нет и, в общем случае, равно сумме фиксированной величины и величины, зависимой от изменения параметра. Данные запроса обрабатывается коллектором за время, зависимое от того изменился параметр или нет и, в общем случае, также равно сумме фиксированной величины и величины, зависимой от изменения.

Для многих параметров, характеризующих надежностные и нагрузочные характеристики ОМУ, характерно, что функция распределения имеет вид экспоненциального распределения.

Для других параметров, характеризующих значения характеристик ОМУ (задержка пакета, джиттер, часто температура оборудования), характерно, что функция имеет вид равномерного распределения. В этом случае важно соотношение рабочего диапазона параметра и диапазона его возможных значений, которое позволит определить вероятность того, что за время получения измеренного значения параметра оно будет адекватно отражать значение этого параметра.

Однако, в силу влияния разных случайных факторов при запросе определенного параметра он не может быть получен за время, выделенное на данный запрос, и для учета вероятности этого применяются модели распределения Бернулли, нормальное и пуассоновское приближения для него.

Верзун Н.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

МОДЕЛЬ ПРОЦЕССА ПЕРЕДАЧИ ИНФОРМАЦИИ В СЕТИ С РАЗГРАНИЧЕНИЕМ ПРАВ ДОСТУПА С ИСПОЛЬЗОВАНИЕМ УСТРОЙСТВА КОНТРОЛЯ ДОСТУПА

В сетях передачи информации с разграничением прав доступа актуальной является проблема организации доступа пользователей к ресурсам сети. Одним из вариантов решения этой проблемы является применение централизованного управления доступом. В состав сети добавляются новые элементы: шлюзы контроля доступа (распределенные элементы) и централизованное устройство контроля доступа. Через шлюзы контроля доступа рабочие станции подключаются к сети и перед началом каждого нового сеанса связи отправляют запрос на его разрешение устройству контроля доступа. Основная задача устройства контроля доступа - принятие решения о доступе рабочей станции и отправка ответа-разрешения (либо ответа-запрета) на создание сеанса связи, основываясь при этом не только на определенной политике безопасности, но и на текущем состоянии системы. Устройство контроля доступа может также давать дополнительные команды управления рабочим станциям, и может рассматриваться как рабочее место администратора сети.

Логически данная сеть представляет собой совокупность двух подсетей: подсеть передачи информации между рабочими станциями и подсеть передачи запросов-ответов к/от устройству контроля доступа. Предполагается комбинированный метод разделения общего канала передачи: между подсетями используется временное разделение, а внутри подсети передачи информации между рабочими станциями случайный синхронный доступ. Запросы от рабочих станций (либо команды от устройства контроля доступа) обрабатываются центральным устройством контроля доступа в режиме с удержанием канала.

Рассматриваются алгоритмы и временные диаграммы процессов передачи (и обработки) информации и предлагаются выражения для расчета длительности временных окон в обеих подсетях, учитывающие режимы их работы.

Математическая модель сети задается совокупностью моделей подсетей, входящих в её состав. Каждая подсеть представляется системой массового обслуживания M/G/1 в дискретном времени и определяется следующими выражениями: z-преобразованием ряда распределения времени задержки при передаче информации (запросов/ответов), z-преобразованием ряда распределения интервала обслуживания. Взаимовлияние подсетей учитывается в системе уравнений интерференции.

Представлены выражения для расчета вероятностно-временных характеристик процессов передачи информации в сети с разграничением прав доступа с централизованным устройством контроля доступа. Вероятностно-временные характеристики рассматриваются отдельно для каждой подсети: среднее время задержки при передаче и обработке, вероятность своевременной доставки (либо доставки и обработки) информации при стохастическом ограничении времени пребывания сообщения в подсетях и др. С помощью представленных выражений может быть проведен анализ вероятностно-временных характеристик и исследовано влияние параметров устройства контроля доступа на работу каждой подсети и сети в целом.

Воронков К.Л., Логинов А.А., Шерстюк Ю.М.
Россия, Санкт-Петербург, ЗАО «Институт инфотелекоммуникаций»

ПРИМЕНЕНИЕ ОДНОНАПРАВЛЕННЫХ ШЛЮЗОВ В СИСТЕМАХ МОНИТОРИНГА ТЕЛЕКОММУНИКАЦИЙ

В настоящее время расширяется парк устройств односторонней передачи данных (однонаправленных шлюзов), предназначенных для обеспечения однонаправленной передачи данных из одной вычислительной сети в другую. Однонаправленный шлюз (ОШ) передает информацию на физическом уровне только в одном направлении, исключая возможность передачи в обратном. ОШ может осуществлять фильтрацию ip-трафика и иные действия, сопутствующие передаче трафика в рамках устройства с применением протокола udp.

Благодаря своим свойствам ОШ, например, может использоваться внутри корпоративной сети для защиты более важных в отношении безопасности информации участков сети от НСД из других ее частей.

В системах сетевого мониторинга телекоммуникаций (ССМТ) основными вариантами применения ОШ являются:

– передача данных мониторинга из «не доверенного» сегмента ССМТ в «доверенный»;

– передача данных мониторинга из множества автономных ССМТ в единый центр мониторинга.

Для каждого варианта цель использования ОШ – обеспечить возможность консолидированного хранения, обработки и отображения данных мониторинга из разных сегментов ССМТ, то есть односторонняя информационная интеграция сегментов / подсистем ССМТ.

Передача данных из «не доверенного» сегмента ССМТ в «доверенный» может осуществляться как на каждом узле сети, где имеются средства обоих сегментов, так и в «точках шлюзования», размещаемых на пунктах управления сетью.

ОШ может использоваться для передачи оперативных и/или ретроспективных данных мониторинга.

В первом случае ОШ должен оказывать минимальную задержку на передачу данных из одного сегмента в другой. Передача ретроспективных данных может осуществляться как с накоплением, так и без – когда новое поколение актуальных значений мониторируемых параметров «затирает» значения, которые еще не были переданы. Очевидно, что вероятность такого события должна быть минимальной.

Во втором случае передаче подлежат последовательности данных (временные ряды наблюдений), для которых характерны в общем случае существенно больший объем и минимальные требования к оперативности передачи. Критериями начала передачи могут быть расписание передач (периоды накопления данных) и/или объем накопленных данных.

При сочетании передачи оперативных и ретроспективных данных целесообразно реализовать приоритетную передачу оперативных данных с прерыванием передачи ретроспективных данных и последующим возобновлением их передачи с «точки прерывания».

Авторами апробировано применение одного из имеющихся ОШ по первому варианту с одновременной передачей оперативных и ретроспективных данных.

Воронков К.Л., Рожнов М.Д.
Россия, Санкт-Петербург, ЗАО «Институт инфотелекоммуникаций»

РОЛЕВАЯ МОДЕЛЬ РАЗГРАНИЧЕНИЯ ДОСТУПА К СЕРВИСАМ УПРАВЛЕНИЯ ТЕЛЕКОММУНИКАЦИЯМИ

Современные телекоммуникационные сети являются сложными динамическими системами, задачей которых является предоставление услуг связи, с заданным качеством, конечным потребителям. Решение этой задачи невозможно без создания автоматизированной системы управления связью (АСУС) обеспечивающей контроль функционирования, мониторинг состояния и управление, как сетью связи в целом, так и составляющими ее компонентами, будь то зоны связи, различные подсети или телекоммуникационные устройства. Эффективное функционирование АСУС не возможно без построения профиля (подсистемы) безопасности, отвечающего за комплексное обеспечение информационной безопасности не только АСУС, но и всей сети связи. Одной из

основных задач, решаемых указанным профилем, является разграничение доступа субъектов к различным сервисам, обеспечивающим предоставление некоторых услуг, в том числе и сервисам управления компонентами сети.

Решение задачи разграничение доступа и построение соответствующей подсистемы в профиле безопасности целесообразно решать на основе модели ролевого разграничения доступа – Role Based Access Control (RBAC), позволяющей осуществлять избирательное управление доступом и группировку прав доступа субъектов системы, объединенных в группы, к некоторым объектам с учетом специфики их применения.

При рассмотрении вопросов управления телекоммуникациями в качестве субъектов могут выступать:

– технический персонал, обеспечивающий функционирование сетей связи или их элементов;
– администраторы системы управления;
– компоненты системы управления (серверы, менеджеры, программные шлюзы), участвующие в информационном взаимодействии на правах клиентов.

В качестве объектов в системе управления телекоммуникациями могут выступать:

– телекоммуникационные устройства (сетевые элементы);
– различные программные сервера, например сервера систем управления базами данных;
– сети и образующие их линии и тракты;
– компоненты системы управления, участвующие в информационном обмене на правах серверов.

Однако, использование классической модели RBAC с поддержкой иерархии и, как следствие наследования полномочий, при построении АСУС не всегда целесообразно. Так, например, все множество возможных привилегий будет определяться декартовым произведением множества групп субъектов на множество всех возможных функций связанных с объектом системы. При таком подходе размерность решаемой задачи будет увеличиваться в геометрической прогрессии, что в свою очередь приведет к дополнительной нагрузке на компоненты системы, обеспечивающие разграничение доступа, и как следствие к более низкой эффективности их функционирования, а также к сложности администрирования АСУС. Все вышеперечисленное, в свою очередь, будет приводить к уменьшению эффективности не только АСУС, но и всей системы связи в целом.

Решением данной проблемы может являться расширение модели RBAC, позволяющие сократить размерность исходной модели. Это может быть достигнуто — построением нескольких деревьев ролей, связанных с определенными аспектами обеспечения функционирования АСУС (администрирование, управление, мониторинг, контроль и т. д.), классификацией функций управления различных сетевых элементов, с целью уменьшения мощности множества функций управления, введением динамической составляющей в RBAC модель. Динамическое расширение указанной модели заключается в формировании множества пользовательских атрибутов для каждого правила, обеспечивает гибкую систему настройки прав и полномочий без изменения самого дерева ролей.

Представленный подход к построению модели разграничения доступа при решении задач построения АСУС телекоммуникационными сетями позволяет добиться эффективного разграничения доступа к объектам управления, что в свою очередь снижает возможность несанкционированного доступа к управляемым объектам. Таким образом, можно говорить о повышении защищенности АСУС в целом и как следствие об увеличении защищенности всей сети связи, как объекта применения АСУС.

Воронков К.Л., Таран В.В., Шерстюк К.Ю., Шерстюк Ю.М.
Россия, Санкт-Петербург, ЗАО «Институт инфотелекоммуникаций»

ИНФОРМАЦИОННАЯ ИНТЕГРАЦИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМЕ УПРАВЛЕНИЯ ТЕЛЕКОММУНИКАЦИЯМИ

Современные системы управления телекоммуникациями (СУТ) являются сложными техническими комплексами, образуемые множеством распределенных программных и программно-аппаратных средств. Следует отметить, что практически каждый из компонентов образующих СУТ, начиная от операционной системы (систем) и заканчивая прикладными серверными и клиентскими приложениями имеют собственные средства защиты информации (СЗИ). Также свои средства защиты наличествуют и у телекоммуникационных и программных средств, образующих некоторую сеть связи, управляемую СУТ.

Данные СЗИ имеют локальный характер, являются независимыми друг от друга и как следствие, не позволяют получить общую картину защищенности сети связи. В телекоммуникационных сетях объектами атаки могут являться: телекоммуникационные устройства, хранилища данных, отдельные компоненты СУТ и СУТ в целом, присоединяемые системы управления

Учитывая требования по оперативности, предъявляемые к ряду связных систем общего и специального назначение имеет место противоречие между своевременностью принятия решения по поддержанию сети в работоспособном состоянии и полнотой сведений по состоянии информационной безопасности, влияющих на принятие управленческих решений.

Устранением данного противоречия может являться информационная интеграция всех имеющихся в системе СЗИ в единую подсистему информационной безопасности сете связи. Такую интеграцию целесообразно проводить в рамках СУТ, как системы автоматизирующей все процессы мониторинга и управления телекоммуникационной сетью.

В качестве интегрируемых средств могут выступать:

– СЗИ, входящие в состав операционных систем;
– специализированные комплексные средства, обеспечивающие защиту некоторого узла сети;
– программные средства обнаружения и предотвращения сетевых атак;
– СЗИ различных хранилищ данных;
– СЗИ присоединяемых к СУТ систем управления;
– средства мониторинга и управления входящие в состав СУТ;
– средства администрирования СУТ.

Информационную интеграцию целесообразно проводить путем построения подсистемы регистрации атак, состоящей из средств хранения и отображения событий нарушений информационной безопасности, семейства программных шлюзов, опрашивающих различные интегрируемые подсистемы и подсистема восстановления целостности телекоммуникационной сети.

Шлюзы, обеспечивающие сбор сведений от различных СЗИ, осуществляют периодический опрос и фиксацию событий, связанных с теми или иными нарушениями. Сформированные события поступают в подсистему регистрации и доводятся до должностных лиц, обеспечивающих информационную безопасность. Принятие управленческих решений по предотвращению угроз может осуществляться как в автоматизированном (ручном режиме), так и в автоматическом, с помощью средств контроля и восстановления целостности. В последнем случае эти средства, на основании системы правил, определяют, какие управляющие воздействия должны быть осуществлены. Объектами таких воздействий могут выступать любые объекты образующие сеть или ее систему управления при наличии у них внешних интерфейсов, обеспечивающих информационное взаимодействие. К самим воздействием могут быть отнесены — восстановление эталонного состояния параметров телекоммуникационных устройств, смена идентификационных, аутентификационных и/или авторизационных данных, блокировка пользователей или узлов сети, восстановление данных из архивов и другие. Действия, предпринятые по устранению угроз или результатов атак, в свою очередь, также должны регистрироваться в соответствующей подсистеме.

Представленный подход к информационной интеграции средств защиты информации, может быть использован при построении масштабных гетерогенных сетей связи, с целью повышения их защищенности и эффективности функционирования.

Выговский Л.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им.В.И. Ульянова (Ленина)

ПРОБЛЕМЫ ЛИЧНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ОБЛАЧНЫХ ПРИЛОЖЕНИЙ

Сегодня все большую популярность приобретают облачные сервисы, распространяемые по принципу программа как сервис», причем не только в сегменте b2c (businesstocustomer, т.е. когда конечным потребителем является частное лицо), но и в b2bсегменте (конечным потребителем является юридическое лицо). При этом не достаточно широко освещается проблема использования данных сервисов с точки зрения аспектов информационной безопасности: доступность, целостность, конфиденциальность [1]. Можно выделить следующие категории сервисов, представленных на рынке в сегменте b2c:

– облачные хранилища данных, при которых пользователь может загружать произвольные файлы в инфраструктуру провайдера;

– замена традиционных офисных приложений, таких как MSOfficeи Libra(Open) Office, позволяют пользователем создавать и редактировать документы, электронные книги, презентации и т.п., используя браузер. Данные сохраняются на серверах провайдера;

– сервисы по доступу к объектам интеллектуального права, таким как книги, музыка, фильмы. Как правило, пользователь не получает возможности полноценно использовать купленное произведение. Он может просматривать (прослушивать) его online или с помощью специального программного обеспечения.

Для всех категорий сервисов актуальна проблема конфиденциальности. В случае хранения данных и документов, в первую очередь, с точки зрения пользователя. Только пользователь вправе определять, кто имеет доступ к данной информации. В случае сервисов-подписок вопрос

конфиденциальности остро стоит и перед поставщиком. При этом следует отметить, что в случае хранения данных (в виде файлов или документов) существует два места утечки информации: во время передачи информации в инфраструктуру поставщика в результате атаки «человек-по-середине»; доступ к сохраненным данным через инфраструктуру поставщика решения. Наиболее безопасным подходом является шифрование данных на стороне клиента, что часто невозможно для офисных приложений.

Отдельно стоит вопрос доступности данных. В случае отсутствия соединения с серверами поставщика решения, данные могут быть не доступными для клиента. В качестве решения, приложения должны кэшировать данные локально на компьютере. Также существует угроза закрытия сервиса и возможной потери всех данных.

Григорьев В.А., Хворов И.А.
Россия, Санкт-Петербург, ООО «Лаборатория инфокоммуникационных сетей»,
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

ТЕХНОЛОГИЯ DSRC КАК ОСНОВА РЕАЛИЗАЦИИ СЕТИ ПЕРЕДАЧИ ДАННЫХ В ИНТЕЛЛЕКТУАЛЬНЫХ ТРАНСПОРТНЫХ СИСТЕМАХ

Современная Интеллектуальная транспортная система (ИТС) объединяет в единый технический и технологический комплекс подсистемы организации дорожного движения, обеспечения безопасности дорожного движения, а также предоставления информационного сервиса для участников дорожного движения и потенциальных субъектов транспортного процесса. Построение ИТС невозможно без разработки и реализации проектных решений по формированию различных вариантов взаимодействия подсистем и обмена информацией между ними.

Для обеспечения коммуникационной составляющей ИТС необходимы три основных компоненты: радиосистема высокоточного навигационного обеспечения, системы электронно-картографического обеспечения и системы радиосвязи и передачи данных различного радиуса действия.

Последние во многом отвечают за безопасность, в транспортных сетях, и к ним предъявляются строгие требования, обусловленные спецификой ИТС. Конфигурация подобных сетей постоянно меняется, что требует применения mesh-технологий, позволяющих быстро изменять маршруты следования информационного потока. Сигналы, генерируемые движущимся источником электромагнитного излучения, подвержены эффекту Доплера, что требует использование узкополосных импульсов для передачи данных. Условия распространения сигналов не постоянны, на их пути появляются и исчезают различные препятствия, что требует применения помехоустойчивого кодирования с динамически меняющимися параметрами. Для ускорения процесса обмена данными, особенно между двумя находящимися рядом автомобилями, желательно, чтобы они передавались по самому кратчайшему пути, минуя, например, сервер провайдера, а для реализации подобной функции время вхождения в сеть должно быть минимальным.

Единственной технологией, создаваемой специально для этой целей беспроводной передачи данных в ИТС является технология DSRC, способная обеспечить полный спектр необходимых сервисов по управлению, контролю и обеспечению безопасности дорожного движения.

Технология DSRC – это комбинации разновидности Wi-Fi и Mesh-сети, функционирующей без базовых станций, путем передачи сигнала от одного объекта к другому. Каждый автомобиль, в таком случае, становится узлом связи, и чем больше оборудованных автомобилей, тем стабильнее и эффективнее сеть. Дальность передачи сигнала в условиях городской застройки – до 1,0 км при скорости передачи данных до 27 Мбит/с и устойчивой работе при движении транспорта со скоростью до 250 км/ч. При этом система будет работать и в случае глобального отключения электроэнергии, за счет источников электричества в автомобилях.

Изучение технологии строительства сети передачи данных между подвижными транспортными средствами и объектами транспортной инфраструктуры на основе технологии DSRC в настоящее время проводится на базе соответствующей лаборатории кафедры Беспроводных телекоммуникаций НИУ ИТМО и разворачиваемой при поддержке Комитета по транспорту Санкт-Петербурга опытной зоне.

Гурьев С.Н., Дмитриенко О.А.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного

ПОСТРОЕНИЕ ВИРТУАЛЬНЫХ ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ В ЛВС СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

В современных условиях реформирования ВС РФ локальные вычислительные сети специального назначения (ЛВС СН) выполняют важную роль в обеспечении информационных процессов в автоматизированных системах военного назначения (АС ВН). В связи с этим одним из важных направлений повышения эффективности управления войсками и связью является

совершенствование методов и средств защиты информации в ЛВС СН. Непрерывное функциональное и структурное усложнение средств обработки информации способствует появлению, как современных технологий цифровой обработки информации, так и новых уязвимостей, что в свою очередь расширяет спектр угроз безопасности информации и обуславливает постоянную актуальность вопросов защиты информации в ЛВС СН. В качестве источника не преднамеренной угрозы рассматриваются санкционированные пользователи ЛВС СН, имеющие регламентированный доступ к сетевым ресурсам, знакомые со структурой и принципами построения ЛВС СН, спецификой решения задач и возможностью полнодоступного использования штатных средств вычислительной сети.

Виртуальной локальной вычислительной сетью называется сеть, построенная на основе коммутаторов, программно-аппаратное обеспечение которых позволяет отделить логическую структуру сети от физической структуры. Физическая структура определяется электрическими соединениями компьютеров. Логическая структура отражает разбиение сети на сегменты. В пределах сегмента пакет сообщения доставляется всем компьютерам, входящим в этот сегмент, а принимается только тем компьютером, которому он адресован. Таким образом, реализуется метод множественного доступа.

В настоящее время существует несколько способов построения ВЛВС:

1) на основе анализа физических портов коммутатора;
2) на основе анализа MAC-адресов подключенных к коммутатору устройств;
3) на основе анализа адресов сетевого уровня (IP или IPX);
4) на основе специального тега ВЛВС, который определен в спецификации 802.1Q.

Выбор способа построения ВЛВС зависит от сложности и протяженности ЛВС, а также количества и видов используемого, для построения и эксплуатации ЛВС оборудования.

Целесообразность использования в ЛВС СН технологии виртуальных сетей обусловлено тем, что одновременно решаются следующие задачи:

1) повышается производительности в каждой из виртуальных сетей за счет того, что управляемый коммутатор передает пакеты сообщений только узлу назначения;
2) повышается безопасность сети вследствие изоляции прав доступа пользователей к другим виртуальным сетям и создания защитных барьеров на пути широковещательных штормов;
3) уменьшается нагрузка на администратора ЛВС при перемещении пользователей.

Таким образом, построение на виртуальных локальных вычислительных сетей в ЛВС СН позволит повысить безопасность и производительность сети, уменьшить рутинный труд обслуживающего персонала ЛВС.

Гурьев С.Н., Емцова А.А.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ БЕСПРОВОДНЫХ СЕТЕЙ В ТАКТИЧЕСКОМ ЗВЕНЕ УПРАВЛЕНИЯ

В настоящее время единая система управления тактического звена управления (ЕСУ ТЗУ) включает в свой состав программно-технические комплексы, которые обеспечивают должностных лиц различными видами связи, а также обеспечивают работу абонентов в сетях передачи данных, образованных в основном радио и проводными средствами. В ЕСУ ТЗУ применяются единые системотехнические решения по применению средств связи и унифицированных комплектов автоматизированного управления войск, что обеспечивает интеграцию функций управления, огневого поражения, разведки, связи, радиоэлектронной борьбы, навигации и опознавания, позволяющих с максимальной эффективностью управлять тактическими воинскими формированиями.

Развитие современных телекоммуникационных технологий дает толчок для развития перспективного беспроводного принципа обмена информацией между элементами системы управления в ТЗУ. Применение беспроводных сетей широкополосного доступа в ЕСУ ТЗУ позволит создать единую сеть управления войсками на пространстве современного боя, что объединит в единую информационную сеть различные подразделения видов и родов ВС РФ и увеличит качество их взаимодействия на порядок.

Принцип построения беспроводных сетей в ТЗУ основывается на объединении набора командно-штабных машин (КШМ) или комплектов – абонентов военнослужащих в ряд серверов. В беспроводной локальной сети назначается командный серверный комплект, далее с использованием программного обеспечения (ПО) между абонентами сети организуется процесс обмена информацией и устойчивая связь. В случае уничтожения одного сервера предусмотрены процедуры передачи полномочий другому серверу, что решает проблемы связанные с потерей управления.

Программное обеспечение реализует целевые и обеспечивающие функции единой системы автоматизированного управления уровня тактического звена путем формализованной обработки информации, а также производства расчетов и моделирования боевых действий, обеспечения функционирования технических средств комплексов средств автоматизации органов и пунктов

управления ЕСУ ТЗУ в полном объёме заданных требований во все периоды обстановки. За счёт большого количества терминалов, размещённых на пространстве боя и их взаимоперекрываемостью радиусов действия абонентских комплектов, создается единое информационное пространство, в котором каждая боевая единица (КШМ или комплект военнослужащего) будет себе и своим подразделениям обеспечивать связь и управление. Следовательно, возможно будет отказаться от привычной концепции наличия на ТВД огромного количества аппаратных связи и КШМ. Для проведения исследований необходимо на КШМ командира батальона установить терминал с радиусом работы до четырех километров, смоделировать различные условия местности, а также возможные варианты боевых действий и провести расчеты.

Таким образом, применение беспроводных сетей в ТЗУ позволить расширить возможности управления подразделениями для командиров и предоставлять жизненно важную информацию солдатам на поле боя своевременно и с высоким качеством.

Гурьянова Я.М., Деньжонков К.А., Кий В.Я.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного

ПОВЫШЕНИЕ ЗАЩИЩЕННОСТИ РАСПРЕДЕЛЕННОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ВВУЗ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ VPN

Инфотелекоммуникационное оборудование в высших военных учебных заведениях (ВВУЗ), образовательный процесс в которых имеет направленность на изучение техники связи и автоматизации, как правило, объединено в единую вычислительную сеть учреждения. Учебный процесс в ВВУЗ имеет ряд особенностей, обуславливающих целесообразность применения защищенных виртуальных сетей:

– обучение курсантов проводится на нескольких территориях, расположенных в различных районах города (базовый городок, лагерь, полигон, обеспечивающие подразделения); обмен информацией осуществляется по открытым каналам связи, арендуемым у региональных поставщиков услуг связи;

– подготовка курсантов осуществляется по различным специальностям на отдельных факультетах ВВУЗ; также осуществляется подготовка курсантов иностранных государств на специальном факультете, что требует организации разграничения доступа к совместно используемым ресурсам;

– совместное использование помещений, учебной и боевой техники связи и автоматизации обучающимися различных факультетов;

– необходимость обеспечения удаленного контроля работы обучающихся преподавателями кафедр с других территорий ВВУЗ, а также обеспечения удаленного контроля работы самих преподавателей должностными лицами учебно-методического отдела;

– информация, обрабатываемая в распределенной вычислительной сети ВВУЗ, может носить характер ограниченного доступа и иметь различный гриф секретности.

Распределенная вычислительная сеть ВВУЗ, как правило, строится с использованием стандартного коммуникационного оборудования, которое имеет возможности по организации защищенных виртуальных сетей. Построением защищенных виртуальных сетей на основе заявок кафедр и учебно-методического отдела будут заниматься должностные лица отдела средств автоматизации, за которыми закреплено коммуникационное оборудование ВВУЗ. Однако ввиду многочисленных обязанностей сотрудников данного отдела, значительного числа коммуникационного оборудования в техническом ВВУЗ, возможной не укомплектованности штатным личным составом развертывание защищенных виртуальных сетей может вызывать затруднения и потребовать существенных временных ресурсов.

Представляется актуальным проведение исследования, включающего следующие вопросы: рассмотрение состава и структуры распределенной вычислительной сети ВВУЗ, анализ средств построения распределенной вычислительной сети ВВУЗ, в котором особое внимание уделено возможностям и порядку развертывания VPN, разработка обоснованных предложений и методических рекомендаций для обслуживающего персонала по применению защищённых виртуальных сетей в учебном процессе. Также полученные результаты могут быть использованы при проведении тактико-специальных занятий и узловой практики. Обучающиеся в качестве одного из учебных вопросов могут отрабатывать развертывание защищенной сети между территориями ВВУЗ, используя имеющиеся программные и аппаратные средства для организации защищенного взаимодействия между сегментами вычислительной сети.

Давыдов А.В., Синюк А.Д.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного

МЕТОД ОТКРЫТОГО КЛЮЧЕВОГО СОГЛАСОВАНИЯ СЕТИ СВЯЗИ

Обмен информацией между корреспондентами сети связи закрытый на сетевом ключе имеет преимущества: возможность обмена каждого с каждым, простой ввод нового корреспондента,

возможность контролировать передаваемую информацию и использовать ее для оповещения или передачи команд и т.д. Однако компрометация сетевого ключа нарушителем влечет за собой полную потерю криптографической связности одновременно всех корреспондентов сети связи. Поэтому актуализируется разработка метода открытого ключевого согласования сети связи.

Предлагается метод открытого ключевого согласования сети связи. Функции непосредственного управления формированием сетевого ключа и проверки его наличия у всех корреспондентов сети связи возложены на главную станцию. Формирование сетевого ключа осуществляется посредством использования специальных устройств формирования ключа, имеющихся у всех корреспондентов сети связи до начала ключевого согласования.

Предварительно согласованы все алгоритмы обработки информации о формируемом сетевом ключе и во все устройства формирования ключа сети связи введены открытые исходные данные, к которым могут относиться открытые ключи электронной цифровой подписи всех корреспондентов, объем сети связи и др. После выявления компрометации действующего сетевого ключа в устройстве формирования ключа сети связи на главной станции вводится информация о корреспондентах, у которых имела место компрометация сетевого ключа. Затем устройство формирования ключа главной станции по сети связи оповещает другие устройства формирования ключа о компрометации, запрете работы в закрытом режиме, переходе в открытый режим работы сети связи и запуске процедуры формирования нового сетевого ключа с оставшимися не скомпрометированными корреспондентами. Данная процедура реализуется в автоматическом режиме по заранее записанной в устройство формирования ключа программе посредством обмена вырабатываемой информацией между устройствами формирования ключа всех не скомпрометированных корреспондентов сети связи по имеющимся открытым каналам связи. После формирования сетевого ключа по команде с главной станции все корреспонденты сети связи переводятся в закрытый режим работы.

Предполагается, что групповые ключи, формируемые в ходе выполнения метода открытого ключевого согласования сети связи, формируются на основе реализации протоколов формирования ключа в сети с минимальным числом корреспондентов. Особо рассмотрены случаи решения задач ключевого согласования между двумя, тремя и четырьмя корреспондентами связи.

Представлено алгоритмическое описание и проведен подробный анализ предложенного метода открытого ключевого согласования сети связи. Метод обладает рядом преимуществ. Во-первых, он ориентирован на использование первичных каналов. Во-вторых, стойкость сетевого ключа обеспечивается случайностью ошибок, всегда имеющих место в реальных каналах связи. В-третьих, формирование сетевого ключа производится без участия центра распределения ключей, что увеличивает стойкость сетевого ключа.

Анализ предложенного метода показывает его высокую практическую ценность. Определены возможные пути его применения в смежных областях для решения задач: незащищенного распределения идентификационной и парольной информации систем защиты информации; безопасного распределения радиоданных по радиоканалам связи; формирования расширяющего сигнала системы связи с расширенным спектром и др.

Демидов А.А.
Россия, Санкт-Петербург, Комитет по телекоммуникациям и информатизации Ленинградской области

ОБЩИЕ КОНЦЕПТУАЛЬНЫЕ ПОЛОЖЕНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИИ НА ОБЪЕКТАХ ОРГАНОВ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Исследования и систематизация существующих подходов к формированию концепций защиты информации и принципов построения современных информационных технологий позволили развить и сформулировать концепцию обеспечения и контроля безопасности информации (БИ) на объектах органов государственного управления (ОГУ).

Концепция обеспечения и контроля БИ на объектах ОГУ представляет, по существу, содержание методологических основ обеспечения и контроля БИ и их прикладных направлений, обеспечивающих принципы реализации оптимального уровня защиты информации, информационного ресурса, информационных систем, информационной среды должностных лиц органов государственного управления с учетом затрат ресурсов, направленных на получение конечного результата.

Содержанием этой концепции определяется реализация дифференцированной комплексной защиты информации, при которой интегрированы в единое целое направления, средства, механизмы, процессы, методы, мероприятия, программы и их взаимосвязи, способствующие реализации целей защиты, обеспечению структурного построения системы защиты, реализации системного подхода комплексной защиты объектов ОГУ и ее функционирования на всех этапах жизненного цикла. С учетом этого, содержание концепции может быть представлено направлениями, обусловленными развитием методологических основ БИ, а также практическими направлениями их реализации. Первый компонент представлен обобщенным методом КБИ на объектах ОГУ, а второй – практическая

реализация концепции, предполагает системное использование совокупности сведений и решений, необходимых и достаточных для решения задач анализа и синтеза системы контроля безопасности информации (КБИ), а также других задач, возникающих в различных условиях постоянного внешнего воздействия дестабилизирующих факторов и множества потенциальных угроз. С учетом этих направлений структуру концепции обеспечения и контроля БИ можно представить следующими положениями.

1. Формирование и выбор принципов структурного представление ОГУ, как потребителя информации заданного качества, с учетом сфер деятельности, отношения к различным организационно-правовым формам собственности, степени самостоятельности функционирования, деятельности, взаимосвязей с различными государственными и общественными организациями.

2. Формирование целей, задач обеспечения и контроля безопасности информации и выбор моделей и методов их решения.

3. Формирование правового поля, как основополагающего базиса любых законных видов деятельности, представляющего систему нормативных правовых актов, определяющих множество отношений в информационной и сфере контроля безопасности, а также в других, взаимосвязанных с ними сферах деятельности государства.

4. Формирование структурного представления системы обработки информации с учетом: сфер деятельности (экономика, политика, оборона, социальная сфера, управление, СМИ, и др.); отношения к различным организационно-правовым формам собственности; степени самостоятельности функционирования, деятельности, взаимосвязей с различными государственными и общественными органами (министерствами, ведомствами, организациями) внутри страны и за рубежом.

5. Системная классификация информации циркулирующей на объектах ОГУ: по степени важности (отнесение сведений и информации к государственной тайне, коммерческой тайне, интеллектуальной собственности, персональным данным и др.); сферам (областям) ее использования (военная, экономическая и т.д.); степени (возможности) использования наработанной информации в интересах народного хозяйства (двойное применение закрытой информации и информационных технологий в рамках программ Государственного заказа); степени компьютеризации, автоматизации процесса обработки информации.

6. Унификация структуры информационных ресурсов и потоков на объектах ОГУ: формирование информационного ресурса по объектам отношений физических и юридических лиц государства (документы, массивы документов, в том числе находящиеся в информационных системах государственного, общественного и ведомственного характера), по классам информационных систем различного назначения (библиотеки, архивы, банки данных, базы данных, информационные технологии, процедуры и алгоритмы сбора, обработки, передачи, хранения, информации, научно-технический потенциал и т.д.); формирование структуры потоков обмена информационными ресурсами в системе обработки информации ОГУ.

7. Структурирование и представление среды, в которой должна осуществляться защита информации, в том числе агрессивной.

8. Выявление, классификация и оценка возможных дестабилизирующих факторов, характеристик источников угроз безопасности информации и каналов утечки информации, оказывающих влияние на защищенность информации.

9. Уточнение перечня, структуры, классификации и характеристик объектов защиты информации.

10. Выбор способов, методов и средств обеспечения КБИ, а также системных оценок их эффективности.

11. Разработка системы концептуальных решений, обеспечивающих организацию эффективной защиты информации от любых потенциально возможных угроз.

12. Формирование системы условий, обеспечивающих практическую реализацию заданных вариантов и стратегий эффективного контроля и защиты.

13. Разработка организационной структуры единой системы обеспечения КБИ в рамках концепции интеграции информационных технологий и объектов ОГУ различного назначения и уровня.

14. Формирование направлений развития государственной программы КБИ, системы научных исследований, подготовки специалистов на базе действующих и создания новых учебных заведений, ведомств, страны, межгосударственных органов в области БИ.

15. Разработка и уточнение направлений оптимизации экономических затрат на обеспечение КБИ с учетом существующих и перспективных условий социально-экономического, политического, научного и других направлений развития страны.

Предложенная общая структура концепции, представляет собой программу развития системы обеспечения и контроля безопасности информации. При этом, эффективность и безопасность функционирования объектов ОГУ может быть обеспечена только при наличии обоснованной классификации ее компонент, достаточно полного перечня проблем, ранжированных по степени важности и очередности решения, рационального распределения исследовательских ресурсов по проблемам и методов исследования, адекватных специфике исследуемых компонент и их проблем. В

свою очередь, это предполагает разработку такого содержания программы исследований, которое позволит решать задачи описания, обобщения, предсказания, объяснения, определения направлений исследований, постановки новых задач и проблем, обнаружения имеющихся методологических ошибок, выявления связей с важнейшими научными теориями, законами, принципами, явлениями, методами, а также классификации и систематизации накопленных знаний в предметной области.

Разработка этой программы осуществлялась на основе концептуальной теоретической модели информационной системы с учетом принципов системного и информационного подхода. На основе такой модели была сформулирована структура основных исходных методологических посылок системного подхода. Она включает:

понятия "информация" и "объект – источник информации"; семантические, аксиологические, гносеологические, семиотические, физические, синтаксические, коммуникативные, прагматические, когнитивные, праксиологические и другие аспекты и свойства информации, а также отношений в информационных системах; понятия и содержания информационного пространства, отражающего объект и рассматриваемого с позиций смыслового содержания; уровни преобразования информации в знаковой среде; формы представления информации, являющейся причиной действий объекта ее потребления и результатом действий объекта; меры соответствия кванта информации кванту действия объекта; направления обеспечения БИ объектов ОГУ; представления объектов ОГУ как технологических систем; представления объектов ОГУ совокупностями элементов различной природы, объединенных определенными отношениями для реализации заданных целей; объективные и субъективные факторы, влияющие на количественные и качественные характеристики информации; взаимосвязи системы на этапах ее жизненного цикла, характеризующихся фазами, состояниями, внешней и внутренней средами; группировки свойств информационных систем по признаку обладания различным временем проявления негативных последствий и негативных факторов; требования обеспечения процесса построения концептуальной модели информационной системы (истинность, непротиворечивость, возможности развития, и др.); направления развития концептуальной модели и т.д.

Представленные методологические посылки являются лишь постановкой задачи построения исходной модели, позволяющей классифицировать информационные системы, ставить проблемы и определять направления и методы их решения. С учетом этой постановки решалась задача разработки структуры концепции и решение ряда ее задач и проблем, связанных с формированием основ контроля БИ и его научно-методологического базиса, исследованием вопросов разработки научно-технических предложений по созданию вариантов эффективных компонентов системы БИ на объектах ОГУ.

Предложенная концепция, как результат исследований, позволяет анализировать существующие направления в сфере БИ, определять пути преодоления существующих противоречий в теоретических и практических аспектах решения задач комплексной защиты информации, выделять перспективные проблемы и направления развития информационной сферы и ее составляющих.

Деньжонков К.А.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного

НАПРАВЛЕНИЯ РАЗВИТИЯ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ УЗЛОВ СВЯЗИ

В настоящее время практически завершено построение Объединённой автоматизированной цифровой системы связи ВС РФ. Одной из основных составляющих современной системы связи являются модернизированные узлы связи, которые представляют собой комплекс программно-технических средств, позволяющих обеспечить создание линейных трактов между узлами связи пунктов управления и на линиях привязки к узлам доступа единой сети электросвязи (ЕСЭ) РФ, сопряжение с оборудованием цифровых систем передачи ЕСЭ РФ, коммутацию и маршрутизацию цифровых потоков, а также предоставление набора телематических служб.

Для обеспечения защиты информации на модернизированных узлах связи предусмотрена система защиты, состоящая из совокупности аппаратного и программного обеспечения, позволяющая обеспечить возможность обмена и обработки информации, содержащей сведения государственной тайны. Система защиты включает: шифрование потоков данных IP-пакетов и скрытие состава оборудования закрытого сегмента; аппаратно-программный модуль доверенной загрузки; средства антивирусной защиты; средства защиты от несанкционированного доступа; средства защиты информации от случайных воздействий и аварийных ситуаций; средства системы обнаружения вторжений.

Так как со временем количество различных типов и способов организации несанкционированных проникновений в автоматизированные системы будет только увеличиваться, то остается актуальным вопрос развития и совершенствования средств защиты информации, в том числе и развернутых на модернизированных узлах связи, несмотря на то, что на данный момент они соответствуют предъявляемым требованиям. Одним из основных направлений развития защиты информации можно считать развитие систем обнаружения вторжений.

Для разработки обоснованных предложений по совершенствованию системы обнаружения вторжений необходимо проведение подробного исследования для выявления возможных недостатков, уязвимых мест и компонентов системы, которые могут с течением времени устаревать и требуют периодического обновления. Основное внимание при проведении данного исследования на наш взгляд должно быть уделено следующим вопросам.

Определение информации, которая должна храниться в журналах регистрации, и способа её сбора для более эффективного управления любой системой обнаружения вторжений, так как в процессе анализа трафика и состояния сети агенты собирают и обрабатывают большое количество информации.

Определение наилучшей структуры и формата хранения регистрационных данных, чтобы они могли быть быстро обработаны, не требуя больших объемов памяти для хранения и обработки.

Дополнительные способы извещения администратора системы обнаружения вторжений об атаках и аномалиях в сетевом трафике, так как администратор может периодически покидать рабочее место.

Порядок распределения ключей между агентами и серверами системы обнаружения вторжений для организации защищенных каналов взаимодействия между ними. Наличие документа, регламентирующего данный процесс.

Деньжонков К.А., Кий А.В.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного

УПРАВЛЕНИЕ ДОСТУПОМ К ИНФОРМАЦИОННЫМ РЕСУРСАМ АВТОМАТИЗИРОВАННЫХ СИСТЕМ С ПРИМЕНЕНИЕМ МЕТОДОВ ПОСЛЕДОВАТЕЛЬНОГО АНАЛИЗА ДАННЫХ

Статистика нарушений безопасности информации показывает, что даже наиболее развитые в плане инфраструктуры организации, не жалеющие затрат на защиту своих информационных активов, оказываются в центре скандалов, связанных с утечкой и разглашением конфиденциальной информации. При этом в большинстве случаев утечка информации происходит по вине сотрудников организации, действующих строго в рамках предоставленных полномочий. Мотивами нарушений безопасности информации могут быть личные убеждения сотрудника, идущие в разрез с деятельностью организации, хулиганство, а также непреднамеренное выполнение ошибочных действий, приводящее к разглашению конфиденциальных данных.

Результаты проведенного анализа показали, что причинами нарушений безопасности являются несовершенство средств защиты, реализующих традиционные модели управления доступом, а также избыточность предоставленных полномочий по доступу к защищаемым информационным ресурсам. Причинами избыточности полномочий являются, в первую очередь, необходимость обеспечить функциональность системы, обеспечение совместимости программных средств, применение типовых наборов полномочий. Нарушению безопасности информации, как правило, предшествует исследование системы, в том числе настроек средств защиты. Традиционные модели управления доступом действуют по принципу «запрещено все, что не разрешено», но не учитывают порядок использования полномочий. Между тем, большинство задач, решаемых сотрудниками, сводится к выполнению рутинных действий, что позволяет выработать жесткий регламент действий пользователя и сформировать в процессе его деятельности эталонную схему использования информационных ресурсов.

Одним из перспективных направлений повышения эффективности управления доступом к информационным ресурсам является применение, в дополнение к реализованным механизмам защиты, критерия принятия решения о доступе, основанного на методах последовательного анализа данных. Сущность данного метода состоит в следующем. Имеется сформированная в процессе работы формализованная типовая схема действий пользователя, соответствующая регламенту его деятельности. Вводится дополнительный критерий управления доступом, основанный на применении алгоритма кумулятивных сумм. В целях обеспечения возможности принятия решения о предоставлении доступа при поступлении каждого очередного запроса применяется контекст контроля, который представляет собой фиксированное количество действий пользователя, используемых для проверки соответствия эталонной схеме использования информационных ресурсов. Применение алгоритма кумулятивных сумм требует задания пороговых значений. При задании пороговых значений кумулятивных сумм должны учитываться допустимые значения вероятностей ошибок первого и второго рода, задаваемые в требованиях к безопасности информации, обрабатываемой в автоматизированной системе. Доступ пользователя к информационным ресурсам по данному критерию разрешается до тех пор, пока ни одна из кумулятивных сумм не превысила соответствующего порогового значения, то есть порядок его действий соответствует регламенту выполнения той или иной функциональной задачи. Применение данного критерия позволяет минимизировать разницу между объективно необходимыми и реально предоставленными полномочиями по доступу к информационным ресурсам и предотвратить ряд угроз безопасности информации.

Дормидонтов А.А., Зубакин В.В., Кривошеева М.В.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного

АНАЛИЗ СПОСОБОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

Технологии беспроводных сетей широко используется во всем мире, привлекая внимание пользователей относительно невысокими экономическими затратами и простотой развертывания, удобством использования и гибкой архитектурой. Лидером на рынке беспроводных сетей является оборудование, отвечающее спецификациям семейства стандартов 802.11. Основным вопросом функционирования беспроводных сетей, является вопрос обеспечения требуемого уровня безопасности информации, циркулирующей в сети. В отличие от проводных сетей, осуществить перехват информации в радиоэфире намного проще – достаточно иметь комплект оборудования, аналогичный комплекту оборудования абонента беспроводной сети и специальное программное обеспечение. Поэтому при построении беспроводных сетей особое внимание необходимо уделять вопросам безопасности.

Основными способами обеспечения безопасности беспроводных сетей являются:

- уменьшение зоны радиопокрытия до пределов контролируемой зоны;
- активация фильтрации по MAC-адресам;
- запрет широковещательной рассылки идентификатора сети (SSID);
- периодическая замена идентификатор сети (SSID);
- активизировать функции шифрования (WEP, WPA, WPA2 и др.);
- периодическая замена ключей шифрования;
- установка персональных межсетевых экранов и антивирусных программ;
- обеспечение резервирования оборудования;
- осуществление мониторинга состояния защищенности беспроводной сети.

Необходимо учитывать технические и технологические проблемы некоторых протоколов шифрования и как следствие, различные уровни сложности взлома подобной сети. Процедура аутентификации клиента беспроводной сети и в WPA, и WPA2 делится на два больших подвида – упрощенная для персонального использования (WPA-PSK, PreShared Key, т.е. авторизация по паролю) и полноценная для беспроводных сетей предприятий (WPA-Enterprise, или WPA-EAP). Второй вариант подразумевает использование специального сервера авторизации. В частности, по эфиру к точке доступа передается не пароль, а некоторая цифровая последовательность, получаемая в результате перемежения случайного числа, пароля и названия сети (ESSID) с помощью пары вычислительно сложных итерационных алгоритмов PBKDF2 и HMAC. Для взлома протоколов шифрования нужно поймать качественную запись процедуры обмена ключами между клиентом и точкой доступа («хендшейк»), знать ESSID и использовать атаку по словарю.

Таким образом, обеспечение безопасности информации требует анализа существующих конструктивных и деструктивных способов воздействия на функционирование беспроводных сетей. Не следует, однако, забывать что постоянный количественный рост технологий в сфере беспроводных сетей играет важную роль в формировании дальнейший направлений исследований.

Калинин М.О., Павленко Е.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ УПРАВЛЕНИЯ УЗЛАМИ ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЕЙ

Стремительное распространение распределенных компьютерных систем, центров обработки данных и сетевых систем хранения данных стимулирует насущную потребность в надежных, высокопроизводительных, хорошо управляемых компьютерных сетях. В настоящее время наиболее активно развивающейся сетевой технологией являются программно-конфигурируемые сети (ПКС), в которых, в отличие от традиционных компьютерных сетей, решение об изменении маршрутов передачи сетевых пакетов принимается выделенным устройством — контроллером ПКС, который является единственным элементом сетевой инфраструктуры, осуществляющей управление всей сетевой системой по протоколу OpenFlow.

Такой принцип построения сетей порождает проблему обеспечения корреляции новых правил с сетевой политикой безопасности, которая обусловлена отсутствием контроля соответствия новых правил, добавляемых сервисами ПКС, взаимодействующими с контроллером, с правилами политики безопасности ПКС. Конфликтная ситуация возникает тогда, когда кандидат на запись в таблицу сетевых потоков должен создать или удалить табличную запись, которая запрещена (или разрешена), в соответствии с существующими правилами политики. Для решения описанной проблемы необходим сервис управления, обеспечивающий авторизацию субъектов, добавляющих правила, на основе ролей и разрешение потенциально конфликтующих правил добавления потоков.

Сервис управления размещается между интерфейсом управления ПКС и сервисами управления, осуществляющими выработку новых правил передачи данных. Архитектура сервиса включает следующие компоненты:

– детектор конфликтов, осуществляющий корреляцию новых правил, добавляемых сервисами управления ПКС;

– подсистема аутентификации на основе введенных ролей;

– компонент загрузки сетевой политики безопасности;

– компонент принятия решений о добавлении (или удалении) записей в таблице сетевых потоков.

Для аутентификации сущностей, которые имеют возможность работы с таблицами сетевых потоков OpenFlow-сетевых устройств используются три базовые роли: администратор, сервис обеспечения безопасности ПКС, сервис управления. Аутентификация приложений производится на основе ЭЦП. В случае нахождения конфликтующих записей разрешение конфликта происходит на основе введенных ролей.

Предложенная система определения и разрешения конфликтующих записей таблиц потоков в ПКС обеспечивает безопасную настройку сетевых ресурсов и защиту от обхода сетевой политики безопасности в сетях данного типа.

Кий А.В. Морозов И.В.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного

СХЕМА КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ В ГЕОИНФОРМАЦИОННЫХ СИСТЕМАХ

В современных геоинформационных системах (ГИС) недостаточно внимания уделяется защите информации от несанкционированного доступа. Защита данных организуется в основном средствами защиты информации операционных систем (ОС) и систем управления базами данных (СУБД). Не стоит при этом забывать, что ГИС может содержать не только конфиденциальную информацию, но и информацию, содержащую государственную тайну. Следовательно, помимо механизмов защиты, реализуемых в ОС и СУБД, должны обеспечиваться меры комплексной защиты информации, включая программные и аппаратные средства сторонних производителей.

Требования к защите информации содержащей государственную тайну установлены в законодательных актах и постановлениях Правительства РФ и распространяются на защиту государственных информационных ресурсов, при обработке информации содержащей коммерческую тайну требования нормативных документов носят рекомендательный характер.

Защита информации должна предусматривать ее сохранность от широкого круга угроз, таких как, утечка, модификация, уничтожение информации.

Эффективное противодействие угрозам НСД обеспечивается только при комплексном использовании программно-технических, программных средств и организационно-технических методов защиты информации. При этом защита информации должна проводиться: своевременно, активно, разнообразно, непрерывно, рационально, комплексно, планово.

Элементами схемы комплексной защиты являются:

1. средства противодействия утечки информации по техническим каналам;
2. средства предотвращения НСД к компьютерной информации;
3. средства предотвращения программно-технических воздействий на технические средства обработки персональных данных;
4. средства защиты носителей информации на бумажной, магнитной, магнитооптической и иной основе.

Более подробно рассмотрим средства предотвращения НСД к компьютерной информации. Решением этой задачи – создание систем разграничения доступа (СРД), являющихся необходимым и важным элементом защиты ресурсов в информационных системах. СРД на практике реализуют какую-либо модель, формализующую правила доступа субъекта к объектам. Наибольшую практическую направленность и ценность имеют две основные модели это дискреционная и мандатная модели доступа. Данные модели РД в целом позволяют решить проблему защиты от НСД в ГИС, однако ГИС имеют ряд особенностей, которые не позволяют в классическом виде применить существующие модели РД.

Цифровая карта может содержать большое количество слоев, с которыми связаны иерархическими связями многочисленные описательные данные. Доступ к этим данным необходимо разграничить так, чтобы каждый пользователь видел только то, что ему предназначено и мог наносить только те объекты, к которым имеет доступ.

Решение данной задачи заключается в следующем: необходимо разграничить доступ субъектов к объектам в соответствии с «ролью» (должностным предназначением), а объекты распределить по слоям таким образом, чтобы количество слоев было минимальным. Решение данной задачи позволит в первую очередь исключить дублирование объектов в базе данных, введения ложной информации в обход мандатной модели доступа.

Кононов О.А., Кононова О.В.
Россия, Санкт-Петербург, Смольный институт РАО, Санкт-Петербургский государственный университет аэрокосмического приборостроения

О ГУМАНИТАРНЫХ АСПЕКТАХ ИНФОКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Сегодня информационные технологии оказывают все большее влияние на нашу повседневную жизнь. Упрочняется тесный союз компьютера и современных телекоммуникаций. Одной из форм этого союза стали инфокоммуникационные технологии, обладающие следующими характеристиками:

– доступ аудитории к огромным объемам информации;
– интерактивность (увеличение возможностей для обратной связи);
– транзактность (возможность смены коммуникативных ролей коммуникатора и аудитории);
– мультимедийность (объединение в одном техническом устройстве практически всех современных ИТ);
– асинхронность (возможность для реципиента получать необходимую для него информацию в любое удобное для него время).

Все эти характеристики инфокоммуникационных технологий заставляют во многом по-новому оценить роль аудитории, реципиентов (получателей сообщений), с одной стороны, и коммуникатора (отправителя сообщений) — с другой, по сравнению с их ролями в традиционных телекоммуникациях.

Реципиенты (пользователи) современных систем инфокоммуникаций, благодаря интерактивности последних, имеют возможность выступать и в качестве коммуникаторов, т.е. проявлять свою активную роль.

Следует также отметить, что как зарубежные, так и отечественные авторы отмечают не только достоинства инфокоммуникационных технологий, но и те гуманитарные проблемы, которые вызывает их использование. Это, например, проблемы справедливости и равноправия в доступности широкой аудитории к новым информационным технологиям; информации о низших слоях общества; непристойности, порнографии, плагиата, пиратства или просто копирования принадлежащей другим людям информации с целью ее перепродажи.

Результаты анализа современного состояния информационных отношений указывают роль системы высшего образования, как социального института, нацеленного на решение задачи внедрения в сознание современных и будущих участников информационного взаимодействия необходимости соблюдения норм компьютерной этики и привития навыков ее применения через введение информационной этики в разряд дисциплин, изучаемых в высшей школе.

Крживокольский Д.В.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ ДЕКАМЕТРОВЫХ ПАКЕТНЫХ СЕТЕЙ ЗА СЧЕТ ПРИМЕНЕНИЯ АЛГОРИТМОВ ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ ЧАСТОТНЫМ РЕСУРСОМ

Преимущества пакетных радиосетей (ПРС) в наибольшей степени могут быть реализованы в сети пакетной радиосвязи (СПР), представляющей собой организационно-техническое объединение нескольких ПРС с использованием методов динамического управления общими ресурсами. СПР обладает потенциально более высокими показателями помехоустойчивости и помехозащищённости, пропускной способности, а также устойчивости функционирования вследствие выхода из строя отдельных элементов сети. Частотный ресурс (ЧР) является важнейшим ресурсом необходимым для функционирования СПР.

Для реализации потенциальных возможностей СПР необходима разработка алгоритмов динамического управления ЧР, учитывающих особенности декаметрового диапазона, изменение трафика, методы доступа к общей среде передачи, воздействие непреднамеренных и преднамеренных помех. Существует следующие подходы к использованию общего ЧР СПР: централизованный, децентрализованный и комбинированный.

При децентрализованном подходе общий ЧР распределяется между ПРС. При этом ЧР, назначенный в одну из ПРС, не может быть использован другими ПРС. Централизованный подход предполагает управление ЧР на уровне всей СПР. При этом весь ресурс может быть доступен каждой из ПРС, но в различные моменты времени. Централизованное управление ЧР позволяет достичь потенциально более высоких показателей эффективности в каждой из ПРС, но при этом требуется использование части пропускной способности СПР для передачи команд управления. Комбинированный способ предполагает разделение ЧР между ПРС, при этом создается также резерв ЧР СПР.

В качестве показателя эффективности передачи информации в ПРС может выступать вероятность своевременной передачи потока пакетов при соблюдении требований по достоверности и безопасности. В качестве целевой функции при распределении ресурсов СПР могут быть выбраны следующие: максимизация минимальной вероятности своевременной передачи потока пакетов во всех ПРС; максимизация пропускной способности всей СПР, которая определяется как сумма

пропускных способностей всех ПРС; минимизация использования частотного ресурса СПР при соблюдении требований по своевременности, безопасности и достоверности передачи информации в каждой из ПРС и т.д. Метод оптимизации, применяемый в алгоритмах управления ЧР, определяется видом целевой функции и ограничений.

Таким образом, повышение эффективности функционирование СПР может быть достигнуто за счет оптимального распределения ЧР, выделенного для работы СПР. При этом потенциально наиболее высоких показателей эффективности функционирования СПР возможно добиться при централизованном управлении ЧР.

Курилов Д.А., Костиков В.В.
Россия, Санкт-Петербург, ЗАО «Институт инфотелекоммуникаций»

КОНТРОЛЬ ДОСТУПНОСТИ ХОСТОВ IP-СЕТИ

Одной из важнейших частей информационной инфраструктуры современных предприятий и многих государственных организаций являются сети передачи данных, обладающие высокой сложностью в силу территориальной распределенности инфраструктуры, совмещения возможностей передачи данных с возможностями телефонии и видеоконференцсвязи и наличия встраиваемых систем поддержания информационной безопасности, а также резервных и дублирующих элементов, отвечающих за обеспечение надежности и доступности сети. Выход из строя такой системы фактически означает остановку деятельности всей организации.

В качестве инструмента, позволяющего централизовано мониторить и управлять оборудованием сетей, может быть использован программный комплекс (ПК) «Технологическое управление» (ТУ), в задачи которого входит сбор данных мониторинга о состоянии множества оборудования и осуществление (реализация) управляющих воздействий на это оборудование посредством изменения их управляемых параметров, с взаимодействующим программным комплексом «Оперативно-техническое управление», задачей которого уже является мониторинг сетей в целом.

Для поддержания нормального функционирования IP-сети, помимо мониторинга и управления внутренними состояниями важных узлов и мониторинга состояния трактов, может быть использован периодический контроль состояния доступности ее оборудования (узлов сети) по их сетевым ip-адресам. Такой периодический контроль может быть реализован посредством отправки/приема диагностических пакетов данных – в автоматическом режиме для списка заданных сетевых адресов оборудования и/или по явному запросу пользователя к отдельному узлу. Также нужным инструментом для диагностики сети является определение трассы прохождения диагностических пакетов данных к указанному пользователем узлу ip-сети и отображение трассы прохождения этих пакетов.

Функционал средства включающего периодический контроль доступности хостов сети с возможностью просмотреть по необходимости маршрут прохождения пакетов к интересующим узлам, а также сигнализацию о возникающих ошибках доступности хостов, может быть использован вместе с ПК ТУ, расширив его возможности по мониторингу и интегрировав все в едином инструменте. Для этого требуются два компонента:

– программный компонент «Средство контроля хостов IP-сетей» (СКХ) включающий в себя функционал по контролю доступности хостов, имеющий интерфейс взаимодействия с ПК ТУ и предоставляющий для ТУ всю необходимую информацию о состоянии доступности оборудования.

– информационный компонент «Набор данных для технологического управления контроля хостов ip-сетей» предназначенный для регистрации компонента СКХ в службе ТУ, содержащий в себе описание мониторируемых и управляемых параметров компонента СКХ и описание интерфейса пользователя для работы с СКХ.

Распределенная архитектура позволит устанавливать СКХ в интересующих сегментах сети и собирать мониторируемые данные и управлять средством из одного или нескольких ТУ.

Логинов А.А., Олимпиев А.А., Рожнов М.Д.
Россия, Санкт-Петербург, ЗАО «Институт инфотелекоммуникаций»

АРХИВАЦИЯ И ВОССТАНОВЛЕНИЕ ДАННЫХ СЛУЖБ УПРАВЛЕНИЯ ТЕЛЕКОММУНИКАЦИЯМИ

Для повышения надежности служб управления телекоммуникациями и минимизации периодов простоя в случае выхода из строя аппаратных средств необходимо предусмотреть наличие средств архивирования и восстановления данных.

Средства архивирования и восстановления данных (САВ) должны обеспечивать выполнение следующих функций:

– периодически формировать копий файлов и/или баз данных пользователя с одной или нескольких универсальных вычислительных машин (УВМ);

– полученные копии должны сохраняться в локальном хранилище данных и для повышения надежности копироваться в удаленное хранилище при этом должно быть предусмотрено хранение нескольких поколений резервных копий;

– по команде оператора САВ должно восстановить состояние файлов и/или баз данных из сохраненной резервной копии.

Основой САВ является программный сервер резервирования и восстановления (СрАВ) и приложение администрирования, позволяющие настраивать сервер.

СрАВ содержит перечень «задач» – формальных описаний алгоритмов резервирования/восстановления копий данных, направленных на работу с файлами и/или базами данных. С каждой задачей связан управляющий скрипт, выполнение которого приводит к получению соответствующей резервной копии или восстановлению резервной копии.

Задача может состоять из предваряющего алгоритма, т.е. действий по подготовке УВМ к выполнению алгоритма резервирования/восстановления (например, остановка служб работающих с БД), сам алгоритм резервирования/восстановления с архивацией результатов резервирования в файл, и завершающего алгоритма, переводящего УВМ в штатный режим функционирования.

Задача представляет собой скрипт на языке Bash принимающий на вход два параметра: режим функционирования (архивирование или восстановление данных) и абсолютный путь к файлу данных (в режиме архивирования в него будут сохранены данные, в режиме восстановления этот файл содержит данные для восстановления).

Перечень задач поддерживаемых САВ может быть расширен без изменения программного кода.

Приложение администрирования позволяет оператору сформировать «задание» — периодический процесс, состоящий из одного или нескольких этапов и направленный на выполнение действий, описанных в задаче, на указанном УВМ с заданным периодом.

СрАВ с периодичность заданной оператором запускает процесс создания резервной копии, состоящий из следующих этапов:

– этап инициализации задания и формирования резервной копии: на этом этапе СрАВ определяет задачу и УВМ, после чего копирует скрипт задачи на целевую УВМ и инициирует его выполнение;

– этап передачи резервной копии в локальное хранилище начинается в случае успешного завершения формирования резервной копии. Резервная копия создается автоматически в каталоге целевой УВМ, данный файл копируется на УВМ, где функционирует СрАВ и помещается в локальное хранилище резервных копий;

– этап архивирования начинается в случае успешного завершения первых двух этапов. На этом этапе СрАВ осуществляет копирование резервной копии в удаленное хранилище. При необходимости в удаленном хранилище осуществляется удаление устаревших поколений резервных копий.

Процесс восстановления не выполняется автоматически и может быть инициирован оператором только в ручном режиме. На этапе инициализации СрАВ определяет задачу и УВМ, после чего копирует скрипт задачи и резервную копию на целевую УВМ и инициирует выполнение скрипта.

Использование протокола SSH (Secure SHell) для передачи файлов на удаленные УВМ и для запуска задач резервирования/восстановления позволяет использовать незащищенные каналы связи. Также благодаря использованию протокола SSH компоненты САВ устанавливаются только на одну УВМ, необходимость установки дополнительных программных компонентов на УВМ-источники данных и УВМ-удаленное хранилище отсутствует.

Лопатин Д.В., Анурьева М.С., Ерёмина Е.А., Лопатина М.В., Калинина Ю.В.
Россия, Тамбов, Тамбовский государственный университет имени Г.Р. Державина

АКТУАЛЬНЫЙ УРОВЕНЬ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ УГРОЗ ДЛЯ ПОЛЬЗОВАТЕЛЯ

Современный тренд развития инфокоммуникационных процессов состоит в обеспечении доступа к любому контенту всех пользователей, независимо от местоположения и используемого устройства. Это неизбежно порождает ряд проблем, связанных с безопасным применением информационно-коммуникационных технологий. Цель работы - привести описание основных методов блокирования актуальных угроз информационного характера для молодежной группы пользователей (школьники, студенты) и состоявшихся специалистов (сотрудников), работающих в сфере информационных и коммуникационных технологий.

На сегодняшний день для пользователя можно выделить следующие инфокоммуникационные угрозы: вредоносное программное обеспечение, вымогательство, фишинг, интернет-зависимость, нежелательный (вредоносный) контент, манипулирование сознанием и действиями пользователей. Такое деление достаточно, т.к. все многообразие угроз инфокоммуникационного характера можно

свести к рассмотренным выше. Были проведены исследования, направленные на выявление актуальных инфокоммуникационных угроз для пользователей различных возрастных групп (учащиеся средних школ, студенты, сотрудники государственных и коммерческих компаний, профессиональные разработчики информационных систем). Показано, что абсолютное большинство (78%) респондентов активно пользуются инфокоммуникационными технологиями. Так, больше пяти часов в день проводят в сети 45% респондентов, у 40% постоянно включены на компьютере или мобильных устройствах определенные сетевые сервисы. Среди молодежной группы пользователей только 10% не являются интернет-зависимыми, среди сотрудников этот показатель достигает 43–53%. До 70% студентов и 36% школьников считают, что интернет становится причиной частых или случайных проблем в жизни; 17-42% опрошенных студентов и 48% школьников признают, что интернет – основная причина постоянных проблем в жизни; 10% школьников отмечают, что интернет – основная причина постоянных проблем в жизни. Отметим, что интернет-зависимость, помимо ощутимого воздействия на жизнь пользователя, ведет к уязвимости пользователя перед другими инфокоммуникационными угрозами. Большая доля – 60–70% – IT сотрудников могут противостоять угрозам, связанным с фишингом, вирусными и хакерскими атаками, коммуникационными рисками. В группе сотрудников государственных и коммерческих организаций хорошие знания демонстрируют только 29–50% специалистов. Почти все студенты и школьники имеют неглубокие знания в области рассматриваемых ИКТ-угроз. Исследования показали, что в целом пользователи адекватно относятся к нежелательному контенту. Только 10–14% респондентов регулярно и намеренно посещают ресурсы, содержащие агрессивный, неэтичный и незаконный контент.

Таким образом, видно, что молодежная группа и значительная часть сотрудников имеют средний и начальный уровень знаний об угрозах, не способны адекватно реагировать на данные угрозы и, как следствие, подвергаются рискам.

Работа выполнена при финансовой поддержке гранта РГНФ № 12-16-68005

Моляков А.С.
Россия, Москва, ФГУП «НИИ «Квант»

ИССЛЕДОВАНИЕ НОВЫХ МОДЕЛЕЙ И МЕТОДОВ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ С ЦЕЛЬЮ ПРОТИВОДЕЙСТВИЯ СРЕДСТВАМ СКРЫТОГО ВОЗДЕЙСТВИЯ

В докладе будет представлены Формализованная модель «скрытого» функционирования агентов защиты ПО АСУ и методика обнаружения скрытых процессов вредоносного кода. Автором были разработаны и успешно реализованы новые методы и алгоритмы поиска скрытых процессов средств скрытого воздействия. Апробация проводилась на примере поиска вредоносного кода в ядре ОС Windows.

Никифоров О.Г.
Россия, Санкт-Петербург, ОАО «НИИ «Рубин»

О ПОДХОДЕ К СИНТЕЗУ СИСТЕМЫ МНОГОУРОВНЕВОЙ МНОГОПОЗИЦИОННОЙ ЗАЩИТЫ

Система многоуровневой многопозиционной защиты (ММЗ) может применяться для обеспечения информационной безопасности объектов различного назначения. При этом уровни системы ММЗ соответствуют взаимодействующим областям функциональных задач, решаемых системой защиты, а позиции – местам размещения ее элементов.

В общем виде система ММЗ может содержать пять уровней: уровень непосредственной защиты, уровень обнаружения и идентификации опасных событий, уровень сбора и обработки информации и принятия решения, уровень оперативного реагирования и уровень нейтрализации опасного события. Очевидно, что для обеспечения высокой степени защиты система ММЗ должна содержать множество дублирующих элементов, размещаемых на разных позициях, каждый из которых в свою очередь может быть многорубежным.

При решении практической задачи по созданию системы ММЗ важную роль в ее рациональном построении по критерию минимальных затрат при обеспечении заданного качества играет оптимальной определение необходимого количества позиций и их основных параметров, которые должны обеспечиваться путем применения различных наборов технических средств защиты и их многорубежного использования.

Учитывая стохастический характер процессов возможного воздействия различных видов нарушителей и других деструктивных воздействия, в качестве показателей качества защиты могут использоваться вероятность выполнения системой ММЗ возложенных на нее задач $P_З$ и затраты на ее реализацию С.

Для определения значения вероятности $P_З$ рассмотрим модель системы защиты в виде совокупности S позиций защиты, каждая из которых содержит M_S элементов (технических средств защиты, в том числе и при многорубежном использовании). Для учета взаимосвязи различных

позиций и подсистем системы защиты введем обобщенное понятие веса, характеризующего априорную ценность *s*-й позиции для системы ММЗ.

Таким образом, имеет место следующая физическая постановка задачи.

Система защиты, содержит *S* позиций (*s*=1,…,*S*), каждая из которых может быть реализована X_s вариантами и характеризуется вектором весов $A=\{A_s\}$. Эффективность защиты на каждой из возможных позиций, характеризуется вероятностью выполнения задачи при ее использовании для решения задачи защиты, которая для всех возможных вариантов их физической реализации, а также стоимость реализации каждого из вариантов таких позиций защиты задаются матрицами.

Синтез системы ММЗ сводится к решению задачи выбора необходимого количества позиций размещения средств защиты и вариантов их реализации так, чтобы вероятность защиты объекта была максимальной при условии, чтобы стоимость системы не превышала заданного значения (задача оптимального выбора проектов реализации подсистем сложной системы при ограничениях на ее стоимость).

Наиболее часто для решения таких задач (оптимального выбора) используются методы дискретного динамического программирования, которые известны и описаны в литературе.

Результат решения задачи позволяет определить наиболее эффективные позиции и рубежи защиты, последовательность их создания, что является основой дифференцированного подхода к построению системы ММЗ с учетом топологического размещения, функциональных особенностей и веса ее элементов (позиций и рубежей).

Решение такой задачи позволяет определить оптимальную структуру системы ММЗ и параметры ее элементов, значение *которых* характеризует потенциальные возможности системы защиты по выполнению возложенных на нее функциональных задач.

Овчинников А.В., Чуднов А.М.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного

ОПТИМИЗАЦИЯ ПРИЕМНИКА С «МЯГКИМ» РЕШАЮЩИМ ПРАВИЛОМ В УСЛОВИЯХ ПРЕДНАМЕРЕННЫХ ПОМЕХ

Система передачи данных (СПД) специального назначения выполняет функцию передачи данных в автоматизированных системах управления с требуемой своевременностью, достоверностью и безопасностью обмена всеми видами информации. Эффективность функционирования СПД специального назначения определяется в основном вероятностно-временными характеристиками доставки сообщений и параметрами достоверности передачи данных на различных уровнях иерархии эталонной модели взаимодействия открытых систем (ЭМВОС) с учетом возможности воздействия на систему преднамеренной (оптимизированной) помехи.

В частности, когда решение о принятом символе (блоке символов) в точке приема не может считаться надежным, такой символможет заменяться на элемент, получивший название – «стирание». Далеена более высоком уровне ЭМВОС осуществляется исправление ошибочно принятых и стертых символов на основе использования избыточности в передаваемой информации (декодирование с исправлением ошибок и стираний и/или переспрос стертых блоков).

На физическом уровне при приеме двоичных сигналов решающее правилоприемника с «мягким» решением задается тремя областями: области принятия решений «нуля», «единицы» и области принятия решения на выдачу на более высокий уровень сигнала «стирание». В рассматриваемом случае область стирания представляется в видепространства ограниченного двумя гиперплоскостями в *n*-мерном евклидовом пространстве (*n* – база псевдослучайного сигнала). Исследуемая задача состоит в нахождении оптимального порога стирания, определяемого соответствующим коэффициентом стирания, в различных условиях помеховой обстановки и оценке выигрыша, обеспечиваемого за счет использования приемником «мягкого» решения.

Определены оптимальные значения коэффициента стирания. Установлено, что использование «мягких» решений обеспечивает энергетический выигрыш системе до 0,8 дБ. Вместе с тем, как установлено, с ростом длины используемого в системе кода эффективность рассмотренного варианта «мягких» решений снижается.

Изучены вопросы повышения эффективности функционирования системы передачи информации при использовании более сложных конструкций зон стирания.

Олимпиев А.А., Шерстюк Ю.М.
Россия, Санкт-Петербург, ЗАО «Институт инфотелекоммуникаций»

ВОЗМОЖНОСТИ И ВАРИАНТЫ РАЗГРАНИЧЕНИЯ ДОСТУПА К ОБЪЕКТНОЙ МОДЕЛИ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

Методология объектного представления гетерогенных телекоммуникационных сетей представляет собой набор концепций, методов и моделей, позволяющих создать службу сетевого мониторинга и управления в составе АСУС как объектно-ориентированную информационную систему, где информационная модель сети связи представлена в виде частично направленного,

взвешенного графа, узлами которого являются объекты, а ребрами — отношения над объектами. Каждый объект графа может рассматриваться в разных аспектах — являться узлом некоторого множества подграфов.

Если на уровне технологического управления правила разграничения доступа направлены на распределение единиц оборудования по областям ответственности субъектов управления, то на уровне оперативно-технического управления в качестве элементов области ответственности субъекта должны выступать зоны (фрагменты) сети связи и отображение их на подмножества объектов информационной модели.

Потенциально в качестве субъектов управления на оперативно-техническом уровне могут выступать:

– администраторы сети связи и иные должностные лица, отвечающие за мониторинг ее состояния;

– должностные лица старшего в иерархическом отношении объекта (пункта управления) АСУС, либо субъекты управления организационного уровня;

– потребители услуг связи мониторируемой сети.

Для каждого из перечисленных субъектов управления требуется предусмотреть возможность предоставления услуг мониторинга и управления с учетом их места и роли в системе, что предполагает наличие в системе управления аппарата разграничения доступа, в котором:

– определено множество ролей и множество функций управления сетью;

– множество субъектов управления представлено в виде леса, каждое дерево в котором — иерархия наследования полномочий (в общем случае субъект управления может принадлежать нескольким подразделениям и/или организациям);

– полномочия субъекта управления определяется по правилам объединения, пересечения и/или вычитания множеств — каждой вершине дерева должна соответствовать одна или несколько ролей и некий оператор условного наследования полномочий (например, роль может применяться к всему отделу за исключением одного подотдела);

– на множестве объектов информационной модели АСУС логически выделены подмножества — подграфы, характеризующие некоторые аспекты сети и/или подсети, по отношению к которым может быть применена одна или несколько функций управления;

– для каждого подграфа строится матрица отношений [функция управления, роль], характеризующая булево отношение между ролью и функцией управления.

Другим вариантом применения дискреционного управления доступом к объектной модели может рассматриваться подход, в котором множество объектов информационной модели рассматривается как лес, базирующийся на отношении «целое – часть целого». В этом случае булева матрица отношений [функция управления, роль] задается для каждого листа, что позволяет вычислять область ответственности субъектов управления по доступности им тех или иных участков телекоммуникационной сети.

Выбор варианта построения аппарата разграничения доступа зависит от цели и назначения АСУС. Примером применения первого варианта может служить сетевое оперативно-техническое управление, второй вариант целесообразно применять для узлового оперативно-технического управления.

Паращук И.Б.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного

СЕТЕВОЙ МОНИТОРИНГ КАК КЛЮЧЕВОЙ ЭТАП ПОДГОТОВКИ И ПРИНЯТИЯ РЕШЕНИЯ ПО УПРАВЛЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ РЕГИОНАЛЬНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Процессы мониторинга состояния и качества информационной безопасности (ИБ) региональных телекоммуникационных сетей (РТКС) являются неотъемлемой частью процесса управления такими сложными системами. Анализ публикуемых данных, посвященных проблемам управления ИБ сложных телекоммуникационных сетей, позволил выделить несколько этапов в цикле управления ИБ сетей такого класса, определить общую роль и место задач мониторинга состояния (качества) ИБ в цикле управления ИБ сети. Основу организации и проведения всех мероприятий по управлению ИБ РТКС, составляют решения должностных лиц (сетевых администраторов), принимаемые в цикле управления ИБ. В общем случае, решения в процессе управления структурой, параметрами и режимами работы системы ИБ РТКС, принимаются на всех уровнях иерархии, но применительно ко всему процессу управления, как процессу достижения поставленных целей, решения, принимаемые в ходе (в цикле) оперативно-технического управления ИБ РТКС можно условно разделить на три категории: информационное решение; организационное решение; собственно (окончательное) оперативно-техническое решение.

В соответствии с этими категориями подготовку и принятие решений по организационно-техническому управлению ИБ РТКС можно разбить на три этапа: выработка информационного

решения (оценка состояния и качества ИБ РТКС); выработка организационного решения (выработка замысла управления ИБ РТКС) и выработка окончательного оперативно-технического решения (разработка управляющих воздействий, команд управления).

Рассмотрим этапы подготовки, принятия решения по управлению ИБ РТКС и соответствующие им категории решений. Информационное решение вырабатывается в результате уяснения стоящих перед ИБ РТКС задач, определяемых верхним иерархическим уровнем управления и текущего оценивания состояния ИБ. Данное решение представляет собой результат анализа состояния ИБ РТКС, результат текущей оценки качества объекта ИБ и процесса его функционирования. Организационное решение соответствует разработке варианта вектора управляющих воздействий и является стержнем оперативно-технического управления ИБ РТКС.

На основе полученных новых данных детализируются выводы из информационного решения. Полученные на начальном этапе принятия организационного решения результаты составляют основу замысла управления ИБ РТКС. После текущей оценки состояния ИБ РТКС и выработки общей концепции (замысла) управления ИБ РТКС начинается важнейший этап управления, который завершается принятием окончательного оперативно-технического решения. На этом этапе осуществляется окончательное формирование управляющих воздействий (команд управления) и определение порядка управления структурой, параметрами и режимами работы системы ИБ РТКС. Команды управления доводятся до элементов системы ИБ РТКС. Вся взаимосвязанная совокупность элементов оперативно-технического решения составляет структуру решения по управлению ИБ РТКС.

Таким образом, процесс оценки обстановки, включающий сбор и систематизацию информации о состоянии среды функционирования РТКС (с точки рения ИБ), оценивание состояния ИБ РТКС и элементов системы ИБ, является базовым процессом в структуре цикла управления ИБ. Качество оперативно-технического решения по управлению структурой, параметрами и режимами работы системы ИБ РТКС в огромной степени определяется полнотой и рациональностью информационного решения – результатами сетевого мониторинга ИБ РТКС.

Платонов В.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

АНАЛИЗ ПОДХОДОВ К ОБНАРУЖЕНИЮ СЕТЕВЫХ АТАК В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ

Системы обнаружения сетевых атак и вторжений (СОВ) прочно занимают свою нишу в системах защиты информационно-коммуникационных сетей организаций. Современные тенденции перехода к использованию облачных вычислений позволяют использовать традиционные подходы к использованию хостовых и сетевых СОВ. Но специфика облачных вычислений заставляет пересматривать существующие подходы, методы и средства обнаружения.

Как и в любом информационно-технологическом сервисе, в облачных системах имеются уязвимости с точки зрения безопасности. В качестве общих угроз безопасности обработки информации в системах облачных вычислений можно выделить следующие:

1. Угрозы, направленные на нарушение функционирования облака как единого вычислительного и информационного ресурса. Эти угрозы могут исходить как от внешних по отношению к облаку нарушителей, так и со стороны пользовательских задач в облаке.
2. Угрозы, направленные на конкретные задачи и данные пользователей облака, которые также могут исходить извне и изнутри облака.
3. Угрозы, направленные на использование вычислительной мощности облака для решения задач злоумышленника или для скрытия своего местоположения.

Все типы угроз необходимо ставить в соответствие используемой службы. Рассматриваются основные параметры безопасности облачных вычислений, к числу которых можно отнести: базы данных, операционные системы, системы виртуализации, распределение ресурсов, управление транзакциями, уравнивание нагрузки, управление согласованием и управление памятью. Рассмотрено участие основных параметров для каждой из облачных служб: Software as a Service (SaaS), Platform as a Service (PaaS) и Infrastructure as a Srvice (IaaS).

Применительно к службе SaaS рассматриваются основные типы СОВ. Описывается концепция построения SecaaS (безопасности как службы). Рассматриваются примеры внедрения различных типов СОВ в системы облачных вычислений. Особое внимание уделено применению СОВ на различных уровнях виртуализации.

В заключении формулируются основные проблемы, которые требуют своего решения:

- необходимость обнаружения на хостовом, виртуальном и системном уровнях;
- необходимость взаимодействия со средствами защиты хостовой системы;
- необходимость учета специфики построения гипервизора;
- необходимость разработки специализированных СОВ для различных виртуальных машин.

Платонов В.В., Семенов П.О.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

МЕТОДЫ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА В ЗАДАЧЕ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК

В связи с высокими темпами развития вычислительной техники и информационных технологий в последнее время стала актуальной проблема обработки больших данных. Информация по своей природе и содержанию становится более разнообразной и обширной. Для работы с такой информацией не достаточно простого статистического анализа, что вызывает переход к более сложному интеллектуальному анализу данных (ИАД, Data mining).

Методы ИАД весьма разнообразны и позволяют решать широкий спектр задач. Можно выделить следующие группы методов: моделирование, классификация, кластеризация, прогнозирование, а также ключевые методы: искусственные нейронные сети, генетические алгоритмы, деревья решений и нечёткая логика. К методам Data Mining также относятся некоторые статистические методы: факторный анализ, дисперсионный анализ, корреляционный и регрессионный анализ и др. Основная задача методов ИАД заключается в обнаружении в данных ранее неизвестной, неявной и неструктурированной информации и представлении её в наглядном виде, пригодном для использования.

Современные сетевые атаки, специфические методы, используемые в этих атаках, и набор параметров информационной системы или сетевого трафика, необходимых для контроля состояния защищаемой системы, составляют огромное множество данных. Большинство средств обнаружения сетевых атак в своей основе имеет постоянно растущую базу сигнатур. Интеллектуальные методы, применяемые в существующих программных средствах, нацелены на дополнительную защиту, но не на использование их в качестве альтернативы сигнатурной базе данных.

В работе исследуется возможность применения различных методов интеллектуального анализа данных в задаче обнаружения сетевых атак и вторжений. При помощи методов классификации возможно отнесение последовательности сетевых пакетов к множеству атак или нормальному трафику. Методы сокращения размерности позволяют сформировать оптимальное признаковое пространство из параметров сетевого трафика для обнаружения заданного набора атак. Методы кластеризации позволяют объединять различные атаки в классы с общим модулем обнаружения. Использование нечёткой логики позволяет сократить число ошибок первого и второго рода.

Для проведения исследования разрабатывается прототип системы обнаружения вторжения (СОВ), основанный на методе опорных векторов (SVM) для классификации сетевых пакетов и методе главных компонент для сокращения размерности множества параметров трафика. Разрабатываемый прототип имеет модульную архитектуру: множество атак, выбранных для обучения, разделяется на классы, для каждого класса создаётся набор модулей обнаружения.

При формировании каждого модуля обнаружения набор данных, составленный из параметров заголовков IP, TCP, UDP и ICMP пакетов и параметров TCP-сеансов с метками атака/норма, обучается на методах сокращения размерности. Это позволяет отбросить наименее важные «базовые» параметры, определить наиболее значимые параметры и сформировать новое признаковое пространство меньшей размерности, в котором сохраняются глубинные свойства данных. В новом пространстве набор данных обучается на методе опорных векторов и формируется разделяющая гиперплоскость (SVM-модель), позволяющая классифицировать наблюдаемый вектор как атаку или нормальное поведение.

Была исследована работа прототипа на тестовых сетевых дампах DARPA для атак категорий User-to-Root и Remote-to-Local. Проведённые эксперименты показали хорошую работоспособность СОВ. Машина опорных векторов позволяет идентифицировать значительную часть исследованных атак со 100% вероятностью, а для остальных ошибка не превышает нескольких процентов от числа всех пакетов. Методы сокращения размерности помогают сократить объём информации, необходимой для классификации сетевых пакетов, и существенно повысить производительность системы.

Решение о вторжении принимается блоком реакции на основании сигналов всех модулей обнаружения. Такой подход позволяет включать отдельные атаки или классы сразу в несколько модулей обнаружения, что повышает вероятность обнаружения и существенно сокращает число ложных срабатываний системы. Планируется использование нечёткой логики для принятия решения о вторжении и методов кластеризации для группировки атак в классы.

Проведённые эксперименты показали, что за счёт настройки внутренних параметров и пороговых значений возможно добиться оптимального соотношения производительности прототипа и точности распознавания атак, что подтверждает применимость выбранных интеллектуальных методов анализа данных для поставленной цели

Сазонов В.В., Манаенко С.С., Беззубов О.В.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного

О НЕОБХОДИМОСТИ СИНТЕЗА АНСАМБЛЕЙ ДИСКРЕТНЫХ ОРТОГОНАЛЬНЫХ СИГНАЛОВ ДЛЯ ЗАЩИЩЕННЫХ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ

В последние годы российской дипломатией достигнуты существенные результаты между Российской Федерацией и мировым сообществом в области сокращении вооружений, в том числе и химического оружия. Однако, не смотря на это, последние события в мире показывают, что развязывание новых конфликтов с эвентуальным противником, будет влечь за собой новые противоречия агрессивного характера, которые придется решать, в том числе и российской дипломатии.

Современный уровень развития инфокоммуникационных систем внёс коренные качественные изменения в средствах и способах ведения шпионажа, выдвинув проблему совершенствования ведомственных систем в число важнейших.

В условиях переоснащения и частичной аренды иностранного инфотелекоммуникационного оборудования ведомственными службами становится очевидным, что характеристики помехозащищенности систем управления реализованных в радиоканалах сверхдлинноволновых, коротковолновых диапазонов и каналам спутниковой связи становятся первостепенными. Однако, используемые в настоящее время сигналы, в качестве переносчиков в указанных выше каналах связи, обладают низкой помехоустойчивостью к воздействию естественных и преднамеренных помех и не позволяют эффективно использовать энергетические и частотные ресурсы линий для обеспечения высокой помехоустойчивости и скрытности.

Существующие пути совершенствования каналов связи ориентированы на применение шумоподобных сложных сигналов в сочетании с использованием помехоустойчивого кодирования и методов оптимального приема. Анализ ряда работ показывает, что применение сложных сигналов позволяет обеспечить требуемую помехоустойчивость и скрытность. Однако использование широкополосных сигналов ориентировано на наличие каналов с избытком частотных ресурсов, что возможно только для каналов с большой частотной емкостью, а помехоустойчивое кодирование сопровождается значительным снижением скорости передачи информации, что в условиях низкоскоростных радиоканалов, особенно сверхдлинноволнового диапазона, недопустимо.

Учет этих факторов предъявляет ряд требований к характеристикам сигналов, реализация которых может быть обеспечена соответствующим выбором их структуры. Последнее обстоятельство явилось основной причиной постоянно растущего интереса специалистов к ансамблям дискретных ортогональных сигналов, вопросы теории которых и различных ее приложений постоянно рассматриваются в отечественной и зарубежной литературе.

В докладе для повышения защиты ведомственных инфотелекоммуникационных систем, предложено развить теорию применения уникального математического аппарата систем и ультрасистем синтеза систем дискретных ансамблей ортогональных сигналов по совокупности показателей, который впервые изложен в работах профессора В.С. Попенко. В этом случае задача синтеза отличается от традиционных задач оптимизации из-за неклассической постановки за счет многопараметричности и многокритериальности, связанных с формированием ансамблей дискретных ортогональных сигналов.

Синюк А.Д.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного

МЕТОДИКА ОЦЕНКИ ЭФФЕКТИВНОСТИ ОТКРЫТОГО СЕТЕВОГО КЛЮЧЕВОГО СОГЛАСОВАНИЯ

Постановка задачи. Пусть все корреспонденты сети связи имеют возможность связаться между собой в рамках открытой сети связи. Каждый из них имеет аппаратуру шифрования, реализующую единый в сети связи алгоритм шифрования. Функции непосредственного управления формированием сетевого ключа и проверки его наличия у всех корреспондентов сети предлагается возложить на главную станцию сети, а остальные считаются подчиненными станциями. Пусть предварительно между всеми корреспондентами сети связи распределены необходимые открытые исходные данные.

Нарушитель представляется совокупностью каналов перехвата противника. Он способен перехватить всю передаваемую информацию между корреспондентами в сети связи. Его целью является вычисление (получение, перехват и т.д.) формируемого корреспондентами сети связи ключа. Предполагается, что нарушитель пассивен и имеет ограниченный вычислительный ресурс. В качестве допущений сделано предположение о том что, нарушителю точно известно полное описание систем генерации, передачи, хранения и обработки информации, порядок и последовательность процедур, выполняемых корреспондентами для формирования сетевого ключа, а также выбранные параметры для реализации этих процедур. Кроме этого он знает статистические свойства множества генерируемых сообщений, формируемых ключей, широковещательных каналов связи.

Пусть главной станции сети связи работающей на сетевом ключе с подчиненными станциями становится известно, что у одного из корреспондентов или у нескольких корреспондентов произошла компрометация сетевого ключа (т. е. он стал известен нарушителю). Возникает необходимость формирования сетевого ключа между оставшимися корреспондентами. Назовем эту группу группой не скомпрометированных корреспондентов.

Предлагается модель оценки эффективности процесса формирования сетевого ключа по открытым каналам связи с ошибками включающая систему показателей качества сетевого ключа, систему требований к сетевому ключу, показатель эффективности формирования сетевого ключа и порядок оценки эффективности его согласования. Разработана методика оценки эффективности открытого ключевого согласования сети связи выполняемого в соответствии с методом «пересекающихся групповых ключей».

Постановка задачи оценки эффективности в методике описывается следующим образом. На основе требований к сетевому ключу и исходных данных для оценки вероятностей ошибок в каналах сетей связи выбираются условия для наихудшего сценария формирования группового ключа.

С использованием известных методик рассчитываются оценки вероятностей ошибок в каналах для формирования группового ключа. Использование метода «пересекающихся групповых ключей» позволяет получить большое многообразие маршрутов передачи зашифрованного сетевого ключа всем корреспондентам сети связи. Это определяет необходимость переопределения требований к групповому ключу исходя из требований к сетевому ключу.

По уточненным требованиям выполняется выбор протокола формирования групповых ключей.

Производится оценка минимального времени формирования сетевого ключа и показателя эффективности, которая учитывает все риски процесса формирования сетевого ключа по открытым каналам связи.

В заключении сравнивается полученная оценка эффективности с требованиями и формулируется вывод о эффективности процесса формирования сетевого ключа.

Старков А.М.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного

ПРОБЛЕМА ОПЕРАТИВНОГО УПРАВЛЕНИЯ ВИРТУАЛЬНЫМИ ВЫЧИСЛИТЕЛЬНЫМИ СЕТЯМИ В КОРПОРАТИВНЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Виртуальная локальная вычислительная сеть (VLAN) – это логическая («виртуальная») локальная компьютерная сеть, которая представляет собой группу хостов с общим набором требований, взаимодействующие между собой так, как если бы они были подключены к широковещательному домену, независимо от их физического местонахождения. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным станциям группироваться вместе, даже если они не находятся в одной физической сети. Такая реорганизация может быть сделана на основе программного обеспечения вместо физического перемещения устройств.

В процессе жизнедеятельности корпоративной сети происходит ее реструктуризация: количество подразделений и сотрудников, их территориальное расположение меняется. Возникает проблема оперативного переопределения приоритетов, разграничения доступа единичным пользователям и группам пользователей, при этом обеспечивая минимальные затраты на устанавливаемое оборудование. Решение в сложившейся ситуации является использование VLAN.

Применение данной технологии позволит:

– уменьшить количество широковещательного трафика в сети, тем самым увеличится производительность сети без замены или добавления дополнительного оборудования;

– создать группы пользователей по их функциональному, а не территориальному назначению, а также вносить в них изменения без изменения физической инфраструктуры и отсоединения пользователей и серверов от сети,

– повысить безопасность сети за счет невозможности пользователей одной группы попасть к пользователям другой группы.

Данная технология достаточно давно используется во многих организациях и у провайдеров Интернета.

VLAN обеспечивает гибкость в разработке и внедрении инфраструктуры коммутируемой сети. Сети VLAN является частью любой серьезной сетевой разработки. Однако системному администратору необходимо понимать потребности пользователей и пути потоков информации до внедрения виртуальных сетей. Данная технология при всей своей полезности имеет и ряд недостатков, с которыми приходится считаться. Раньше наиболее частой была проблема совместимости оборудования – не все коммутаторы и хабы могли безболезненно пропускать тегированные кадры, и не все сетевые адаптеры поддерживали увеличенный размер кадра. Сейчас вероятность столкнуться с таким сетевым устройством очень мала. Поэтому на первый план выходит необходимость вручную настраивать каждый порт каждого коммутатора. При часто меняющейся топологии сети возникает ситуация, когда необходимо за кратчайший промежуток времени внести

изменения в топологию сети, при этом сохраняя высокий показатель производительности и безопасности. Зачастую большое количество настроек коммутационного оборудования и отсутствие полной карты логических соединений не позволяет это сделать. Этим обосновывается наличие проблемы оптимизации работы системного администратора по определенным алгоритмам, которые должны анализировать предложенную топологию сети и формировать оптимальную схему построения VLAN, а также указывать, какие следует внести изменения в сложившейся ситуации, чтобы обеспечить подключение новых клиентов и серверов.

Суворова А.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

УГРОЗООБРАЗУЮЩЕЕ ПОВЕДЕНИЕ В СЕТИ ИНТЕРНЕТ: МЕТОДЫ ОЦЕНКИ ПАРАМЕТРОВ

При анализе степени защищенности информационной системы необходимо принимать во внимание данные, характеризующие поведение пользователя информационной системы. К таким данным, в частности, можно отнести сведения об интенсивности угрозообразующего поведения, то есть поведения пользователя, которое потенциально может создать угрозу защищенности информационной системы.

Разработанный инструментарий предназначен для косвенных измерений интенсивности по сведениям о нескольких последних эпизодах, что позволяет производить мониторинг интенсивности с необходимой регулярностью. Указанный инструментарий применялся при проведении опросов респондентов об эпизодах их поведения в рамках полевых исследований, однако, заметим, что подобным образом можно проводить опросы в и социальных сетях для изучения интересующего нас вида поведения. Кроме того, такие особенности социальных сетей, как фиксирование эпизодов некоторых видов поведения и предоставление возможности доступа к таким данным позволят использовать разработанные алгоритмы и их программные реализации и без проведения опроса, то есть инструментарий быть использован и при обработке данных, полученных из интернет-контента.

Критерием потенциально опасного события может являться изменение интенсивности рассматриваемого поведения, при этом нас интересуют в большей степени последние и резкие изменения интенсивности. Предложенный инструментарий позволит оценивать интенсивность по последним событиям, причем вычислять такие оценки с требуемой регулярностью.

Тарасов О.М., Кузнецова О.В., Мусаева Г.К.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного

ПОИСК ОПТИМАЛЬНОГО ПРОСТРАНСТВЕННОГО ПОЛОЖЕНИЯ ВВОДИМЫХ В СИСТЕМУ СВЯЗИОБЪЕКТОВ ПО МИНИМАЛЬНОСТИ СУММАРНОГО РАССТОЯНИЯ ДО КОРРЕСПОНДИРУЮЩИХ УЗЛОВ

В данной работе определяется методика оптимизации положения системы вводимых подвижных объектов по заданному показателю оптимизации.Предполагается, что в условном пространстве имеется ряд узлов связи с заранее известными координатами и нужно по заданному показателю оптимизации определить оптимальные координаты системы вводимых объектов связи.В качестве показателя выбрана минимальность суммарного расстояния между вводимыми объектами и корреспондирующими узлами связи.Количество вводимых объектов ограничивается только временем расчета на ЭВМ.

Алгоритм поиска оптимального пространственного положениясистемы вводимых узлов связи предполагает следующую последовательность действий:

1. Составляется уравнение, описывающее пространственное положение подвижных узлов связи согласно заданному показателю оптимизации.
2. По каждой из координат вводимых узлов связиберется частная производная от составленного уравнения.
3. Полученные частные производные приравниваются к нулю, и относительно каждой из координат каждого из вводимых объектов решается система составленных дифференциальных уравнений.

Уравнения системы можно суммировать и решать как единое выражение. Количество уравнений равняется удвоенному количеству вводимых объектов. Решение системы уравнений определяет координаты вводимых в систему связи объектов.

4. Анализ полученных результатов.

Наличие у системы уравнений вещественных корней является необходимым признаком существования экстремума. Поскольку система уравнений при оптимизации по минимальности суммарного расстояния до корреспондирующих узлов всегда имеет хотя бы одно решение (всегда найдется набор точек, каждая из которых минимально удалена от корреспондирующих узлов), необходимый признак существования экстремума у системы одновременно является достаточным. Поэтому отпадает необходимость составления матрицы Гессе и нахождения ее определителя.

Наличие у системы нескольких решений (и соответственно нескольких экстремумов) даст несколько вариантов расположения узлов, но только один из них будет являться оптимальным в плане минимизации суммарного расстояния. Расчет значения суммарного расстояния до корреспондирующих узлов для каждого из полученных решений позволит определить оптимальную расстановку вводимых объектов.

Увеличение числа условных единиц, составляющих условное пространство, приводит к увеличению точности определения оптимального местоположения объектов, однако снижает скорость машинных расчетов. Кроме того, на скорость машинных расчетов существенно влияет количество вводимых узлов. Время определения координат каждого из них увеличивается в геометрической прогрессии с введением нового объекта. При трех одновременно вводимых узлах решение задачи на компьютере со средней вычислительной мощностью занимает около полутора часов.Поэтому при синтезе топологической структуры телекоммуникационной сети необходимо использовать алгоритмы ускорения вычислений, что позволяет в 10 – 15 раз повысить скорость машинных расчетов. Это дает возможность увеличить до пяти максимальное число одновременно вводимых объектов.

Программу оптимизации топологии сети связи желательно составлять в языковой среде MATLAB, поскольку данный язык оптимизирован к матричным операциям и потому удобен при построении сетевых структур, задаваемых посредством матриц смежности. Программы на языке MATLAB, как правило, обладают хорошими скоростными качествами.

Удалов В.С.
Россия, Лодейное Поле, Свирский район гидросооружений и судоходства – филиал ФБУ «Администрация «Волго-Балт»

ИСПОЛЬЗОВАНИЕ СХЕМ ПАРАЛЛЕЛЬНОГО КОМПЛЕКСИРОВАНИЯ С ЦЕЛЬЮ ПОВЫШЕНИЯ ЭЛЕКТРОМАГНИТНОЙ ЗАЩИЩЕННОСТИ (ЭМЗИК) КАНАЛОВ CDMA

При CDMA-технологии каждый из каналов системы полностью использует весь выделенный частотно-временной ресурс; радиоканалы систем CDMA перекрываются как по времени, так и по частоте. Разделение сигналов отдельных каналов осуществляют за счет того, что каждый канал имеет свою «поднесущую» - адресную кодовую последовательность. Стандарт CDMA обеспечивает высокое качество связи в сотовых системах связи за счет «мягкой» эстафетной передачи мобильной станции MS (Soft handover) из одной соты в другую несколькими базовыми станциями BS, не вызывая перегрузок. Стандарт CDMA может найти широкое применение в информационных сетях АСУДС вследствие того, что сложные (широкополосные) сигналы (ШПС) испытывают меньшие потери на трассе распространения и позволяют эффективно бороться с искажениями в информационном канале в условиях воздействия сосредоточенных по спектру помех.

Под комплексированием принято понимать процесс совместного преобразования информации от разных навигационных систем с целью минимизации ошибки (повышения точности) при определении навигационных параметров.

Возможны два способа комплексирования при измерении одного и того же навигационного параметра.

При параллельном комплексировании для оптимального оценивания навигационного параметра используются результаты одновременного его измерения однотипными или разными техническими средствами навигации. Например, оценка дальности цели с помощью параллельно работающих двух и более РЛС либо одной РЛС в сочетании с тем или иным приемоиндикатором какой-либо РНС и т.п.

При комбинированном комплексировании с целью повышения точности измерения навигационного параметра используются результаты измерения не только его, но и других параметров. Так, например, для определения расстояния до движущегося судна с минимальной ошибкой целесообразно измерять его дальность и скорость и т.п.

Используя схемы параллельного комплексирования, становится возможным снизить вероятности появления ошибок в канале передачи информации до уровня, необходимого для практически безошибочного принятия навигационных параметров, а, следовательно, и наиболее точного расчета координат судна-цели. Например, если использовать параллельные сложные сигналы CDMA, то обеспечивается защищенность лишь от незначительных по мощности узкополосных помех, но при значительной по мощности сосредоточенной по спектру узкополосной помехи коэффициенты ЭМЗИК оказываются слишком низкими и не обеспечивают даже удовлетворительного уровня электромагнитной защищенности информационного канала. Однако при увеличении базы субсигнала электромагнитная защищенность повышается до допустимого уровня, дальнейшее повышение которого обусловлено применением предложенных схем комплексирования. При использовании же сложных субсигналов последовательной структуры отмечается достаточно высокий уровень электромагнитной защищенности.

ЭМЗИК широкополосных сигналов последовательно-параллельной структуры находится на значительном уровне, следовательно, при использовании этого вида сигналов можно достичь наибольшего эффекта от применения схем комплексирования. Кроме того малая зависимость данного вида сигналов от частотно-временных структур (законов кодирования) делает этот тип канала CDMA наиболее привлекательным для практической реализации.

Комплексирование информационных каналов в одинаковых электромагнитных условиях позволяет уменьшить вероятность появления ошибки при передаче данных (при наличии всего лишь двух одинаковых информационных каналов) в среднем в два раза (при использовании схем параллельного комплексирования). В случае если же сам информационный канал обеспечивает удовлетворительный уровень электромагнитной защищенности, посредством применений к нему схем комплексирования появляется возможность повысить этот уровень до приемлемого, а в некоторых случаях, и вполне высокого. Например, сложные (широкополосные) сигналы испытывают меньшие потери на трассе распространения и позволяют эффективно бороться с искажениями в информационном канале в условиях воздействия сосредоточенных по спектру помех. Ели применить к ним схемы параллельного или комбинированного комплексирования то можно значительно улучшить электромагнитную защищенность данных каналов связи от всевозможных помех. Конечно, для каждого района плавания необходимо тщательно изучить электромагнитную обстановку, и, вдобавок, обеспечить выполнение требований по электромагнитной совместимости оборудования судовых радиоэлектронных средств. В противном случае все принимаемые меры по обеспечению электромагнитной защищенности могут быть напрасны или же просто не способными ее обеспечить на должном уровне, но при соблюдении всех правил и норм комплексирование информационных каналов является прекрасной перспективой для развития спутниковой радионавигации.

Черняков А.В.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ В ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ

Благодаря ежегодно усиливающейся информации общества, количество связанных сетями устройств неуклонно растет. Плюсы этого очевидны: расстояние между отправителем и получателем больше не является помехой для общения, увеличивая скорость документооборота. Однако у систем автоматизированной обработки и хранения информации есть существенный недостаток по сравнению с традиционными методами обработки – даже при организации надлежащей физической защиты помещений со средствами вычислительной техники, злоумышленник всё равно может получить доступ к обрабатываемым и пересылаемым данным. Кроме того, существует крайне мало эффективных способов идентификации злоумышленников и применения к ним судебных мер.

Причин возникновения такой серьёзной уязвимости несколько: отсутствие разграничения доступа сотрудников предприятия к разнородным информационным ресурсам, ошибки технического персонала, допущенные при конфигурировании сетевого оборудования, а так же несовершенство программно-аппаратных комплексов, установленных в сети.

Эффективной мерой компенсации рисков эксплуатации данной уязвимости является сегментирование локальной сети на независимые участки со строгим контролем информации, передаваемой между сегментами. Организациям, обрабатывающим персональные данные и иные виды информации ограниченного доступа, не относящиеся к государственной тайне, разделение сети может существенно сэкономить средства на обязательной аттестации ЛВС, так как ей подлежат только участки, в которых обрабатываются вышеуказанные данные.

При планировании новой сети следует принять во внимание возможность её расширения и заложить потенциал для сегментации изначально, тем самым сэкономив средства на последующее изменение конфигурации ЛВС. В существующих сетях для экономии времени специалистов, бюджетных средств и уменьшении времени простоя бизнес-процессов принято использовать технологию виртуальных локальных сетей (Virtual Local Area Network, VLAN) и виртуальных частных сетей (Virtual Private Network, VPN).

VLAN – технология сегментирования локальной сети, изменяющая заголовок и контрольную сумму IP-пакета, добавляя идентификатор сегмента перед полями адреса. Пакеты с одинаковым значением идентификатора (VLAN ID, VID) считаются принадлежащими отдельной логической ЛВС и маршрутизируются по отдельным от других пакетов правилам. Её преимуществом является отсутствие необходимости прокладки новых линий связи при сегментации или перемещении оборудования, а так же уменьшение широковещательного траффика в сети. Недостатком такого решения можно считать отсутствие шифрования трафика, необходимость ведения специальной документации и наличия хотя бы одного устройства 3-го уровня для маршрутизации между сегментами. Кроме того, все оборудование, через которое проходит трафик имеющий метку VLAN, должно отвечать требованиям стандарта 802.11Q. В противном случае контрольная сумма пакета,

вычисленная таким оборудованием, не совпадет с контрольной суммой, находящейся в самом пакете, что приведет к его уничтожению.

VPN – семейство технологий, позволяющее с помощью туннелирования и шифрования сетевого трафика создавать виртуальные каналы защищенного обмена данными между устройствами. В отличие от VLAN, VPN не вносит изменения в заголовки ip-пакетов, а инкапсулирует исходный пакет в пакет-переносчик целиком. Такой подход позволяет создавать логические туннели передачи данных поверх сетей с различными, возможно несовместимыми друг с другом, протоколами, не внося в конфигурацию сетей значительных изменений. Благодаря гибкости VPN можно создавать каналы между двумя компьютерами (в конфигурации хост-хост), между компьютером и сетью, а так же между двумя сетями. Для шифрования трафика используются технологии IPSec (IP Security), OpenVPN и PPTP (Point-to-Point Tunneling Protocol). Таким образом, сегментация сетей, в отличие от VLAN, производится с использованием шифрования. Плюсы VPN очевидны: канал обмена информацией защищен от прослушивания и изменения, внутренняя структура сети остается скрытой от наблюдателя, сети VPN могут быть сертифицированы ФСБ РФ для передачи защищаемой информации, а так же промежуточное оборудование не требует специальной настройки. Из минусов можно отметить необходимость специального программно-аппаратного (или программного) комплекса на обоих концах туннеля, сложность отладки конфигурации протоколов шифрования, вероятность потери трафика на этапе инкапсуляции при превышении порогового значения MTU.

Рассмотренные методы защиты информации в локальных сетях позволяют избежать кражи, модификации или уничтожения информации лицами, не имеющими к ней доступ.

Шерстюк Ю.М., Воронков К.Л., Олимпиев А.А.
Россия, Санкт-Петербург, ЗАО «Институт инфотелекоммуникаций»

ВИДЫ ПРАВ И ПОЛНОМОЧИЙ В КОМПЛЕКСЕ СЛУЖБ УПРАВЛЕНИЯ ТЕЛЕКОММУНИКАЦИЯМИ

Согласно общим рекомендациям по созданию автоматизированной системы управления связью она должна включать в себя комплекс служб управления телекоммуникациями, которые представляют собой множество средств связи, линий, трактов, сетей связи и их зон (фрагментов). В отечественной практике создания такого комплекса сложилась следующая практика его организации:

– на главном пункте управления функционирует служба организационного управления, пользователи которой осуществляют контроль и планирование процессов управления с учетом накопленной статистики за сеть;

– на пунктах управления функционирует сервер оперативно-технического управления, отвечающий за подчиненный ему участок сети (зону связи);

– на каждом узле связи функционирует сервер технологического управления, отвечающий за мониторинг и управление элементами сети;

– службы технологического управления узлов связи образуют иерархическую службу технологического управления за счет включения в состав каждого сервера агента управления;

– службы оперативно-технического управления образуют иерархическую службу за счет включения в сервер интерфейса старшей системы управления;

– сервера служб оперативно-технического и технологического управления могут предоставлять услуги проксирования управляющих воздействий службам того же ранга, что позволяет осуществлять горизонтальную навигацию по системам управления.

Такой подход требует сложной системы контроля прав доступа к объектам мониторинга и управления. Для детального изучения такой системы следует рассмотреть, какие виды прав и полномочий требуется контролировать:

– права доступа должностных лиц (пользователей служб) к каждой службе управления — возможность предоставления услуг управления;

– права на возможность осуществления горизонтального взаимодействия между службами одного ранга;

– права на возможность вертикального взаимодействия между службами старшего и младшего рангов;

– права доступа должностных лиц к удаленным службам управления — возможность осуществления управляющего воздействия на элементы сети соседнего узла связи (пункта управления);

– полномочия должностных лиц локального и удаленных (соседних и старших) узлов связи на возможность мониторинга состояния и параметров элементов сети;

– полномочия должностных лиц локального и удаленных (соседних и старших) узлов связи на выполнения функций управления ассоциированных с каждым элементом сети;

– вычисляемые права полномочия, которые являются следствием назначения или отмены полномочий, указанных в предыдущих перечислениях, — некоторые комплексные правила, которые определяют область видимости и зону ответственности субъекта управления;

– полномочия на инициализацию и контроль процессов управления.

Перечисленные виды прав и полномочий, которые следует учитывать при реализации технических решений по созданию и организации комплекса служб управления телекоммуникациями, требуют наличия единой службы идентификации и контроля доступа. Такая служба должна осуществлять учет должностных лиц, организационных структур и программных средств локального и всех взаимодействующих узлов связи — всех, кто может выступать в качестве пользователей услуг мониторинга и управления.

Следует отметить, что каждое правило на тот или иной вид прав доступа (не полномочий) должно быть продублировано на принимающей и передающей стороне, что усложняет их настройку и синхронизацию. Этот факт позволяет утверждать о необходимости исследования данного вопроса с целью, во-первых, поиска решений по упрощению настройки систем контроля доступа, а во-вторых, с целью исследования вопросов синхронизации полномочий и контроля этих процессов.

Шерстюк Ю.М., Костиков В.В., Курилов Д.А.
Россия, Санкт-Петербург, ЗАО «Институт инфотелекоммуникаций»

СЕРВИСНЫЕ СРЕДСТВА ТЕХНОЛОГИЧЕСКОГО КОНТРОЛЯ ТЕЛЕКОММУНИКАЦИОННОГО ОБОРУДОВАНИЯ

Технологический контроль телекоммуникационного оборудования может осуществляться посредством службы технологического управления (СТУ), образованной на основе предназначенного для этого программного комплекса. Примером такого программного комплекса является разработанное ЗАО «Институт инфотелекоммуникаций» программное изделие «Технологическое управление инфотелекоммуникациями» (ТУ ИТК), позволяющий осуществлять мониторинг и управление средствами инфотелекоммуникаций узла (объекта) связи. Совокупность взаимодействующих СТУ образует сетевую службу технологического управления, в которой для межузлового информационного обмена используются механизмы проксирования и шлюзования.

В силу ряда технических решений, реализованных в ТУ ИТК, природа объектов мониторинга и управления (ОМУ) не существенна. Благодаря возможности применения метаданных (наборов данных технологического управления (НДТУ)), разрабатываемых для классов ОМУ, в контур технологического контроля и управления могут быть включены любые ОМУ, в состав которых входят агенты управления.

В ТУ ИТК поддерживаются протоколы взаимодействия с ОМУ SNMP и XMLNMP. В случае, когда агент управления предполагает применение другого протокола взаимодействия, разрабатываются программные шлюзы – конверторы протоколов.

Также в ТУ ИТК, по правилам, зафиксированным в НДТУ осуществляется вычисление интегральной оценки состояния ОМУ по данным их контроля (значениям объектов MIB), а также интегральная оценка состояния всей СТУ – как «худшее» состояние из всех контролируемых ОМУ.

Вышеизложенное, в частности, дает возможность реализовать на практике следующее техническое решение, актуальное при размещении телекоммуникационного оборудования в одном телекоммуникационном шкафу:

– в шкаф помещается управляющая ЭВМ, имеющая не менее двух сетевых интерфейсов, с установленным и функционирующим на ней программным комплексом ТУ ИТК с необходимыми НДТУ и программами – шлюзами исходя из номенклатуры оборудования – ОМУ в данном шкафу;

– к одному интерфейсу управляющей ЭВМ подключается коммутатор локальной вычислительной сети, также размещаемый в этом шкафу, а к нему – интерфейсы (порты) управления всего остального оборудования, выступающего в качестве ОМУ;

– остальные интерфейсы управляющей ЭВМ используются для ее включения в локальную вычислительную сеть узла и/или транспортную сеть системы сетевого управления;

– к управляющей ЭВМ также могут быть подключены датчик вскрытия двери шкафа, датчики температуры и влажности – благодаря этому указанные датчики становятся ОМУ в СТУ;

– к управляющей ЭВМ может быть подключено устройство отображения – например, светодиодная матрица, управляемая отдельной программной, которая устанавливает цвет свечения в зависимости от интегральной оценки состояния СТУ.

Тем самым, в рамках шкафа с телекоммуникационным оборудованием образуется локальная СТУ, имеющая собственную физически выделенную подсеть мониторинга и управления, и позволяющая дополнительно контролировать условия работы оборудования и факты несанкционированного физического доступа к нему. Подобная СТУ доступна через механизмы проксирования и шлюзования для локальной или удаленной СТУ узла, что позволяет применять различные варианты построения сетевой системы управления. Датчики и их программы - агенты управления с соответствующими НДТУ, а также устройство отображения с программой управления для него в этом случае составляют сервисные средства технологического контроля телекоммуникационного оборудования, расширяющие возможности ТУ ИТК.

Шерстюк Ю.М., Логинов А.А., Олимпиев А.А., Шерстюк К.Ю.
Россия, Санкт-Петербург, ЗАО «Институт инфотелекоммуникаций»

МИГРАЦИЯ ПОЛНОМОЧИЙ УПРАВЛЕНИЯ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

Рассмотрению подлежит подсистема управления функционированием в составе АСУС, образованная службами оперативно-технического и технологического управления. Основой каждой из служб является программный компонент, выполняющий функции сервера, назначением которого является централизованное хранение учетных сведений об объектах мониторинга и управления, находящихся в его зоне ответственности, а также мониторинг состояния и управление этими объектами.

Зоной ответственности сервера технологического управления является узел связи, где он функционирует. Зоной ответственности сервера оперативно-технического управления является одна или несколько зон связи, организационно подчиненных пункту управления, где функционирует программный компонент. Пункты управления, как и узлы связи, образуют иерархическую структуру на основе правил их организационной подчиненности друг другу. В иерархической структуре роль старшего узла связи выполняет главный пункт управления, на котором сосредоточена информация о всей системе связи.

Для повышения устойчивости централизованного управления сетью связи в различных условиях обстановки в подсистеме управления функционированием целесообразно иметь запасной пункт управления, дублирующий функции главного пункта управления. Поскольку в любой момент времени основным может быть только один пункт управления (главный или запасной), интерес представляет организация и техническая реализация процессов миграции полномочий на управление объектами между этими пунктами управления.

В общем случае задача миграции полномочий между главным и запасным пунктом управления может быть решена разработкой программного комплекса со следующими характеристиками:

– в состав комплекса входит сервер изменения статуса, АРМ дежурного по контролю за статусом и агент управления статуса, функционирующий на каждом узле связи и пункте управления;

– центральным понятием информационной модели комплекса является понятие статуса пункта управления (значение статуса пункта управления зависит от наличия соответствующих полномочий на мониторинг и управления объектами);

– множество значений статуса пункта управления состоит из следующих элементов: «Резервный», «Резервный – готов к переходу в основной», «Переход к основному», «Основной», «Основной – готов к переходу к резервному», «Переход к резервному», – характеризующих состояние пункта управления как конечного автомата;

– сервер осуществляет контроль доступности агентов смены статуса, которые в свою очередь отвечают за контроль и актуализацию полномочий на подчиненных узлах связи и пунктах управления;

– для осуществления изменения статуса пунктов предусмотрен ряд условий, являющийся достаточным для однозначного определения необходимости осуществления перехода между состояниями (к таким условиям относится доступность агентов изменения статуса, находящихся в подчинении у главного пункта управления — вертикальный контроль, доступность агентов пунктов управления — горизонтальный контроль).

В случае выполнения условий изменения статуса осуществляется предупреждение (сигнализация) дежурного об обнаружении ситуации, в результате которой возможен автоматический или ручной перевод статуса пункта управления из состояния «Резервный» в «Основной». В процессе перехода из первого режима во второй агенты изменения статуса получают команду на переключение полномочий на мониторинг и управление объектами. В режиме «Резервный» пункта управления его должностные лица имеют полномочия только на мониторинг состоянием ключевых телекоммуникационных элементов системы связи, в режиме «Основной» – должностным лицам доступны для мониторинга и управления все элементы системы. Обратный переход в режим «Резервный» должен осуществляться вручную после урегулирования сложившейся обстановки.

Таким образом, сервер и агентов изменения статуса можно представить как множество взаимодействующих конечных автоматов двух типов, что существенно упрощает реализацию указанного выше программного комплекса.

Шерстюк Ю.М., Логинов А.А., Рожнов М.Д., Таран В.В.
Россия, Санкт-Петербург, ЗАО «Институт инфотелекоммуникаций»

УРОВНИ ЗАЩИТЫ СРЕДСТВ ОПЕРАТИВНОГО УПРАВЛЕНИЯ ТЕЛЕКОММУНИКАЦИЯМИ

Как и любая информационно-управляющая система, система оперативного управления телекоммуникациями (СОУТК) требует защиты от несанкционированного доступа (НСД) – и не только к информации, но и к сервисам / средствам управления оборудованием, сетями и услугами.

Можно выделить три основных логически связанных области защиты от НСД в СОУТК – телекоммуникационное оборудование, вычислительные и транспортные сети, программно-аппаратные комплексы и средства управления. Применительно к современным программно-аппаратным комплексам и средствам управления (разного рода комплексов сервисных, терминальных, периферийных, АРМ) в общем случае можно определить следующие базовые уровни защиты:

– физический уровень, на котором осуществляется защита от НСД субъектов к средствам управления – модули доверенной загрузки, охранные датчики и цепи и т.д.;

– уровень операционной системы – средства и механизмы, реализованные на уровне операционной системы – средства поддержки мандатного и дискреционного разграничения доступа, очистки памяти и т.д.;

– уровень «надсистемный» - средства защиты, дополняющие возможности операционной системы и инвариантные по отношению к прикладному программному обеспечению;

– уровень общего программного обеспечения – средства защиты, реализованные в системах управления базами данных, офисных приложениях и т.д.;

– прикладной уровень, или уровень прикладного программного обеспечения.

Следует отметить, что криптосредства могут использоваться на любых уровнях средств защиты и протоколов обмена данными для защиты хранимых данных / передаваемого трафика.

Наиболее сложным и специфичным для каждой СОУТК является прикладной уровень.

Если придерживаться парадигмы служб управления, образуемых прикладным (функциональным) программным обеспечением, то уровень прикладного программного обеспечения можно считать уровнем служб управления, для которого существуют следующие понятия, применимые к локальным и удаленным субъектам и службам управления:

– права доступа к службе;

– полномочия в службе.

Права доступа к службе в клиент-серверной архитектуре означают возможность аутентификации и идентификации клиента по отношению к серверу, определения его роли (например – локальный или удаленный пользователь, администратор).

Полномочия в службе – это полномочия на использование ресурсов службы и/или ее сервисов (функциональных возможностей), возможно – сопоставленные с объектами мониторинга и управления.

Так, например, в службе технологического управления полномочия могут быть определены по отношению к каждому управляемому оборудованию и заключаться в возможности мониторинга состояния оборудования или возможности выполнения отдельных или всех функций управления (управление состоянием интерфейсов, маршрутами, кросс-коммутацией, политиками и т.д.).

Комплексное сбалансированное применение средств защиты всех уровней дает возможность с определенной вероятностью гарантировать требуемую степень защищенности СОУТК от НСД.

Шубников М.М.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова

РАДИОЛОКАЦИЯ И РАДИОНАВИГАЦИЯ

Радиолокация – метод обнаружения, определения местонахождения объектов, а так же определение их свойств и характеристик посредством радиоволн. Эти волны излучаются радиолокационной станцией, отражаются от объекта и возвращаются на станцию. Радионавигация является достаточно близким термином, однако, в радионавигации более активную роль играет объект, координаты которого измеряются.

Радиолокационные станции играют важную роль в обеспечении безопасного плавания в условиях недостаточной видимости. Их главное назначение – обеспечение обнаружения судов, буев, других надводных объектов и препятствий, а так же береговой черты и навигационных знаков. При этом они способны обнаружить объекты, находящиеся не только непосредственно в области видимости, но и находящиеся за линией горизонта.

Выделяют два вида радиолокации: пассивная и активная. Пассивная радиолокация основана на приеме собственного излучения объекта. При активной радиолокации радар излучает импульс и принимает его отраженным от цели. Активная радиолокация бывает так же двух видов: с пассивным ответом и с активным ответом. С пассивным ответом – запросный сигнал отражается от объекта и воспринимается в пункте приёма как ответный. С активным ответом – на объекте находится радиопередатчик, который излучает радиоволны в ответ на принятый от радара сигнал. Активный ответ применяется для опознавания объектов, а так же для получения дополнительной информации.

Наибольшее распространение получили импульсные радиолокационные станции. Так как излучение зондирующего импульса заканчивается раньше времени прихода отраженного сигнала, для передачи и приема в импульсных радиолокационных станциях служит одна и та же антенна. В судовых навигационных РЛС почти всегда используется именно импульсный метод. Он позволяет обнаруживать и наблюдать на экране радиолокатора одновременно большое количество целей, то есть контролировать всю окружающую обстановку в радиусе действия станции. Такая РЛС периодически излучает кратковременные импульсы колебаний сверхвысокочастотных излучений, а в промежутке принимает отраженные от объектов импульсные сигналы, запаздывающие на кратковременные интервалы. По этим интервалам определяется расстояние или дальность объекта, а с помощью антенны – направление на обнаруженный объект.

Одной из основных характеристик импульсных РЛС является длина излучаемой волны. Чем больше длина волны, тем больше расстояние, на которое «видит» станция, в то же время, тем короче волна, тем выше точность определения расстояния до объекта. В корабельных и наземных РЛС используются главным образом дециметровые и сантиметровые волны.

Судовые навигационные РЛС должны быть построены таким образом, чтобы одновременно обеспечивать круговой обзор, дающий возможность контролировать окружающую обстановку, обнаружение больших и маленьких надводных объектов, отображение на экране движения объектов, надежность работы, простоту обращения, работоспособность в условиях плохой погоды, при этом иметь относительно небольшие габариты.

Основной проблемой радиолокации является дальность действия локатора. Для того чтобы увеличить дальность действия в 10 раз, необходимо увеличить мощность в 10000 раз. Таким образом, попытки увеличить дальность быстро подошли к возможным пределам, которые непросто преодолеть. Было проведено много исследований по модификации излучаемого сигнала, изменении передающих устройств с целью как-либо преодолеть этот барьер. Некоторые разработки позволяли увеличить радиус действия и находили свою область применения, но, тем не менее, исследования продолжаются, продолжается поиск альтернативных вариантов построения систем, которые так же помогут решить проблему дальности действия.

Ющенко Н.А., Тулупьева Т.В.
Россия, Санкт-Петербург, Северо-Западный институт управления РАНХиГС,
Санкт-Петербургский институт информатики и автоматизации РАН

КЛАССИФИКАЦИЯ ПУБЛИКУЕМЫХ ПОСТОВ В АККАУНТАХ ПОЛЬЗОВАТЕЛЕЙ СОЦИАЛЬНЫХ СЕТЕЙ

Социальные сети, как широкое информационное поле, образуют особую реальность «Онлайн» и вследствие этого рождают новую культуру со своими понятиями, ценностями, образом мыслей и языком, которая на сегодняшний день является одной из главных составляющих становления информационного общества. Неоднозначность влияния социальных сетей на молодежь вызывает интерес к изучению этой проблемы. Анализ социальных сетей дает интересные данные при изучении как индивидуального, так и коллективного поведения. Поэтому возникает необходимость исследования процессов, отражающих ценности современной молодежи в социальных сетях. Для этого должен быть разработан и использован объективный и в достаточной степени формализованный инструментарий, допускающий в последующем автоматизацию на основе компьютерных технологий.

Одним из способов исследования данной проблемы является анализ интернет-контента пользователей социальных сетей: изучение наполняемости фотографиями, видео, музыкой, постами групп и пабликов, анализ комментариев пользователя аккаунта и другое.

На данном этапе исследования мы подробно останавливаемся на анализе публикуемых постов пользователями социальных сетей и предлагаем их классификацию.

По месту возникновения посты могут классифицироваться следующим образом:

– внутренние. Посты публикуются на личной странице пользователя, т.е. автор текста и владелец аккаунта – это один пользователь социальной сети;

– внешние. Посты публикуются на страницах других пользователей или в группах, т.е. автор текста и владелец аккаунта – это два (или более в случае группы) пользователя социальной сети.

По способу отображения посты могут подразделяться на:

– текстовые. Посты, содержащие последовательность символов, выраженную в словах, словосочетаниях, предложениях.

– аудиальные. Посты, содержащие прикрепленный файл с аудиозаписью.

– визуальные. Посты, содержащие прикрепленный файл с картинкой или фотографией.

– смешанные. Посты с использованием нескольких типов одновременно. Например, картинка и аудиозапись.

По жанрам постов можно выделить следующие:

– информационный пост;
– новостной пост;
– мотивационный пост;
– образовательный пост;
– эмоциональный пост;
– рекламный пост;
– «продажный» пост;
– пост-цитата;
– пост - «личный опыт»;
– пост-возмущение;
– пост-хвастовство;
– пост-развлечение.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ

Алексеев А.В.
Россия, Санкт-Петербург, Институт автоматизации процессов борьбы за живучесть корабля, судна

КОНЦЕПЦИЯ РАНГОВОЙ ПАРТНЕРСКОЙ СЕРТИФИКАЦИИ СИСТЕМ ОБРАБОТКИ И ЗАЩИТЫ ИНФОРМАЦИИ КАК СРЕДСТВО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЭКСПЛУАТАЦИИ И КОНКУРЕНТНОСПОСОБНОСТИ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ

Важнейшая особенность современного этапа развития систем обработки и защиты информации (СОЗИ) в критических инфраструктурах, вызванная бурным ростом информационных технологий, состоит в том, что сегодня всё большее значение приобретает адекватный учёт факторов их сложности, информационно-технической насыщенности, оценки и анализа их качества и конкурентной способности. И, в первую очередь, при сертификации СОЗИ. Особенно ярко это проявляется в отношении объектов повышенного риска, включая ядерные суда, супертанкеры, химовозы, стационарные ледостойкие морские платформы и другие.

Анализ практики проведения сертификационных испытаний СОЗИ с проверкой преимущественно факта выполнения требований, определенных стандартами, техническими регламентами или условиями договоров, без соответствующего измерения оцениваемых характеристик и, тем самым, измерения их качества далеко не полно отражает само качество СОЗИ, не учитывает величину «запаса» по качеству в сравнении уровнем, предусмотренным в соответствующих требованиях. Более того, это не позволяет ранжировать объекты сравнения по достигаемому уровню качества, фактически оценивать их конкурентную способность, уровень безопасности эксплуатации, оптимизировать параметры проектирования и применения.

Таким образом, использование только факта сертификации не позволяет оценивать их конкурентную способность, не дает возможности сузить область неопределенности оценивания качества СОЗИ и, особенно, при использовании сравнительной шкалы оценок.

Практика многочисленных сравнительных оценок качества современных сложных СОЗИ в критических инфраструктурах показывает, что одним из нереализованных ресурсов обеспечения информационной и безопасности в целом в настоящее время является должное обеспечение «информационной прозрачности», как того требуют Доктрина информационной безопасности (2000), ФЗ №184-2002 «О техническом регулировании». В том числе, наряду с публикацией государственных реестров сертифицированных средств (www.fstec.ru) этому во многом будет способствовать публикация актов и протоколов проведения сертификационных испытаний, содержащих весьма ценную информацию, необходимую для исследователей, разработчиков, проектировщиков, конструкторов, менеджеров, маркетологов и многих других при формировании модели качества объектов сравнения, обоснования концепций, стратегий, программ и планов развития СОЗИ, обеспечения их конкурентной способности.

Другим важнейшим механизмом обеспечения безопасности эксплуатации и конкурентоспособности в критических инфраструктурах должен быть переход к новой ранговой (квалиметрической) концепции оценки и сертификации качества современных СОЗИ, а также аттестации объектов информатизации (концепции РСА) на основе количественного измерения и ранжирования качества СОЗИ, как основной их системной характеристики.

Практическое решение проблемы повышения качества создаваемых СОЗИ по пути их технологического развития на основе реализации концепции РСА в контексте парадигмы информационной безопасности и конкурентоспособности СОЗИ является одним из наиболее доступных, реальных и системно целесообразных путей, а также способов обеспечения конкурентной способности СОЗИ, минимизации потребительского риска при их использовании и развитии.

Реализация концепции РСА наряду с повышением корпоративного и национального имиджа технологического развития открывает уникальную возможность выхода на мировой рынок с соответствующей методологической, метрологической, технологической и фактологической «аргументацией открытого типа». При этом, не вступая в противоречие с тенденцией и концепцией внедрения международных стандартов ISO 9000-2005 и, более того, в контексте их развития будет вполне своевременным и уместным определиться с национальными технологическими возможностями в «своей» нише продуктов и услуг. Четко очертив при этом её границы, в первую очередь, применительно к объектам критических инфраструктур, с последующим их расширением за

счет концентрации реальных ресурсов на наиболее предпочтительных направлениях, включая конкурентоспособные с мировыми лидерами, тем самым будет обеспечено качественное повышение информационной и в целом безопасности эксплуатации на ключевых объектах информатизации. При этом, известная проблема методической сложности, верификации и валидности оценивания качества СОЗИ, как показывает анализ практик последних десятилетий, может быть успешно решена на основе полимодельного подхода с соответствующим агрегированием получаемых оценок и неизбежным развитием самих методик и технологий оценивания за счет возможности сопоставления получаемых результатов в сопоставимых условиях и с соответствующим повышением их качества.

Алексеев А.В., Марченко А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

ИНФОРМАЦИОННАЯ СИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЭКСПЛУАТАЦИИ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ

Одной из актуальных проблем развития систем обеспечения информационной и в целом безопасности объектов морской техники и инфраструктуры является поиск оптимальных системных и технологических решений по информационной безопасности и поддержке (ИБП) судоводителя при комплексной оценке и мониторинге состояния безопасности эксплуатации (БЭ), локализации аварий (ЛА) и борьбе за живучесть корабля, судна (БЖКС).

С интенсивным развитием функциональности, информативности и соответствующим ростом сложности современных систем и комплексов автоматизированного управления кораблем, судном проблема ИБП лишь обостряется и становится критичной. Особенно, при объеме представляемой судоводителю информации, превышающем возможности её адекватного восприятия, анализа и эффективного использования, в том числе в экстремальных условиях БЖКС. Данная тенденция становится все более устойчивой, что требует своевременной её нейтрализации.

Одним из возможных и конструктивных направлений решения данной проблемы, как показывает опыт и результаты специальных исследований, является переход к парадигме бинарной визуализации многомерных данных при оценке и мониторинге состояния БЖКС. Это позволяет за счет отказа от отображения многочисленных и, подчас, малозначимых данных и перехода к (2…4) – разрядной (с цветовым кодированием) визуализации, прежде всего, агрегированных данных системного уровня при ИБП судоводителя создать информационно комфортную обстановку эксплуатации, оценки обстановки.

Более того, непрерывный мониторинг и регистрация комплексных показателей состояния живучести технических средств и оружия, непотопляемости корабля, судна, его взрывопожаробезопасности, защищенности (безопасности службы) экипажа судна, устойчивости системы управления (управляемости) системы обеспечения БЖКС с соответствующим интегрированным показателем живучести корабля, судна позволяет судоводителю комплексно и в кратчайшее время воспринимать системные показатели состояния корабля, судна и принимать эффективные управленческие решения. В том числе, из состава вариантов, предлагаемых системой ИБП судоводителя.

Использование бинарного или 2-х битового цветового кодирования уровней БЭ (например, более 90% – «нормальное состояние», зеленым цветом; (90…95)% – «угроза БЭ», желтым цветом; >95% – «аварийная ситуация», красным цветом) и визуализация только данных по техническим средствам, вышедшим из «штатного» состояния, позволяет представлять судоводителю развитие аварийных ситуаций и БЖКС в виде специфических визуальных образов.

Их ассоциативное восприятие, анализ и интерпретация (с учетом данных обучения по типовым вариантам, опыта и т.п.) отличаются от традиционных минимизацией информационной избыточности, существенным сокращением времени и повышением безошибочности. Именно это имеет особенно важное значение в экстремальных условиях БЖКС. Более того, комплексирование и визуализация аналогичным образом данных по БЭ, ЛА и БЖКС с данными по срокам и качеству выполнения технических регламентов, ремонтных работ и т.п. позволяет классифицировать и идентифицировать варианты развития АС в удобной форме и перейти при решении задач ИБП к парадигме автоматического обнаружения и обработки образов. Это позволяет существенно снизить уровень информационно-психологической напряженности судоводителя при принятии решений, минимизировать уровень возможных ошибочных решений.

Вместе с тем, бинарная визуализация данных повышает требования к научно-технической обоснованности и точности используемых моделей оценки групповых и сводных показателей качества, контролю погрешностей оценок. Это требует выполнения комплекса исследований по отработке алгоритмов ситуационного моделирования, поиска эффективных и оптимальных вариантов видеосцен (интерфейсных форм), вариантов информационно-технического сопряжения возможностей средств автоматизации процессов БЖКС с психофизиологическими возможностями операторов. В том числе формирования и использования когнитивных баз данных и знаний на основе

теории нечетких множеств и теории квалиметрической ранговой оптимизации решений, методов и технологий экспертного оценивания, управления структурной динамикой, мультиагентного и 3D-моделирования, нейросетевого моделирования.

Практика построения и оптимизации интерфейсных форм обеспечения ИБП судоводителя, разработка технологии их реализации и результаты проведенных испытаний подтвердили возможность рекомендации концепции бинарной визуализации многомерных данных для широкого круга систем обработки и защиты информации, характеризующихся высоким динамизмом, непредсказуемостью ситуаций и информационных инцидентов и сложностью их распознавания.

Верховых Н.И., Перепелкина С.Ю., Франк А.В.
Россия, Екатеринбург, ФГУП «Научно-производственное объединение автоматики имени академика Н.А. Семихатова»

ВОССТАНОВЛЕНИЯ ТЕЛЕМЕТРИЧЕСКОЙ ИНФОРМАЦИИ В УСЛОВИЯХ ИЗБЫТОЧНОСТИ

Цифровая телеметрическая информация (ЦТМИ), зарегистрированная в ходе летных испытаний и запусков ракетно-космической техники, обладает большой значимостью в целях подтверждения правильности функционирования изделия в целом и, в том числе, системы управления. Полученная при этом информация зачастую является неполной или искаженной за счет ошибок в процессе приема-передачи, вызванных различного рода атмосферными помехами, изменением направленности антенн изделия относительно Земли на участках разделения ступеней и пр.

В обеспечение гарантированного послеполетного восстановления информации используется ряд технических и программных решений, к которым относятся:

– наземная избыточность – регистрация ЦТМИ отдельными измерительными пунктами, имеющими перекрываемые зоны видимости;

– бортовая избыточность аппаратуры системы телеметрических измерений – включение в ее состав кольцевого запоминающего устройства, обеспечивающего временную задержку повторной выдачи информации в эфир;

– бортовая избыточность аппаратуры системы управления – дублирование информации на выходе специализированного телеметрического вычислительного устройства (УСВТ);

– информационная избыточность кадра ЦТМИ – частичное дублирование информации непосредственно в составе кадра и введение контрольных сумм;

– контрольные точки кадра ЦТМИ, связанные с особенностями построения кадра ЦТМИ (маркерная группа слов, соответствующая началу кадра, счетчик циклов, счетчики частот, признаки достоверности, признаки четности и т.д.).

В рамках решения задачи парирования ошибок приема-передачи ЦТМИ ФГУП "НПО автоматики" было разработано специализированное программно-математическое обеспечение, позволяющее автоматизировать процесс формирования единого потока информации (ЕПИ), содержащего максимально полную и достоверную ЦТМИ.

Первоочередной задачей формирования ЕПИ является совмещение потоков ЦТМИ, зарегистрированных различными измерительными пунктами, с использованием соответствующих синхронизирующих поправок временной шкалы. Непосредственный сам процесс обработки ЦТМИ и формирования ЕПИ можно разделить на следующие этапы:

– ранжирование кадров по принципу достоверности;
– контроль и восстановление номера цикла;
– поиск «потерянных» маркерных групп (кадров);
– формирование содержимого кадра.

На первом этапе происходит поиск максимально «чистых» кадров в потоке телеметрической информации и определение весового коэффициента найденного кадра. На втором этапе происходит контроль полученных кадров на монотонность с учетом изменения счетчика цикла и принудительное назначение счетчика цикла кадрам, нарушающим принцип монотонности. На следующем этапе происходит попытка найти кадры по более «мягким» критериям и присвоение номера счетчику циклов на основе принципа монотонности. На последнем этапе происходит непосредственно формирование ЕПИ путем совмещения информации с отдельных измерительных пунктов и использованием весовых коэффициентов достоверности. Полученный ЕПИ предоставляется разработчикам отдельных систем для дальнейшего анализа алгоритмов.

Программа формирования ЕПИ реализована в среде Lazarus, позволяющей получать готовый программный продукт для различных операционных систем (Windows, Linux). Программа предусматривает возможность адаптации под конкретную структуру кадра ЦТМИ текущих и перспективных разработок посредством выделения характерных особенностей кадра ЦТМИ и ряда сложно формализуемых настроек в отдельные динамические библиотеки, созданные под конкретный заказ.

Дмитриев А.Г., Михайленко Е.И., Стефановская Н.В.
Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс»

ПРОТОКОЛ РЕГУЛИРУЕМОГО ВИРТУАЛЬНОГО КАНАЛА ВИРТУАЛЬНОЙ ПРИВАТНОЙ СЕТИ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Данный протокол определяет логическое взаимодействие между двумя объектами по организации регулируемого виртуального канала (Regulation Virtual Channel) через IP сеть. Протокол обеспечивает возможность достоверной доставки пакетов данных удаленной стороне с квитированием доставки. Квитирование позволяет регулировать поток данных в виртуальном канале и избегать перегрузок. Протокол определяет форматы и состав кадров виртуального канала (далее VC-кадр), а также алгоритм обмена VC-кадрами через IP сеть.

Формат и состав кадров протокола RVCP. Протокол RVCP строится на основе кадрового протокола LAPB [ITU-T Recommendation X25], но реализуется на транспортном уровне, над протоколом IP. Каждый кадр протокола инкапсулируется в IP-пакет, который имеет следующие установленные поля:

– IP-адрес источника, равный IP-адресу сетевого порта;
– IP-адрес назначения, равный IP-адресу респондента, устанавливаемому для каждого виртуального канала;
– поле TOS;
– номер протокола.

Формат и состав кадров протокола RVCP, а так же алгоритм обмена кадрами соответствует описанию протокола LAPB. Есть некоторые особенности по установке параметров протокола, которые описаны далее.

Все кадры перед инкапсуляцией в IP дополняются в конце контрольной суммой, которая записывается и проверяется при приеме на удаленной стороне.

Параметры протокола RVCP. Протокол LAPB имеет несколько основных конфигурационных параметров, определяющих его работу: T1, N2, K, режим DTE/DCE. В рамках протокола RVCP они определяются следующим образом:

– T1 – тайм-аут повторной передачи. Может быть изменен через конфигурационный параметр.
– N2 – количество повторов.
– K – размер кадрового окна.

Режим DTE/DCE. Режимы DCE и DTE могут быть установлены через конфигурационный параметр.

Дополнительно, протокол RVCP определяет еще один параметр id, который обеспечивает идентификацию при установлении нескольких логических каналов к одному удаленному респонденту. Параметр id должен устанавливаться одинаковым на обеих сторонах логического канала.

Емелин В.И. Михайлов Д.С.
Россия, Санкт-Петербург, ОАО «Научно-исследовательский институт «Вектор»

ОЦЕНКА И ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ УСТОЙЧИВОСТИ В КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТАХ

Рассматриваются критически важные объекты (КВО), которые отличаются следующими специфическими особенностями: 1) в информационную систему поступает непрерывный поток постоянно обновляющихся данных в реальном масштабе времени, 2) появление информационных ошибок приводит к неприемлемой величине ущерба. Считается, что любая информационная система критически важных объектов при добывании данных находится в состоянии устойчивого или неустойчивого неравновесия. Это связано с непрерывным изменением обстановки в условиях деструктивных информационных воздействий: 1) изменяется количество элементов обстановки, по которым выполняется требования по оперативности их поступления; 2) по мере устаревания и обновления данных изменяется их достоверность; 3) изменяется количество параметров обстановки, соответствующих требованиям по достоверности информации. Все указанные изменения по своей физической сущности соответствуют определению модификации информации – несоответствию данных, поступающих в информационную систему, реальным данным среды, которые наблюдаются и измеряются в КВО. Несоответствие оценивается по информационным показателям, как способность системы обеспечить заданный уровень качества информации (полнота, достоверность и оперативность) в условиях случайного или преднамеренного воздействия (искажения). Неравновесность – неодинаковость параметров информационной системы и среды – проявляется в непрерывных колебательных процессах, происходящих в течение каждого цикла обновления сведений об обстановке и последующего их старения. При этом предполагается, что обновление сведений может осуществляться дезинформацией.

Предлагается метод качественной оценки информационной устойчивости КВО, в которой сведения о среде формируют следующие 3 класса возможных состояний системы: 1) состояние устойчивого информационного неравновесия системы, в котором область определения параметров

приводит к выбору плана действий, основанного на дезинформации и исключающего возможность достижение цели управления; 2) состояние устойчивого информационного неравновесия системы, в котором область определения параметров приводит к выбору плана действий, обеспечивающего достижение цели управления; 3) состояние неустойчивого неравновесия системы, область определения которого при незначительных информационных воздействиях может привести к выбору любого плана.

Метод основан на определении Юсуповым Р.М. понятия информационной безопасности как следующей триады: защиты информации, защиты от информации и информированности (осведомленности) субъекта о намерениях и возможностях противоборствующей стороны в информационной сфере. В предлагаемом методе качественной оценки значительную роль играет положение аттрактора, которое определяется по критерию информированности как сложное свойство, характеризующее способность субъекта, используя имеющиеся у него информацию, сведения и знания, формировать правильные суждения и вырабатывать на их основе правильные решения в процессе своей деятельности. Уровень информированности определяется как удаленность характеризуемого состояния, от состояния полной не информированности, которому соответствуют исходные значения полноты, своевременности и достоверности информации. Такое понимание информированности позволяет связать его уровень с вероятностью формирования правильного суждения и выработки правильного решения. Это дает возможность использовать в качестве показателей информированности соответствующие вероятностные характеристики. Результатом проведенных вычислений является установление взаимосвязи между пространством, описывающим возможные состояния структуры, и внутренним пространством этой структуры как сложного объекта. В состояниях устойчивого неравновесия управление КВО является детерминированным, в состоянии неустойчивого неравновесия для процесса управления характерно не только упорядоченное, регулярное движение, но и случайное изменение состояния.

Информационная устойчивость систем обеспечивается формированием системы знаний, которая определяет задание таких начальных условий, при котором аттрактор расположен в области устойчивого неравновесия с высоким качеством информации. В этом случае созданный уровень информированности будет притягивать все траектории, построенные из значений ее текущих оценок. Высокий уровень достоверности и валидности знаний позволяет выявлять поступление модифицированных данных.

Завадский С.В. Филиппова Т.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет,
ОАО «Научно-производственное объединение «Импульс»

ВЫСОКОТЕХНОЛОГИЧНЫЕ ИНТЕГРИРОВАННЫЕ РЕШЕНИЯ В ЗАДАЧАХ РАЗРАБОТКИ И ТЕСТИРОВАНИЯ АППАРАТУРЫ ПЕРЕДАЧИ ДАННЫХ

Важной задачей при разработке аппаратуры и интегрированного с ней программного обеспечения является достижение целей процесса верификации качества, особенно, при создании узлов и систем объектов критической инфраструктуры. В отдельных случаях по требованию заказчика, выполняется разработка и поставка ответственного ПО на платформе, использующей только отечественную элементную базу. При этом процесс верификации качества должен быть применён на всех стадиях конструирования и разработки, начиная от стадии проектирования архитектуры и выбора алгоритмов, и заканчивая автоматизированным контролем качества выпускаемых серийных изделий. Нередко при разработке программно-аппаратных систем наращивание функционала идёт итеративно, тогда задачи верификации качества ставятся на каждой итерации. Как известно стоимость внесения изменений в сложную систему растёт экспоненциально, поэтому правильная организация процесса макетирования и тестирования позволяет не просто значительно снизить время и стоимость разработки, а оказаться необходимым условием успешного выпуска программно-аппаратного комплекса, его развёртывания и дальнейшей поддержки.

Платформой для процесса верификационного тестирования выступает единый программно-аппаратный комплекс, в задачи которого входит проверка отклика и функционирования изделия при воздействии заданными цифровыми и аналоговыми сигналами, имитации управляющих команд и режимов, симуляции различных параметров канала и электротехнических условий и макетировании поведения всех узлов и абонентов системы в целом. Автоматизирующее программное обеспечение комплекса рассчитано сопровождать весь жизненный цикл разработки изделия, и организовано таким образом, чтобы по команде оператора запускался сценарий, последовательно выполняющий все этапы диагностики. Немаловажную роль играют введённые в состав диагностики так называемые «обрушивающие тесты», то есть воздействия, проверяющие штатную отработку изделием различных критических ситуаций.

Основной проблемой описанной концепции является реализация целого спектра тестовых алгоритмов, покрывающего всё разнообразие задач верификации качества, на единой диагностической аппаратной базе.

Решение данной проблемы основано на применении в качестве единой диагностической платформы высокотехнологичного измерительного комплекса фирмы National Instruments на шине PXI. Представленный комплекс тесно интегрирован с современными визуальными средами программирования прикладного уровня, такими как NI LabView, MS VisualStudio.NET (C++/C#), MS SQL Server, Matworks MatLab, Simulink. Это позволяет выбрать наиболее удобную среду для реализации каждого из тестирующих алгоритмов. Причём, не зависимо от выбранного инструментария, программист имеет единый интерфейс доступа к диагностическим модулям управления источниками питания, измерения вольтамперной характеристики, генератора аналоговых и цифровых последовательностей, оцифровки входящих измерительных сигналов, спектроанализатора и управляемых коннекторов. Макетирование структурно-логических процессов, как, например, сетевое взаимодействие и маршрутизация сетевой информации реализуется на языках C++/C# в среде MS VisualStudio.NET. Тестирование процессов приёма/передачи информации напрямую связано с задачами математической обработки сигнала и моделированием динамических систем в средах математического программирования MatLab и динамического моделирования Simulink. Процесс поиска и локализации неисправности строится на сравнении цифровых и аналоговых последовательностей сигналов сохраняемых/извлекаемых из базы данных, например, MS SQL Server.

Предложенная автоматизация процессов диагностического тестирования аппаратуры передачи данных основана на объединении программ, управляющих высокотехнологичным измерительно-диагностическим комплексом, интегрированным с современными визуальными средами программирования. Это позволяет организовать визуальный интерактивный интерфейс с пользователем, построение графиков осциллограмм процессов, отображение результатов математической обработки сигналов, хранение и извлечение большого количества данных, представляющих эталонные последовательности из базы данных, построение автоматических отчётов и документирование процесса верификации качества.

Зегжда Д.П., Калинин М.О.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет»

РАЗРАБОТКА ИСПЫТАТЕЛЬНОГО ПОЛИГОНА КРИТИЧЕСКИХ ИНФОРМАЦИОННЫХ СРЕД

Автоматизация управления производственными процессами напрямую связана с обеспечением надежного функционирования информационной инфраструктуры, которая представляет собой объект хозяйственного комплекса, отказ которого способен повлиять на национальную безопасность. Компоненты поддержания, управления и защиты информационных систем критически важных социальных и производственных отраслей, а именно: платформы обработки и хранения информации; компоненты АСУ ТП; среда передачи информации; системы и средства защиты информации в совокупности образуют единую критическую информационную среду (КИС).

КИС представляет собой объект защиты, для которого определить, оценить и, в итоге, расширить функциональные возможности с целью обеспечения устойчивого противодействия киберугрозам, позволяет комплекс мероприятий по исследованию безопасности. При этом препятствием для прямого тестирования функций безопасности КИС является множество факторов:

– высокая степень критичности происходящих процессов – определен риск наступления необратимых последствий в случае проведения произвольных экспериментальных воздействий в «боевых» условиях функционирования;

– гетерогенность – система вычислительных и исполнительных (в т.ч. промышленных) компонентов, которые затруднительно развернуть на площадке испытательной лаборатории по техническим и экономическим причинам;

– консервативность – обновления компонентов (в т.ч. установка «патчей» и актуальных обновлений защитных механизмов) требуют предварительной тщательной проверки на совместимость и происходят редко в силу возможной разладки системных процессов.

Воспроизводить реальные сценарии кибератак и поведение средств защиты, подтверждать устойчивость КИС к агрессивным целенаправленным воздействиям, оценивать возможности КИС по противодействию актуальному множеству кибератак, направленных на нарушение конфиденциальности, работоспособности, целостности обрабатываемых данных и функциональных компонентов КИС производя эксперименты на реальной системе невозможно.

Предлагается подход, заключающийся в переносе экспериментов из реальной среды в имитационную, моделирующую в виртуальном окружении состав и функции реальной КИС. Имитационная среда позволяет исследовать КИС на предмет устойчивости защитных механизмов КИС к актуальным киберугрозам и определять условия и механизмы кибератак, подвергаемые воздействиям активы, отрабатывать контрмеры по предотвращению нарушений безопасности. Для реализации такой среды предназначен испытательный полигон (ИП) — высокопроизводительный программно-аппаратных комплекс, который позволяет воспроизводить КИС и автоматизировать

проведение экспериментов по тестированию защитных механизмов на предмет устойчивости к киберугрозам.

ИП отвечает следующим требованиям:

– высокая производительность, достаточная для параллельного тестирования средств защиты и средств активного воздействия на КИС;

– масштабируемость, обеспечивающая тестирование на различных платформах с возможностью подключения новых компонентов;

– актуальность имитируемых кибератак;

– автоматизация оценки быстродействия, предельной нагрузки и качества функционирования средств защиты в критических рабочих режимах;

– автоматизация сценариев тестирования и протоколирования его результатов;

– защита ресурсов и данных тестирования от НСД.

Круг решаемых задач определяет компонентный состав ИП:

– подсистема моделирования — включает подсистему моделирования объекта защиты и подсистему моделирования субъекта нападения;

– подсистема управления и мониторинга — фиксация и оценка результатов активных воздействий на КИС, контроль подсистем полигона, установка обновлений компонентов ИП;

– подсистема защиты — обеспечение безопасного доступа к вычислительным средствам и результатам работы.

При реализации ИП используются передовые компьютерные технологии:

– высокопроизводительная платформа на базе серверов. Производительность аппаратного комплекса и распараллеливаемость вычислений позволяют за счет консолидации вычислительных мощностей и управляемого разделения задач на комплексе виртуальных машин повысить скорость и эффективность тестирования;

– облачный сервис моделирования вычислительных платформ. Виртуальная среда позволяет создавать на базе виртуальных машин модель компьютерной сети необходимых состава, масштаба и топологии на базе различных семейств и версий операционных систем, ПО и пр.;

– использование аппаратной генерации трафика. Применение устройств генерации трафика направлено на обеспечение воспроизводства различных типов кибератак, генерацию экстремальной нагрузки, эмуляцию взаимодействия с различными компьютерными сетями.

Кораблев И.Н., Вологдин М.А., Калугин П.С., Кабанцов К.К.
Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс»

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ УСТОЙЧИВОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ К АТАКАМ ТИПА «ОТКАЗ В ОБСЛУЖИВАНИИ»

Одним из видов сетевых угроз является атака типа «отказ в обслуживании» (Denial-of-service, DOS-атака). Она относится к преднамеренным антропогенным угрозам безопасности информации. Результатом такой атаки могут являться: нарушение доступности конкретной службы, вывод из строя автоматизированных систем управления, создание условий для последующих деструктивных воздействий. Относительно критически важных объектов (далее – КВО), следствием данной атаки может являться нарушение работоспособности и управляемости газодобывающих и газораспределительных систем, электростанций, систем мониторинга и управления транспортом, систем управления водоснабжением и других инфраструктур. В свою очередь это может привести к возникновению чрезвычайной ситуации или к значительным негативным последствиям для обороноспособности, безопасности, международных отношений, экономики, другой сферы хозяйства или инфраструктуры страны, либо для жизнедеятельности населения, проживающего на соответствующей территории, на длительный период времени.

Несмотря на высокую степень угрозы безопасности информации, возникающей вследствие DOS-атаки, в настоящий момент не разработана методика определения степени устойчивости критически важных объектов к данным атакам.

В докладе предложена методика построения математической модели степени устойчивости КВО к атакам типа «отказ в обслуживании».

Уязвимость КВО к DOS-атакам можно представить следующими характеризующими блоками:

– наличие доступа к глобальным сетям общего пользования;

– пропускная способность канала связи;

– неправильно настроенное сетевое оборудование;

– степень подверженности сети КВО к анализу;

– недостатки сетевого ПО (уязвимости);

– ограниченность вычислительных ресурсов.

Данным характеризующим блокам соответствуют следующие угрозы:

– подключение критически важного объекта к глобальным сетям общего пользования;

– наличие у злоумышленника большей полосы пропускания канала;

– возможность добычи злоумышленника исходного кода или реверс-инжиниринг приложений, применяемых на КВО, на предмет уязвимостей;

– наличие у злоумышленника знаний о конфигурации и настройке оборудования;

– качественное и количественное преимущество вычислительных ресурсов злоумышленника над собственными ресурсами КВО.

Вместе с тем, характеризующие блоки могут взаимодействовать между собой, увеличивая или уменьшая общий потенциал устойчивости КВО. Оценивая общий потенциал КВО на текущий момент времени, можно прогнозировать устойчивость самих КВО на то или иное определенное время.

В докладе рассмотрен метод количественного расчета вклада каждого характеризующего блока в устойчивость КВО к DOS-атакам и метод вычисления значения потенциала устойчивости каждого характеризующего блока. Рассмотренные методы позволяют использовать предложенную методику для построения математической модели степени устойчивости КВО к атакам типа «отказ в обслуживании».

Михайленко Е.И.
Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс»

ОСОБЕННОСТИ СЕТЕВОГО ВЗАИМОДЕЙСТВИЯ КРИТИЧЕСКИХ ИНФРАСТРУКТУР С МУЛЬТИСЕРВИСНОЙ СЕТЬЮ ОБЩЕГО ПОЛЬЗОВАНИЯ

Системы критических инфраструктур, в соответствии с предъявляемыми к ним требованиями, должны осуществлять безопасный информационный обмен, в том числе, с использованием ресурсов мультисервисной сети общего пользования. Мультисервисная сеть общего пользования является составной частью единого информационного пространства общей автоматизированной системы управления и базируется на элементах специальных систем связи, а также на транспортных ресурсах, арендованных у операторов связи единой системы электросвязи (ЕСЭ) России.

Мультисервисная сеть общего пользования формируется на современной архитектурной основе сетей связи следующего поколения (NGN) и выполняет функции общей телекоммуникационной транспортной платформы, предоставляющая услуги передачи различных видов трафика с заданным качеством. Общая транспортная платформа включает интегрированную цифровую сеть высокоскоростных каналов связи, унифицированные комплексы средств передачи данных, устанавливаемые на узлах и формирующие магистральную транспортную сеть общего пользования, ресурсы специализированных региональных телекоммуникационных сетей, создаваемых на современных телекоммуникационных технологиях, сети доступа специальных систем к транспортной сети.

Транспортная сеть использует широко распространённую IP-технологию, выделенные виртуальные сети (VPN MPLS, в том числе, GMPLS) и выделенные высокоскоростные цифровые каналы PDH, SDH для привязки специальных систем к узлам операторов связи ЕСЭ России.

Использование оборудования комплексного оснащения объектов критических инфраструктур обеспечивает сопряжение объектов с цифровыми системами передачи и коммутации мультисервисной сети общего пользования. Оборудование комплексного оснащения представлено закрытым и открытым сегментами.

Подключение систем критических инфраструктур к мультисервисной сети общего пользования обеспечивается с использованием IP - шлюза, реализованного в составе объектов этих систем.

IP-шлюз предназначен для организации множества виртуальных каналов через IP-сеть специального назначения. Он работает как устройство доступа к оборудованию комплексного оснащения, конвертируя поступающие от специального сетевого маршрутизатора (СМ) кодограммы в IP-пакеты (и обратно) с подстановкой IP-адресов через таблицу соответствия, вводимую администратором в изделие на этапе настройки.

IP – шлюз подключается к криптомаршрутизатору закрытого сегмента, создающего криптотуннели, через коммутатор локальной сети и межсетевой экран. Оборудование закрытого сегмента подключается к мультисервисной сети общего пользования через граничный маршрутизатор открытого сегмента.

Удаленный доступ организуется с помощью сетей удаленного доступа узлов связи пунктов управления и включает выделенные цифровые каналы, формируемые аппаратурой цифрового каналообразования по волоконно-оптическим линиям связи и по технологии HDSL.

Данная аппаратура формирует цифровые каналы по кабельным магистралям с медными и оптоволоконными жилами, радиорелейным линиям с закрытием служебной информации и информации пользователей. Услуги, предоставляемые данной аппаратурой, обеспечивают совместную передачу шифрованных данных, телефонных переговоров и телеграфной информации, мультиплексируя их в цифровой поток, а также централизованную и децентрализованную систему синхронизации и автоматизированную реконфигурацию и восстановление каналов, трактов по резервным и обходным путям.

Михайленко Е.И., Стефановская Н.В., Фомин В.Н.
Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс»

ПРОГРАММНЫЙ КОМПЛЕКС СОВМЕЩЕННОГО КОММУТАТОРА И IP-ШЛЮЗА ОБЪЕКТА КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Программный комплекс совмещенного коммутатора и IP – шлюза (ПО СКШ) должен обеспечивать внутреннее взаимодействие элементов локальной сети объектов критической инфраструктуры и внешнее – с сетью доступа к IP – сетям. ПО СКШ реализовано на единой аппаратной платформе в рамках единого устройства.

ПО СКШ реализует:

– разделение локальной Ethernet-сети на сегменты и коммутацию Ethernet-кадров между этими сегментами;

– логическое сопряжение территориально-разнесенных комплексов объектов критической инфраструктуры через IP-сеть специального назначения посредством организации множества виртуальных каналов.

ПО СКШ включает:

– программный модуль управления (ПМУ);
– программный модуль IP-шлюза (ПМШ);
– программный модуль коммутации (ПМК).

Программные модули ПО СКШ размещаются и функционируют во флэш-памяти аппаратных модулей устройства. Объём объектного кода каждого программного модуля не превышает 4 Мбайта. Запуск программных модулей производится после подачи электропитания на соответствующие аппаратные модули, а также после программного перезапуска (рестарта).

После запуска (рестарта), а также периодически, каждый программный модуль должен проводить проверку целостности своих исполняемых кодов с помощью подсчёта контрольной суммы и сравнения её с эталоном. Если целостность была нарушена, программный модуль должен прекратить свое функционирование.

ПМУ обеспечивает инициализацию (реинициализацию) всех остальных модулей устройства после своего запуска или рестарта, логическое сопряжение с внешним управляющим устройством в соответствии с Протоколом управления СКШ, пересылку значений данных конфигурации и директив управления (например, директивы рестарта, организации шлейфа) в другие модули устройства после прихода соответствующей директивы от внешнего управляющего устройства. При инициализации ПМУ определяет текущее состояние модуля.

ПМК после своей инициализации со стороны ПМУ инициирует свои Ethernet-контроллеры, устанавливая для них возможность приёма всех Ethernet-кадров с внешних портов.

ПМШ взаимодействует через свой сетевой Ethernet-порт с IP-маршрутизатором с применением и поддержкой соответствующих сетевых протоколов.

Каждый программный модуль в процессе функционирования для защиты от «зависания» использует механизм «watchdog».

Программный комплекс ориентирован на функционирование в операционной среде реального времени и поддерживает возможность управления со стороны управляющего устройства, обеспечивая, в частности, возможность загрузки/чтения данных своей конфигурации. Данные конфигурации представляют собой текстовые файлы в кодировке ASCII, хранящихся в базе данных объектовой сети и доступны для редактирования.

Новиков А.Е.
Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс»

БАЗОВЫЕ ТЕХНОЛОГИИ СОЗДАНИЯ И СОПРОВОЖДЕНИЯ АСУ КРИТИЧЕСКИХ ИНФРАСТРУКТУР

ОАО «НПО «Импульс» на протяжении многолетней производственной деятельности специализируется в области создания автоматизированных систем управления (АСУ) критических инфраструктур, обеспечивая поддержку все этапов жизненного цикла изделия от проектирования до утилизации за счет взаимоувязанных промышленных базовых технологий, отработанных при выполнении заказов МО РФ. Большой опыт разработки и эксплуатации систем на отечественной элементной базе позволил ОАО «НПО «Импульс» создать уникальную инженерную школу разработчиков и отработать базовые технологии проектирования систем. Основные промышленные базовые технологии, обеспечивающие конвейер Главного конструктора при создании АСУ:

– базовая технология управления проектами;
– базовая технология системного проектирования;
– базовая технология разработки аппаратуры и др.

К АСУ критических инфраструктур предъявляются жесткие требования по обеспечению заданного функционала, как в повседневной жизни, так и под воздействием разрушающих и

дестабилизирующих факторов воздействий техногенного, природного характера. Основные требования, предъявляемые к АСУ критических инфраструктур:

– надежность функционирования;
– достоверность обработки информации;
– устойчивость к кибердарам;
– противодействие РЭП;
– расширенный функционал;
– быстродействие (ВВХ) и др.

Промышленные базовые технологии создания новой АСУ предусматривают эффективное применение базовой технологии управления проектами, при помощи которой увязываются стадии выполнения работ, оптимизируется критический путь создания системы и организуется контроль хода выполнения проекта.

Промышленная базовая технология системного проектирования закладывает фундаментальные основы работы создаваемой системы. В ходе системного проектирования формируются системные алгоритмы работы, системные протоколы, архитектуры технических средств и программного обеспечения системы.

Технология конструирования изделий предусматривает создание семейств специализированных базовых несущих конструкций, обеспечивающих устойчивость к воздействию дестабилизирующих и разрушающих факторов внешней среды, а также унификацию базовых конструктивов, эффективный теплоотвод и необходимую эргономику в эксплуатации изделий.

Специфика функционирования АСУ критических инфраструктур диктует специальные требования к технологии разработки аппаратуры. Такие требования, как надежность, кибер-устойчивость, технологическая независимость требуют применения отечественной элементной базы.

В части реализации функций негативного управления и киберустойчивости к штатному ПО АСУ критических инфраструктур предъявляются следующие особые требования:

– технологическая несовместимость с методами ведения кибер-атак;
– контроль целостности вычислительных процессов, массивов данных и аппаратной архитектуры;
– автоматическая деградация и восстановление архитектуры системы при отказах и восстановлениях аппаратной платформы.

Действующие в ОАО «НПО «Импульс» базовые технологии создания АСУ критических инфраструктур отработаны на трех поколениях систем, находящихся в эксплуатации и в настоящее время развиваются с появлением новой отечественной элементной базы, САПР и производственного оборудования в целях повышения функциональности, качества и надежности систем нового поколения.

Ростовцев А.Г.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

СНИЖЕНИЕ СЛОЖНОСТИ ДИФФЕРЕНЦИАЛЬНОЙ АТАКИ НА AES С ИСПОЛЬЗОВАНИЕМ ВИРТУАЛЬНЫХ ИЗОМОРФИЗМОВ

Для атаки на шифры используются как правило статистические методы, в частности, дифференциальный и линейный криптоанализ.

Шифры изоморфны, если существует вычислимая в обе стороны биекция множеств ключей, открытых и зашифрованных текстов. Указанная биекция φ называется изоморфизмом шифров. В общем случае изоморфизм может действовать по-разному на тексты и на ключ.

Изоморфизм подобно шифру может строиться «запутанно», с использованием композиции коротких подстановок и аффинных отображений. При этом желательно, чтобы к анализу каждого (или каждого второго) раунда изоморфизм возвращался в исходное состояние. Поэтому число изоморфизмов шифров чрезвычайно велико.

Это позволяет строить атаки на шифры по следующей схеме: для данного шифра и данного метода криптоанализа подбираем такой изоморфизм, чтобы изоморфный шифр был уязвим. Такие изоморфизмы могут выбираться с использованием очевидных методов оптимизации. Поскольку изоморфизм шифров существует только в воображении криптоаналитика и может им изменяться в широких пределах, назовем его виртуальным.

Примеры виртуальных изоморфизмов.

1. Аффинная эквивалентность подстановок.
2. Эквивалентность, заданная сопряжением.

Дифференциал характеризуется своей вероятностью. Сложность дифференциальной атаки обратно пропорциональна произведению вероятностей дифференциалов подстановок [3]. Поэтому на практике подстановки выбираются так, чтобы вероятность наиболее вероятных дифференциалов

была минимальна. Техника виртуальных изоморфизмов, позволяет предположить, что такой выбор подстановок не увеличивает сложность дифференциальной атаки.

С учетом аффинной эквивалентности все аффинные подстановки эквивалентные единичной подстановке. Выберем подстановку так, чтобы она имела максимальное число неподвижных точек. Эта операция нелинейна, но ее нелинейность мала. Максимальные вероятности дифференциалов этого отображения увеличиваются в среднем в 8,3 раза по сравнению с дифференциалами оригинального AES, то есть вместо 1/64 не превышают 1/8. Виртуальные изоморфизмы могут меняться от раунда к раунду по воле криптоаналитика. Это создает механизм управления дифференциалами. В частности, можно получать дифференциалы вероятности 1. Таким образом, можно предположить, что сложность дифференциального криптоанализа AES с учетом техники виртуальных изоморфизмов не превышает квадратного корня из традиционной оценки.

Найденное противоречие (шифр с наилучшей подстановкой обладает откровенно плохими криптографическими свойствами) позволяет поставить следующий вопрос. Позволяет ли выбор специальных подстановок повысить стойкость шифра, если криптоаналитик использует технику виртуальных изоморфизмов? Для ответа на него был проведен эксперимент для AES, в котором вместо обращения U в конечном поле используются случайные подстановки, состоящие как и U из циклов длины 2.

Эксперимент показал, что при замене подстановки U на случайные подстановки вероятности наиболее вероятных дифференциалов изоморфного шифра практически не меняются (для пяти случайных подстановок). Это позволяет предположить, что выбор специальных подстановок не дает преимуществ по сравнению со случайными подстановками для дифференциального криптоанализа. Этот результат легко объяснить, так как стойкость изоморфного шифра определяется свойствами виртуального изоморфизма, выбираемого криптоаналитиком, а не дифференциалами подстановки.

Аналогичные выводы справедливы в части линейного криптоанализа: стойкость изоморфного (и следовательно оригинального AES) для того же изоморфизма снижается примерно до квадратного корня из существующей оценки, а специальные подстановки не имеют преимуществ по сравнению со случайными.

Приближенная сопряженность подстановок на оценки стойкости шифра AES практически не влияет (на самом деле подстановка U имеет две неподвижных точки из 256).

ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

Левкин И.М., Микадзе С.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

ОСНОВНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ НА СОВРЕМЕННОМ ЭТАПЕ

Одним из основных признаков современного общества является его информационный характер. Все общественно-политические, экономические и иные процессы в таком обществе приобретают информационный характер. Это относится и к различным аспектам национальной безопасности.

Главным компонентом национальной безопасности государства является экономическая безопасность. Одним из важнейших элементов экономической безопасности является информационная сфера. Учитывая постоянно усиливающуюся взаимосвязь экономической безопасности с информационными процессами, имеет смысл говорить об информационно-экономической безопасности государства.

Под информационно-экономической безопасностью государства будем понимать составную часть экономической безопасности, заключающуюся в защите жизненно важных интересов всех жителей страны, российского общества в целом и государства в экономической сфере от внутренних и внешних информационных угроз.

При этом информационные угрозы экономической безопасности определим как совокупность условий, факторов и событий, которая определяет эффективность деструктивных информационных воздействий на значения соответствующих показателей экономического состояния РФ, создающее опасность экономически важным интересам личности, общества и государства.

Основными проблемами информационно-экономической безопасности являются:

– во-первых, постоянное возникновение информационных угроз из-за наличия соответствующих условий и факторов;

– во-вторых, наличие внешних деструктивных информационных воздействий на экономику страны и отдельные экономические объекты;

– в-третьих, опасность использования для нарушения экономической деятельности внутреннюю информацию экономических объектов.

К основным условиям, которые способствуют возникновению информационных угроз, можно отнести: недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика; отсутствие эффективной информационной политики государства, направленной на информационное обеспечение экономической деятельности; недостаточно развитая информационно-технологическая инфраструктура и другие.

К основным факторам (противоречиям, возникающим в ходе взаимодействия различных сил – участников экономического процесса) способствующим возникновению информационных угроз можно отнести: стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков; стремление РФ к снижению технологической зависимости России в области современных информационных технологий и попытки зарубежных государств усилить эту зависимость; деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов РФ в информационной сфере и другие.

Совокупность условий и факторов составляют необходимые предпосылки для возникновения информационной угрозы экономической безопасности. Достаточными предпосылками является наступление различных событий. Примерами таких событий являются: разработка рядом государств концепций информационных войн; закупка органами государственной власти импортных средств информатизации, телекоммуникации и связи при наличии отечественных аналогов, не уступающих по своим характеристикам зарубежным образцам; вытеснение с отечественного рынка российских производителей средств информатизации, телекоммуникации и связи и другие.

Примерами внешних деструктивных информационных воздействий (активных информационных угроз) являются информационные (информационно-психологические) операции, создание внешней враждебной информационной среды и т.п.

В качестве примеров пассивных информационных угроз можно привести: неправомерный доступ, уничтожение, модифицирование, блокирование, копирование, предоставление, распространение, а также иные неправомерные действия в отношении экономической информации.

Рассмотренные положения касаются лишь самой общей стороны проблемы информационно-экономической безопасности Российской Федерации.

Безрук Г.Г., Левкина С.В.
Россия, Санкт-Петербург, Региональный центр Главного научно-исследовательского испытательного центра робототехники МО РФ, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

ИНФОРМАЦИОННО-ЛИНГВИСТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ СИТУАЦИОННЫХ ЦЕНТРОВ ЭКОНОМИЧЕСКОГО МОНИТОРИНГА

Основой ситуационных центров экономического мониторинга (СЦЭМ) должна стать система информации, включающая в себя ряд информационных контуров, наиболее важными из которых являются: информационный контур текущего слежения за экономической обстановкой, информационный контур вскрытия новых экономических угроз и информационный контур углубленного изучения экономической обстановки. Каждый информационный контур представляет собой совокупность технических и программных средств, методов и алгоритмов обработки информации, порядок их применения для решения определенного класса информационных задач.

Предметной информационной средой СЦЭМ, в которой предполагается функционирование перечисленных информационных контуров, является часть единого экономического информационного пространства в составе:

– фрагмент информационного ядра (онтологии) - численное представление отдельных показателей (основные средства, ценные бумаги, уставный капитал, долгосрочные кредиты и т.д.); априорный словарь информационных признаков - сводное численное представление совокупности информационных (идентификационных) признаков экономического объекта (баланс, сводные справочные данные и т.п.) и информационные (идентификационные) модели различного вида, например, сводный перечень показателей функционирования изучаемого экономического объекта (совокупности объектов, процессов) - экономичность объекта, прибыльность объекта, коэффициент автономии, коэффициент маневренности и т.п.;

– внешняя (информационная) оболочка – информационные документы второго и последующих поколений. Информационные документы первого поколения – это документы, впервые описывающие те или иные информационные (идентификационные) признаки (показатели функционирования) экономического объекта (процесса). Информационные документы второго и последующих поколений – это документы, разработанные на основе информационных документов первого поколения последовательно во времени.

Выявление информационных (идентификационных) признаков экономического объекта осуществляется путем последовательного просмотра информационного документа из внешней оболочки и требует существенных временных затрат. В связи с этим, для актуализации информационного ядра (онтологии) предметной информационной среды, целесообразно использовать информационно-поисковые системы, использующие метод высокоуровневой обработки информации на основе методов математической лингвистики.

Данный метод основан на реализации идеи концептуального анализа текстовой неструктурированной информации. Первым отличием от схожих методов и технологий является то, что, исходно, область поиска представляет собой массивы неструктурированной информации, которая может быть представлена в любом электронном виде (формате) и на естественных языках любой языковой группы.

Вторым отличием данного метода является то, что в основе идеологии доработанных и адаптированных методов математической лингвистики в интересах метода высокоуровневой обработки информации, лежит процесс передачи данных с вариантами результатов анализа текста по уровням иерархии контроллеров обработки. Каждый из них отвечает за свой уровень анализа и каждый подаёт свои данные вышестоящему контроллеру для принятия им адекватного решения.

На базе специально разработанных лингвистических методов сбора информации из разнородных источников, её конвертации, интерпретации и хранения данных, поиска и извлечения пертинентной информации, визуализации результатов, данная информация преобразовывается в набор иерархических конструкций на базе семантических графов.

Именно реализованный механизм определения адекватного варианта такой конструкции сложившейся ситуации в реальном мире и является третьим существенным отличием

высокоуровневого метода обработки от схожих методов и технологий. Далее производится привязывание полученных конструкций к онтологическому описанию предметной области исходного языка поиска и трансляция конечных результатов.

Такие достоинства метода высокоуровневой обработки, как его универсальность, высокие быстродействие и пертинентность, позволяют добиваться высоких показателей эффективности мониторинга экономических угроз там, где это было раньше невозможно - во внешних информационных сетях, содержащих массивы неструктурированной информации на наиболее сложных иностранных языках.

Богатырев В.А., Богатырев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

ВЕКТОРНАЯ ОПТИМИЗАЦИЯ РЕЗЕРВИРОВАННОЙ ДРЕВОВИДНОЙ СЕТИ

Информационно-экономическая безопасность корпораций в определенной степени определяется отказоустойчивостью и надежностью телекоммуникационных систем, которые, как правило, имеют многоуровневую древовидную структуру, с резервированием коммуникационных узлов и их связей. Ограниченность ресурсов на построение сети и требования высокой надежности и производительности обусловливают потребность решения задачи оптимизации коммутационной системы. Оптимизация многоуровневой резервированной коммуникационной системы связана с необходимостью учета роста стоимости и снижения надежности коммутационных узлов при увеличении числа их портов и связей, в результате увеличения кратности резервирования выше и нижерасположенных узлов.

В качестве базовой рассмотрим трехуровневую сеть древовидной топологии. При резервировании каждого коммутационного узла формируются группы с кратностью резервирования n_0, n_1, n_2 соответственно для верхнего, среднего и нижнего уровней. Каждый узел резервированной группы соединяется со всеми узлами соответствующих выше и нижерасположенных резервированных групп. Увеличение кратности резервирования узлов приводит к техническому противоречию, так с одной стороны оно потенциально связано с увеличением надежности всей системы, а с другой - с усложнением коммутационных узлов и, как следствие, со снижением их надежности, что отрицательно сказывается на надежности всей системы. Кроме того увеличение кратности резервирование узлов приводит к возрастанию стоимости системы в результате увеличения не только числа, но и стоимости коммутационных узлов из-за увеличения числа их портов и связей.

Разрешение рассмотренного противоречия требует поиска оптимальной кратности резервирования коммутационных узлов, при которой достигается максимум надежности системы и минимум задержек передаваемых данных при ограничении средств на ее построение.

При оценке задержек пакетов в сети предположим равномерность потоков запросов, передаваемых через все ее ветви. Каждый узел сети представим одноканальной системой массового обслуживания типа M/M/1.

При оценке надежности учитывается , что вероятность невыполнения возлагаемых на сеть функций передачи пакетов определяется не только непосредственным влиянием отказов узлов на нарушение связанности сети, но и их влиянием на перегрузки узлов, приводящие к возможной потере передаваемых через сеть пакетов.

Оценим отрицательное влияние отказов узлов и их связей на среднее время пребывания запросов в сети. В каждом коммутационном узле выделим некоторое общее базовое оборудование, отказ которого приводит к полному отказу узла, и оборудование каждого порта, отказ которого приводит к потере возможности передачи только через соответствующий порт.

При оптимистической оценке среднее время пребывания запросов будем учитывать отказы только базового оборудования. В этом случае получим верхнюю оценку среднего числа функционирующих в каждой резервированной группе коммутационных узлов на верхнем среднем и нижнем уровнях

При пессимистической оценке среднего времени пребывания запросов, будем считать, что имеет место наиболее неблагоприятной случай, когда каждый работоспособный узел подключен только к одному узлу выше и нижерасположенных уровней. При таких предположениях условие работоспособности узла заключается в исправности его базового оборудования, а также оборудования портов и линий связи с единственными работоспособными узлами выше и нижерасположенных уровней.

Сложность оптимизации резервированной сети древовидной топологии вызвана тем, что с ростом кратности резервирования узлов растет стоимость системы в результате увеличения, как числа ее узлов, так и их сложности а, следовательно, стоимости и ненадежности.

Богатырев В.А., Алексанков С.М., Демидов Д.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

РЕЗЕРВИРОВАННАЯ ВЫЧИСЛИТЕЛЬНАЯ СИСТЕМА ОГРАНИЧЕННОГО ВОССТАНОВЛЕНИЯ

Высокая надежность, отказоустойчивость и безопасность систем критического применения, в частности, функционирующих в реальном времени, достигается при резервировании основных подсистем, в том числе средств хранения, обработки и передачи данных.

Обеспечение функциональной безопасности систем в значительной мере определяется информационной безопасностью, и прежде всего, связано с минимизацией риска потери данных при отказах системы, вызванных внешними или внутренними причинами, в том числе в результате злонамеренных воздействий.

Для систем критического применения, используемые в них вычислительные узлы, как правило, строятся на основе дублированных вычислительных комплексов.

Формирование работоспособной структуры после отказов требует реконфигурации, направленной на использование в вычислительном процессе сохраненных ресурсов обоих полукомплексов.

В связи с высоким вниманием в настоящее время к обеспечению безопасности систем критического применения, в том числе систем, критичным к нарушениям доступности и целостности информационных ресурсов, представляется актуальным исследование их надежности. Модели надежности таких систем должны учитывать недопустимость срывов вычислительного процесса и (или) потери важной информации, потенциально приводящие к катастрофическим последствиям, после которых восстановление вычислительной системы теряет смысл. Модели надежности указанного класса систем помимо оценки традиционных показателей надежности должны находить вероятности опасных состояний, при которых возможны срыв критичных вычислительных (управляющих) процессов и невосполнимая потеря критически важных данных.

В работе предложены марковские модели надежности восстанавливаемых ДВК, отличающиеся возможностью учета ограниченного восстановления, при невосполнимой потере накопленных данных (результатов вычислений) или при недопустимости прерываний вычислительного (управляющего) процесса во время процесса восстановления системы.

Рассмотрены ограничения восстановления комплекса, если оно не реализуемо в случаях когда:

– потеря данных не допустима, а перерывы вычислительного процесса во время восстановления допустимы;

– потеря данных и перерывы вычислительного процесса во время восстановления не допустимы;

– потеря данных и перерывы вычислительного процесса во время восстановления допустимы.

Потеря данных происходит, когда при информационной зависимости прикладных функциональных задач, решаемых вычислительной системой, отказывает память в двух полукомплексах, что приводит к невозможности выполнения задач, то есть к отказу системы, при котором ее восстановление невозможно.

Перерывы вычислительного процесса во время восстановления не допустимы, например, для управляющих систем, работающих в реальном времени, при этом будем считать, что для поддержки вычислений достаточно работоспособности хотя бы одного процессора при доступности для него памяти хотя бы в одном полукомплексе. При отказе одного процессора доступ исправного процессора к памяти другого (сопряженного) полукомплекса должен поддерживаться средствами комплексирования по прямому доступу.

Надежность ДВК охарактеризуем нестационарным коэффициентом готовности, который определяется как вероятность того, что в заданный момент времени система находится в одном из работоспособных состояний.

Предложены марковские модели дублированных вычислительных комплексов, позволяющие учесть влияние на надежность ограниченности возможностей восстановления при недопустимости потери данных и прерываний вычислительного процесса во время восстановления.

Представленные модели надежности могут быть использованы при прогнозировании надежности и выборе вариантов построения резервированных вычислительных комплексов защищенных систем критического применения, в том числе работающих в распределенных системах реального времени.

Вербицкий В.С., Утин Л.Л.
Беларуссия, Гомель, Иностранное частное производственное унитарное предприятие «АЛКОПАК»

ОПЫТ ОБЕСПЕЧЕНИЯ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ БЕЗОПАСНОСТИ ОФИСНЫХ ПОМЕЩЕНИЙ В УСЛОВИЯХ ЖЕСТКИХ ФИНАНСОВЫХ ОГРАНИЧЕНИЙ

Организация качественной системы безопасности является насущным вопросом многих руководителей серьезных компаний. Ведь это не только престиж фирмы, но и реальная необходимость в защите от непрошеных гостей, от кражи личного имущества и имущества компании, а также защита от утечки информации.

Качественная система безопасности подразумевает проведение работ сразу в нескольких направлениях, а именно:

– обеспечение пожарной безопасности;
– защита от взлома и проникновения извне;
– обеспечение информационной безопасности;
– обеспечение безопасности жизни и здоровья персонала офиса.

Несмотря на то, что каждое из указанных направлений для различных компаний имеет специфические особенности, можно отметить, что только комплексное применение организационных, технических и правовых мер позволяет создать надежную систему безопасности.

К настоящему времени актуальной становиться проблема выбора конкретных технических средств для построения такой системы. В настоящее время рынок средств защиты информации, насыщен самыми разнообразными техническими новинками, которые отличаются не только стоимостью, габаритными размерами, но и функциональными возможностями.

Наиболее распространенными средствами инженерно-технического обеспечения безопасности офисных помещений являются:

– магнитноконтактные, емкостные и инфракрасные извещатели, используемые как средства охранной сигнализации;

– дымовые, температурные и ручные пожарные извещатели различных типов предназначенных для своевременного обнаружения фактов возгорания помещения и оповещения о нем персонала компании;

– защитные жалюзи, устанавливаемые на оконных и дверных проемах с целью обеспечения дополнительной противовзломной защиты;

– видеокамеры, используемые как средство визуального контроля за территорией, прилегающей к офисному помещению и внутри него;

– тревожные кнопки и радиобрелоки, используемые для подачи установленного, как правило, скрытого сигнала сотрудникам охраны.

Очевидно, что увеличение денежных вложений в создаваемую систему защиты офисного помещения, приводит к снижению возможностей злоумышленников по достижению своей цели. При этом в определенный момент времени затраты на создание защиты становятся избыточными. Оптимизация финансовых вложений в приобретение средств защиты офисных помещений (особенно в условиях жестких финансовых ограничений) является важной задачей, которая до настоящего времени не решена. В результате у руководителей предприятий, как правило, отсутствует инструмент, позволяющий за непродолжительное время сопоставить затраты в создаваемую систему защиты и реальную ее эффективность. Кроме того, при выборе средств защиты необходимо учитывать психологические факторы, влияющие на принятие решения руководителем предприятия. Важность учета данного момента обусловлена тем, что что меры по защите имеют превентивную направленность, а последствия нарушения информационной безопасности предприятия проявляются спустя некоторое время. В случае если созданная система защиты позволяет непродолжительное время предотвратить воздействия нарушителей руководители, как правило психологически не готовы вкладывать средства в модернизацию созданной системы.

Положение усугубляется тем, что выбор конкретных средств инженерно-технической защиты сопряжен с дополнительными трудностями, связанными с тем, что как правило, фирмы-производители не указывают недостатки своих средств и преувеличивают достоинства выпускаемой продукции. А поскольку значительную часть расходов на защиту информации составляют затраты на покупку и эксплуатацию средств защиты, то методология обеспечения инженерно-технической безопасности должна обеспечивать возможность рационального выбора из имеющихся средств защиты.

В докладе, предлагается к обсуждению некоторые практические рекомендации по обеспечению инженерно-технической защиты офисных помещений, полученные авторами в ходе своей практической деятельности в сфере защиты информации.

Воробьев А.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

СТРУКТУРИЗАЦИЯ КОРПОРАТИВНОГО ЦЕНТРА ОБРАБОТКИ ДАННЫХ

Обсуждается вопрос оптимизации инфраструктуры центра обработки данных (ЦОД). Сформулирована задача оптимизации в терминах смешанного программирования, одновременно дискретного, целочисленного и непрерывного типа, поскольку такие параметры оптимизации как число серверов, кластеров, систем хранения, коммутаторов и каналов связи являются целочисленными, выбор пропускных способностей и производительности элементов ЦОД осуществляется из некоторого дискретного ряда, а различные вероятностно-временные характеристики непрерывны.

Рациональной является такая инфраструктура ЦОД, которая не только позволяет выполнять текущие задачи, но и обеспечивает дальнейшее развитие, с учетом роста объемов информационных услуг и повышения требований к показателям качества обслуживания пользователей.

Гейда А.С.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

МЕТОДИКА ОЦЕНИВАНИЯ КОНКУРЕНТОСПОСОБНОСТИ ИЗДЕЛИЙ И ВЫПУСКАЮЩИХ ИХ ПРЕДПРИЯТИЙ НА ОСНОВЕ ИССЛЕДОВАНИЯ ПОТЕНЦИАЛА СИСТЕМ

Современные предприятия функционируют в условиях конкурентных отношений. Эти отношения могут иметь вид соперничества предприятий за потребителя выпускаемой продукции, соперничества предприятий за инвестора. Нами рассматриваются потребители (покупатели) – организации, связанные с обороной и поддержанием безопасности государства. Деятельность таких покупателей протекает в сложных технических системах, оценить совершенство которых только с использованием денежного эквивалента не представляется возможным. Однако, при функционировании таких покупателей возникают конкурентные отношения, аналогичные отношениям на потребительском рынке. Кроме того, между предприятиями складываются конкурентные отношения за предпочтения инвесторов. Эти отношения в рассматриваемой предметной области целесообразно исследовать, опираясь на понятия о совершенстве использования продукции и совершенстве функционирования выпускающих ее предприятий, а не только на основе оценивания прибыльности и цены.

Так, при выпуске продукции (изделий) конкурентные отношения складываются при выборе покупателем того или иного способа обмена продукцией предприятия в сравнении со способами обмена с продукцией других предприятий. В этом случае покупатель предпочитает такой способ обмена такими изделиями, что в результате реализации обмена покупатель сможет достигать свои цели лучше, чем в результате реализации другого способа обмена. Под способом обмена понимается совокупность характеристик планируемого процесса обмена – в том числе, характеристики передаваемых денежных средства, их вид, график передачи и графики поставки. Предполагается, что покупатель – организация, которая будет эксплуатировать купленное изделие в своей системе, путем введения этого изделия в систему. Покупатель предпочитает то изделие, что позволит достигать цели, поставленные перед системой покупателя успешнее. Свойство системы, характеризующее успешность достижения поставленных перед системой целей было названо потенциалом системы. Конкурентоспособность изделия, которое покупатель рассматривает в качестве альтернативы для закупки и последующего внедрения в свою систему, по сравнению с другим изделием, целесообразно рассматривать, связав конкурентоспособность с потенциалом системы покупателя. Конкурентоспособность описывает способ обмена изделием, в описание которого входит и цена изделия. В результате обмена не только повышается потенциал системы покупателя за счет введения нового элемента (закупаемого изделия) но потенциал покупателя может и понижаться за счет перевода соответствующих денежных средств продавцу. Показатель потенциала способа обмена изделием задан, как разность между потенциалом способа обмена до и после обмена изделием и соответствующими денежными средствами, передаваемыми при обмене. Показатель конкурентоспособности изделия определен, как разность потенциала наилучшего способа обмена изделием и потенциала наилучшего способа обмена изделиями конкурентов. Он представляет собой число от минус единицы до единицы. Если эта величина положительна – изделие конкурентоспособно, если отрицательна – изделие неконкурентоспособно.

В случае, если рассматривается предприятие – производитель изделия, то у него могут складываться конкурентные отношения с другими предприятиями в результате того, что инвестор предприятия может предпочесть заданному предприятию предприятие – конкурент. В случае оборонных предприятий такое отношение осложняется государственным регулированием, системой преференций, наличием государства в составе акционеров и тем, что предпочтение может основываться на нефинансовых факторах. Поэтому предложен показатель конкурентоспособности предприятия, представляющий собой разность показателя потенциала инвестирования в заданное предприятие и предприятия – конкуренты. В свою очередь, показатель потенциала инвестирования

определен, как разность между потенциалом инвестора после инвестирования в предприятие и до инвестирования в него.

С использованием введенных понятий предложена вербальная и математическая постановки задачи исследования конкурентоспособности изделий и предприятий, как многокритериальной оптимизационной задачи.

Гейда А.С., Лысенко И.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

МЕТОД ПЛАНИРОВАНИЯ МОДЕРНИЗАЦИИ ТЕХНОЛОГИЧЕСКОЙ БАЗЫ ПРЕДПРИЯТИЙ В УСЛОВИЯХ РИСКА

При функционировании современных предприятий, как свидетельствует практика, часто возникает необходимость модернизации состава производственной базы предприятия. Такая модернизация реализуется в виде мероприятий модернизации, часть из которых может требовать остановки штатного функционирования тех или иных элементов производственной базы. Модернизация должна позволить выполнять новые технологические процессы, получать лучшие результаты функционирования в будущем.

В то же время, может оказаться, что такая модернизация должна осуществляться в условиях, когда предприятие продолжает выполнять производственные планы, в том числе – на модернизируемом оборудовании. Выполняемые производственные планы могут быть направлены на достижение целей, срыв выполнения которых, в том числе из-за модернизации, нежелателен. Возможность таких нежелательных результатов модернизации необходимо учитывать при ее планировании.

Например, модернизация может приводить не только к благоприятным, желаемым результатам, таким, как новые возможности информационной системы, новые производственные процессы, новый ассортимент продукции, но и к задержкам реализуемого при модернизации производственного процесса, перерасходу выделенных средств, потере части заказчиков в результате неблагоприятных событий при реализации модернизации. Для учета этой особенности предлагается реализовывать планирование модернизации с учетом возможностей наступления неблагоприятных событий, то есть — в условиях риска.

Возможности неблагоприятных событий возникают при реализации мероприятий модернизации.

Обоснованы показатели эффективности модернизации в условиях риска. Предложено оценивать план модернизации в условиях риска с использованием пары показателей: показателя потенциала производственной системы, достигнутого в результате модернизации; показателя риска при модернизации.

Потенциал производственной системы, достигнутый в результате модернизации определен, как разность потенциалов системы после модернизации и до нее. Потенциал системы определен, как свойство системы, позволяющее использовать её для достижения возможных целей. При этом предполагается, что цели могут меняться и поэтому должны быть предусмотрены процессы перехода к достижению той или иной новой цели, названные процессами конверсии системы.

С использованием введенных понятий предложена вербальная и математическая постановки задачи планирования модернизации в условиях риска, как многокритериальной оптимизационной задачи распределения ограниченных ресурсов. Для решения поставленной оптимизационной задачи разработан комплекс моделей, позволяющий получить рекуррентные соотношения для расчета значений показателей потенциала, достигнутого в результате модернизации и показателей риска при модернизации, а затем – пересчитывать эти значения при изменении плана модернизации.

Предложена модификация метода случайного поиска, использующий особенности разработанных моделей и решаемой задачи. Метод позволяет сократить объем вычислений в несколько раз, в зависимости от особенностей исходных данных.

Григорова А.В., Емелин В.И.
Россия, Санкт-Петербург, ОАО «Научно-исследовательский институт «Вектор»

ЗАЩИТА ИНВЕСТИЦИОННЫХ ПРОЕКТОВ В СФЕРЕ НЕДВИЖИМОСТИ ОТ ДЕЙСТВИЙ КОНКУРЕНТНОЙ РАЗВЕДКИ

Инвестиционные проекты в сфере недвижимости основаны на использовании технологий с высокой долей вклада интеллектуального труда, затраченного на поиск и реализацию наиболее рациональной стратегии развития недвижимого имущества. Все это приводит к тому, что в современных условиях ведения бизнеса инвесторы начинают активно использовать не три, а четыре основных инвестиционных ресурса: труд, капитал, технологии, а также релевантную информацию (постоянно обновляемые знания и различного рода сведения). В связи с этим утечка, утрата или модификация информации в результате непреднамеренных ошибочных, либо несанкционированных действий приводит к значительному экономическому ущербу.

Главный достигаемый эффект активного использования информационных технологий заключается в снижении трансакционных издержек при добывании разнообразной информации, а также знаний, которые необходимы для снижения риска инвестиций и получения максимальной прибыли в сфере недвижимости. К защищаемой информации относится значительный перечень разнообразных сведений: 1) рыночная информация; 2) информация о конкурентах; 3) макроэкономическая и геополитическая информация; 4) информация о поставщиках (издержки, надежность, качество и время доставки); 5) внешняя финансовая информация (валютные курсы, динамика курсов акций, движение на рынке капитала и т.д.); 6) информация из государственных органов и органов управления: законы, постановления, сообщения налоговых органов и пр.

Без владения такой информацией невозможно быть конкурентоспособным, при этом на ее добывание затрачиваются значительные материальные и временные ресурсы. В связи с этим возникает два тесно взаимосвязанных обстоятельства:

1. Предприниматель вынужден выступать в качестве защитника своей зачастую уникальной информации, накапливаемой в течение длительного времени;

2. Предприниматель вынужден в условиях конкуренции использовать и чужие данные, при этом он должен критически относиться к рекламной информации, которая не всегда является достоверной и может быть дезинформацией.

Соответственно стремительно развивается новое направление разведывательной деятельности — конкурентная разведка (competitive intelligence), которая в настоящее время представляет собой бурно развивающуюся дисциплину, возникшую на стыке экономики, юриспруденции и специальных дисциплин. Конкурентная разведка использует в своей практике легальные методы сбора и обработки информации, получая из открытых источников 80—90% оперативно-ценной информации. Отсюда возникает проблема защиты не только массивов накопленных данных, но и, прежде всего, совокупной информации, которая приобретает значительную ценность в результате сбора разрозненных данных в единое целое. При этом в сфере недвижимости защите подлежат не только уникальные физические и экономические характеристики, но также связанные с каждым объектом права и юридические ограничения на их использование. Таким образом, при построении системы защиты от утечки, утраты и модификации сведений в инвестиционных проектах следует различать: 1) массивы данных, содержащих результаты наблюдений и измерений; 2) результаты обработки данных, представленные в установленной форме; 3) знания, представляющие собой систематизированные факты, полученные в результате сопоставления информации с выдвинутыми гипотезами. Указанная классификация сведений об инвестиционных проектах позволяет организовать защиту информационных ресурсов в соответствии с их ценностью. При определении ценности этих ресурсов необходимо руководствоваться экономическими (стоимость) и информационными критериями (полезность, своевременность достоверность поступивших сведений).

В качестве обобщающего итога подчеркнем, что в современных условиях новым приоритетом в государственной политике обеспечения информационной безопасности является защита сведений экономического характера. Основными направлениями ее развития следует считать следующий комплекс мероприятий:

1) в правовой сфере – уточнение правовых аспектов информационной безопасности по фактам утечки, утраты и модификации информации об объектах недвижимости, как критически важных объектов;

2) в технической сфере – создание аппаратно-программных средств, позволяющих определять источники информационных воздействий и защиту от них;

3) в экономической области – разработка методического аппарата, позволяющего проводить оценку экономического ущерба, причиненного в случае утечки, утраты и модификации данных об объектах недвижимого имущества.

Евдокимов Ю.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

ПРОЕКТИРОВАНИЕ ОСНАСТКИ ДЛЯ УСТРОЙСТВ ЛИНИИ СБОРКИ МИКРООБЪЕКТИВОВ

Автоматизированная линия сборки микрообъективов представляет собой научно-исследовательский полигон для изучения и формирования различных знаний в этой области, таких как, например, технология сборки.

Автоматизированная линия сборки микрообъективов по проекту состоит из 8 станций, отвечающих за разные этапы сборки посредством применения встроенной вычислительной техники и специального программного обеспечения. Работа на станциях осуществляется в соответствии с разработанными алгоритмами в соответствии с технологическим процессом. Связь между станциями осуществляется при помощи транспортной линии, по которой передвигаются шаттлы с тарой,

содержащей собираемые изделия. Также с транспортной линией связан склад, где хранятся детали, откуда они поступают на сборку и куда в итоге поступают собранные узлы и изделия.

Одним из главных требований к работе станции является унификация. Это относится как к аппаратному обеспечению (роботы, конструктивные элементы, оснастка), так и к программному (системы программирования контроллеров, алгоритмы работы). Состав и структура каждой станции разрабатываются с учетом применения однотипных устройств для выполнения общих для всех станций работ (робот-манипулятор, робот-перекладчик, лифтовый склад). Такой подход позволяет провести и программную унификацию, а в дальнейшем и применить средства модульного подхода для формирования алгоритмов работы систем и написания управляющих программ. Это в свою очередь ускорит процесс формирования программ и внесет большой вклад в обеспечение синхронизации.

Помимо этого, одними из важнейших свойств, которым должна обладать автоматизированная линия, являются надежность и безопасность работы устройств. При этом следует уделить особое внимание разработке оснастки для устройств, применяемых на линии. Оснастка, к которой относятся такие элементы, как губки схватов, ручки тары, крепления приспособлений, должна обеспечивать возможность максимально полезного использования возможностей устройств. Автоматизированная система во время работы принятие некоторых решений предоставляет оператору, который помимо этого должен контролировать работу всей системы. Поскольку работа на станции подразумевает присутствие как минимум одного человека, а сам процесс носит иследовательский характер, различного рода ошибки могут привести не только к повреждению дорогостоящего оборудования, но и нанести травму персоналу. В связи с этим при проектировании и разработке оснастки следует учесть эти факторы и либо исключить их, либо сформировать таким образом, чтобы ущерб получало не оборудование или человек, а оснастка. Также форма и требования к оснастке могут исключить необходимость использования того или иного дополнительного оборудования, взяв на себя его функции.

Оснастка проектируется в современных CAD системах (Catia, Solid Works и др.), после чего выполняется ее прототипирование на 3D принтере. На данный момент оснастка уже имеет несколько версий. Они меняются в соответствии с результатами проведенных испытаний. Для ускорения и удешевления процесса проектирования оснастки решено применять CAE системы, такие как NASTRAN и ANSYS.

Колбанёв М.О., Татарникова Т.М., Воробьев А.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

ДВУХУРОВНЕВАЯ МОДЕЛЬ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

При развитии идей кибернетики информационное взаимодействие, сопровождающее любую деятельность человека, рассматривается на двух метауровнях. Идеальный метауровень является продуктом мышления людей и обеспечивает на передающей стороне порождение, а на приемной стороне постижение смыслов. Материальный метауровень поддерживает идеальный и обеспечивает обмен данными, имеющими физическую форму представления. Такой подход позволяет следующее.

1. Разделить информационные процессы на две группы. На идеальном метауровне они связаны с особенностями человеческого мышления, зависят от используемых языков информационного взаимодействия и служат измерителем степени интеллектуальности технологий, поскольку чем выше интеллект взаимодействующих сторон, тем более мягкий язык используется при их взаимодействии. Информационные процессы на материальном метауровне представляют собой последовательность операций над данными, как материальными объектами, и позволяют оценить объемы материальных ресурсов, потребляемых технологией.

2. Обобщить схему связи К.Шеннона, которая «предназначена для точного или приближенного переноса данных между двумя точками пространства» и, таким образом, расширить границы математической теории связи, в том числе, и в части кодирования, защиты информации и борьбы с шумами, поскольку позволяет учесть физические законы взаимодействия, осуществляемого с данными, реальные пространственные координаты расположения пользователей и данных, реальный масштаб времени при перемещении данных, реальные энергетические затраты, которые требуются для преобразования данных и др.

3. Формировать показатели качества информационного сервиса, содержательная сторона которых формулируется на идеальном метауровне, а количественная оценка измеряется на материальном метауровне, например, в единицах пространства, времени, энергии или их соотношения.

4. Построить три типа взаимосвязанных моделей информационного взаимодействия. Концептуальные модели объединяют основные информационные и материальные компоненты и сопоставляют их этапам и фазам реализации процесса информационного взаимодействия. Метрические модели количественно описывают процессы преобразования информационных объектов в системе с координатами пространства, времени и энергии и создают основу для оценки

материальных ресурсов процессов информационного взаимодействия. Эталонные модели представляют собой абстрактное, не связанное с реализацией соглашение о принципах информационного взаимодействия между объектами в электронной цифровой среде.

5. Разделить ограничения на выбор информационных технологий на две группы. Субъективные ограничения относятся к идеальному метауровню. Это правила, действующие в разных предметных областях. Они формулируются и учитываются при автоматизации информационной деятельности и существуют как смысловые понятия, которые могут быть тем или иным образом интерпретированы участниками информационного взаимодействия. Объективные ограничения – это законы природы, в соответствии с которыми мозг человека порождает и постигает смыслы, а данные перемещаются между людьми.

6. Выделить три базовых способа организации процесса информационного взаимодействия. Процесс сохранения данных – это доведение до получателей данных после их содержания в памяти в сохранности, целостности и безопасности в течение требуемого времени. Процесс распространения данных – это своевременное доведение данных по каналам связи до получателей, находящихся в удаленных точках пространства. Процесс обработки данных – это доведение до получателей новых по форме представления данных, полученных из исходных путем выполнения обработчиками данных алгоритмов замены, добавления, исключения знаков информационной последовательности или изменения порядка следования знаков.

7. Предложить новые способы количественной оценки информации, передаваемой между взаимодействующими сторонами, выделяя то или иное свойство информационного взаимодействия. Для этого можно, например, измерять:

– изменения, произошедшие на взаимодействующих сторонах в результате обмена информацией, поскольку это позволит судить о значении переданных смыслов;

– пространственные, временные и энергетические параметры процесса информационного взаимодействия, связанные с материальной природой данных;

– количество знаков и статистические свойства языка взаимодействия, использованного для подготовки сообщения, поскольку это позволит оценить множество состояний, занимаемых сообщениями.

Проведенный анализ позволяет утверждать, что дальнейшее развитие информационных технологий в направлении их интеллектуализации и ресурсной экономичности должно основываться на моделях информационного взаимодействия, отличающихся от кибернетических моделей.

Коршунов И.Л.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

РОЛЬ И МЕСТО ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В НАПРАВЛЕНИИ ПОДГОТОВКИ 080101.65 «ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ»

В соответствии с Федеральным государственным образовательным стандартом (ФГОС) специалист в области экономической безопасности готовится к информационно-аналитической деятельности. Он должен уметь решать целый ряд задач, связанных с поиском и оценкой истинности информации, имеющей значение для обеспечения экономической безопасности; с моделированием экономических процессов в целях анализа и прогнозирования угроз экономической безопасности; с информационно-аналитическим обеспечением предупреждения и выявления экономических рисков и угроз экономической безопасности.

Среди многочисленных компетенций (общекультурных и профессиональных), которыми должен обладать специалист, необходимо отметить следующие: способность работать с различными источниками информации, информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации, применять в профессиональной деятельности автоматизированные информационные системы, используемые в экономике, автоматизированные рабочие места, проводить информационно-поисковую работу с последующим использованием данных при решении профессиональных задач; способность выбирать инструментальные средства для обработки финансовой, бухгалтерской и иной экономической информации и обосновывать свой выбор; способность анализировать и интерпретировать финансовую, бухгалтерскую и иную информацию, содержащуюся в учетно-отчетной документации, использовать полученные сведения для принятия решений по предупреждению, локализации и нейтрализации угроз экономической безопасности.

Анализ приведенных требований ФГОС позволяет констатировать, что специалист в области экономической безопасности должен хорошо знать теоретические основы информационных технологий, уметь применять их в профессиональной деятельности и владеть методами и средствами информационной безопасности. Для достижения этих целей в базовой части математического и естественнонаучного цикла примерной основной образовательной программы имеется дисциплина «Информационные системы в экономике». К сожалению, она не позволит подготовить специалиста, обладающего приведенными выше компетенциями.

Предлагается включить в вариативную часть математического и естественнонаучного цикла дисциплину «Информационная безопасность». В этом случае в рамках дисциплины «Информационные системы в экономике» будут рассматриваться базовые информационные процессы, базовые информационные технологии и информационные системы, реализующие информационные технологии в экономике. Вторая дисциплина «Информационная безопасность» посвящена изучению информационных технологий защиты информации, применяемых в профессиональной сфере специалистов по экономической безопасности.

Далее рассматривается структура и наполнение учебных программ этих дисциплин. Темы и их содержание тесно увязаны с компетенциями, которыми должен обладать специалист по экономической безопасности.

Кравченко К.Ю., Утин Л.Л.
Беларуссия, Гомель, Иностранное частное производственное унитарное предприятие «АЛКОПАК»

ОСОБЕННОСТИ ПРОВЕДЕНИЯ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ИНОСТРАННЫХ ПРЕДПРИЯТИЯХ

В современных условиях, часто в ходе борьбы за рынок сбыта, инструментами выступают недобросовестная конкуренция и нарушения в сфере интеллектуальной собственности. Основными нарушениями являются недобросовестная регистрация объектов, использование чужих обозначений, этикеток, упаковок, торговых марок, промышленных образцов, коммерческих наименований и т.д.

Грамотная и всесторонняя защита прав интеллектуальной собственности является необходимой для выживания предприятия и усиления его позиций на рынке. Следует отметить, что руководство нашего предприятия четко осознает данную проблемму и принимает организационные, правовые и технические меры по обеспечению защиты своих информационных ресурсов. Созданная система защиты информации позволяет своевременно выявлять каналы утечки конфиденциальной информации и принимать меры по их нейтрализации. Например, в ходе проводимой работы были выявлены факты несанкционированного патентования некоторых образцов изделий. По результатам расследования были аннулированы патенты на промышленный образец и полезную модель, позволявший ввоз недобросовестным конкурентам контрафактного колпачка на территорию Украины, а также патент компании Guala Closures (Италия). Это лишь не многие примеры грамотно спланированной и реализованной на практике политики безопасности предприятия «Алкопак».

Вместе с тем, высокая динамика развития сетей связи и их интеграция с глобальными сетями в том числе Интернетом, низкая стоимость средств вычислительной техники, уменьшение их габаритных размеров приводит к увеличению возможностей нарушителей для деструктивного воздействия на информационные ресурсы компании и нанесению материального ущерба. Положение усугубляется тем, что количество сотрудников компании и ее филиалов насчитывает более тысячи человек, каждый из которых может быть потенциальным нарушителем политики безопасности предприятия.

Положение усугубляется и тем, что редкие случаи нарушения безопасности информации, выявленные на предприятии за последние десять лет, приводят к постепенному снижению приоритетности вопросов информационной безопасности. Отсутствие объективных оценок уровня безопасности со стоны независимых экспертов приводит к тому, что руководству компании становиться все сложнее доказывать целесообразность постоянного совершенствования созданной системы. При этом крайне сложно найти поддержку у руководства для принятия решения, которое напрямую не увеличивает эффективность работы предприятия или не приносит существенного эффекта или прибыли.

В этих условиях построенная в компании система управления информационной безопасностью должна периодически подвергаться независимому аудиту, который в соответсвии с требованиями международных стандартов является одним из обязательных этапов жизненного цикла данной системы. Однако рекомендации по проведению стандартной процедуры аудита имеют несколько отрицательных моментов.

Во-первых, в аудиторских отчетах, как правило, не содержится детальных рекомендаций по внедрению конкретных программных, аппаратных и программно-аппаратных средств защиты информации, которые могут лечь в основу технического проекта СОИБ.

Во-вторых, оценка уровня информационной безопасности ИС предприятия, сопоставление его с объективно необходимым уровнем, а в случае несоответствия подбор оптимального комплекса защиты представляет собой весьма непростую и дорогостоящую задачу. Как следствие, для внутреннего аудита ИБ назначаются внештатные аудиторы, которые, как правило, имеют недостаточную квалификацию для качественного проведения аудита. В результате, для проведения аудита должны привлекаться сторонние организации, представляющие консалтинговые услуги в области ИБ. Однако, из-за сохраняющейся потенциальной опасности использования внешними аудиторами выявленных уязвимостей СОИБ в своих корыстных целях, сторонние организации, как правило, не привлекаются.

Возможные направления разрешение данных противоречия представляются для обсуждения.

Левкин И.М., Сорокина Е.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

РЕЙДЕРСКИЙ ЗАХВАТ КАК ОСОБАЯ ФОРМА ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКОЙ УГРОЗЫ

Обеспечение экономической безопасности, как государства, учреждений, обеспечивающих приоритетные направления его развития, так и бизнеса в целом, является важнейшей задачей государственной политики. В основе решения этой проблемы лежит своевременное вскрытие экономических угроз. Одной из наиболее опасных угроз такого рода является недружественное поглощение одного хозяйствующего субъекта другим (рейдерский захват). Угроза рейдерского захвата получает все большее распространение.

В связи с тем, что рейдерский захват представляет собой развивающуюся во времени совокупность мероприятий и основывается на сборе информации об объекте захвата, возникает возможность говорить о рейдерском захвате как об особой форме информационно-экономической угрозы. В свою очередь, при изучении такой информационно-экономической угрозы становится возможным: во-первых, вскрыть факты недружественных действий путем обнаружения характерных информационных признаков (угроз); во-вторых, своевременно перестроить систему информационной защиты хозяйствующего субъекта. Данные обстоятельства с учетом тенденций развития рейдерства в современных условиях обусловливают актуальность выбранной темы.

Следует отметить, что, несмотря на наличие значительного числа публикаций, имеющих несомненное теоретическое и практическое значение, целый ряд направлений в области защиты информации хозяйствующих субъектов остался недостаточно разработанным. К их числу можно отнести: отсутствие методик информационного описания ряда внешних угроз, учитывающих динамику развития недружественных действий непосредственно, как процесса; отсутствие научно обоснованных подходов к отражению массированных информационных угроз различной природы; нерациональное использование сил и средств защиты предприятия в условиях высокой динамики возникновения информационных угроз и другие.

Под «рейдерским захватом» предлагается понимать не конечный результат этого явления, как принято в современной научной литературе, а сложный организационно-экономический процесс: комплекс согласованных и взаимосвязанных по целям, задачам, месту и времени мероприятий, проводимых по единому замыслу и плану различными (в том числе криминальными) структурами, с целью поглощения хозяйствующего субъекта против воли его собственников, имеющих преимущественное положение в данном хозяйствующем субъекте, и/или его руководителя. Как процесс рейдерский захват может быть представлен в виде комплексной информационно-признаковой модели.

Сущность комплексной информационно-признаковой модели рейдерского захвата хозяйствующего субъекта заключается: во-первых, в представлении этой угрозы в виде фрейм-сценария, отражающего последовательность мероприятий при различных вариантах развития событий при белом, сером и черном рейдерстве; во-вторых, в представлении каждого мероприятия в виде иерархической структуры информационных признаков.

Эта модель позволяет: определить проведение рейдерских мероприятий путем мониторинга информационного пространства, обнаружения и идентификации информационных признаков, характерных для этого мероприятия; определить внутреннюю информацию хозяйствующего субъекта, необходимую для реализации этого мероприятия; составить перечень возможных каналов утечки внутренней информации на момент проведения рейдерского мероприятия; спрогнозировать перспективные информационные угрозы при продолжении рейдерских действий.

Левкина С.В.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

ОСОБЕННОСТИ КОМПЛЕКСНОЙ ОЦЕНКИ ТЕКУЩЕГО СОСТОЯНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Адекватное оценивание состояния экономической безопасности является одной из важных проблем экономической теории. В существующих научных работах посвященных решению этой проблемы основной упор делается на периодическое сопоставление текущих значений неких экономических показателей (индикаторов) с плановыми. При этом периодичность оценки зависит от сроков подготовки плановых экономических документов, которые являются неизменными и могут составлять месяц, квартал, полугодие и т.д. Вместе с тем, в промежутках между плановыми оценками могут происходить события, существенно изменяющие уровень экономической безопасности государства. Примерами таких событий являются техногенные и природные катастрофы и катаклизмы (катастрофы на Чернобыльской АЭС (1986 г.), Саяно-Шушенской ГЭС (2009 г.), наводнение на Дальнем Востоке (2013 г.) и т.п.), дискриминирующие экономические решения развитых зарубежных государств, их коалиций, международных финансово-экономических организаций, террористическая деятельность

и т.п. Существующие методики оценивания состояния экономической безопасности государства такие события учитывают с запозданием, которое в отдельных случаях может быть существенным.

В интересах устранения этого недостатка предлагается для расчета интегрального индекса экономической безопасности РФ в качестве базового элемента использовать экономическую компоненту индекса международной безопасности *iSi* и внести в нее следующие изменения:

– уточнить перечень региональных и локальных опасностей и определять вероятность их наступления через текущие и плановые значения наиболее представительных индикаторов;

– определить следующие требования к используемым индикаторам: они должны быть связанными с основными внешними и внутренними угрозами экономической безопасности, охватывать все ее стороны; быть рациональными, то есть не иметь излишних данных и иметь высокий коэффициент использования имеющейся информации; иметь однозначное численное текущее и пороговое значения; обладать доступностью, то есть иметь возможность своевременного получения информации по их значениям; обладать преемственностью, то есть быть способными к использованию на длительном временном интервале; обладать сопоставимостью, позволяющей сравнивать одни и те же показатели в различные моменты времени;

– сформировать перечень возможных событий, случайное наступление которых может оказать существенное влияние на состояние экономической безопасности;

– вероятность наступления случайной угрозы определять через вскрытие информационных признаков возможных событий на основе предложенных информационно-признаковых моделей;

– осуществлять корректировку базового значения индекса экономической безопасности каждый раз при превышении вероятности наступления случайной угрозы выше заданной.

Реализация предложенной методики предполагает создание ситуационных центров экономического мониторинга, которые решают следующие основные задачи: задачи контроля текущего состояния экономической безопасности; задачи вскрытия новых экономических угроз; задачи углубленного описания экономической обстановки.

Основной особенностью решения задач контроля текущего состояния экономической безопасности является выявление информационных (идентификационных) признаков известных внешних и внутренних экономических угроз и оперативная оценка уровня экономической безопасности на момент получения соответствующего признака. Для решения этой задачи используется предложенный перечень дескрипторов. При этом мониторинг должен осуществляется по ограниченному перечню наиболее информативных источников в масштабе времени близком к реальному.

Основной особенностью решения задач вскрытия новых экономических угроз является необходимость более широкого анализа информационных источников с целью: во-первых, выявления информационных (идентификационных) признаков, характеризующих новые экономические процессы (явления) способные нанести экономический ущерб России; во-вторых, оперативной оценки степени опасности, которую несут новые экономические угрозы.

Основной особенностью решения задач углубленного описания экономической обстановки является дальнейшая информационная разработка известных экономических угроз и создание информационных портретов вновь выявленных экономических опасностей. Результаты решения этой группы задач лежат в основе информационного обеспечения всей системы экономического мониторинга.

Москвин Д.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ СОВРЕМЕННЫХ ПОТРЕБИТЕЛЬСКИХ УСТРОЙСТВ

В настоящее время все большее количество различных потребительских устройств получает доступ к сети Интернет. К таким устройствам относятся все современные коммуникационные и вычислительные мобильные устройства (смартфоны и КПК с поддержкой подключения по WiFi), цифровые банки данных и фотоаппараты с беспроводным подключением, игровые приставки, домашнее развлекательное оборудование (современные телевизоры с интерфейсами LAN и WLAN, IP-радиоприемники, мультимедийные сетевые накопители с проводным и беспроводным доступом). Сетевой интерфейс используется такими устройствами для подключения друг к другу (например, телевизор позволяет проигрывать файлы, хранящиеся на удаленном компьютере), скачивания программных обновлений (например, новой прошивки), получения доступа к удаленным сервисам (например, отображение на телевизоре сводки погоды, скачанной из Интернет).

Многие современные потребительские устройства также имеют функции определения собственного геоположения по GPS-приемнику, фото/видеосъемки, записи звука со встроенного микрофона, а также определение присутствия людей, освещенности, запахов, положения в

пространстве, температуры, влажности, наличия различных объектов и д.р., измеряемые с помощью специализированных датчиков.

При этом, как правило, функции безопасности реализованы только в рамках протоколов коммуникации (например, настройки безопасности WiFi). Однако известно, что для реализации достаточной безопасности в беспроводных сетях необходимо использовать ресурсозатратное шифрование, тонкое управление настройками требует высокого уровня знаний в администрировании, что часто невозможно в потребительской технике. В самой потребительской электронике на уровне прошивки или встроенной операционной системы нет реализации собственных функций безопасности. В этой связи возникает новый класс программных угроз, объектом которых является как техника, контент, так и потребитель.

Реализация таких угроз и внедрение вредоносного программного обеспечения (ВПО) предоставит нарушителям следующие возможности по использованию потребительских устройств для нарушения информационной безопасности:

1. Использование потребительских устройств для проникновения на персональные компьютеры и мобильные телефоны. Большинство «умных» потребительских устройств имеют доступ к локальной сети дома или офиса. А поскольку обычно персональные компьютеры, ноутбуки и мобильные телефоны воспринимают домашнюю сеть как доверенную, то они не имеют защиты от угроз со стороны таких потребительских устройств. Таким образом, например, ВПО, установленное в телевизор с операционной системой (ОС) Android, может беспрепятственно самораспространиться на другие устройства и компьютеры домашней сети.

2. Сбор данных средствами потребительских устройств. Информация о пользователе может быть получена средствами самого потребительского устройства. К такой информации относится его местонахождение, видеонаблюдение, запись разговоров. Например, в фотоаппарат Samsung Galaxy Camera встроен GPS приемник, благодаря которому внедренное ВПО может всегда точно определить географическое положение устройства и его пользователя. Другие устройства позволяют собрать более полную информацию о пользователе, включая режим дня, вкусовые предпочтения и т.п.

3. Использование потребительских устройств в качестве proxy или файловых серверов. Установка proxy-сервера, например, на холодильник Samsung T9000 может оказаться для нарушителя существенно проще, чем на компьютер, а эффект анонимности при этом только возрастает. Другой вариант — использование потребительского устройства для хранения собранных на компьютере или мобильном телефоне данных, т.к. ни средства защиты, ни пользователь их там никогда не обнаружат. При этом тот же холодильник Samsung T9000 имеет собственный облачный сервис для хранения данных.

Информационной безопасности потребительских устройств уделяется очень мало внимания, т.к. производители не воспринимают такие устройства как потенциальные объекты компьютерных атак. Однако де-факто они становятся компьютерами со специфическими функциями. Поэтому современные «умные» потребительские устройства открывают множество новых угроз информационной безопасности. Их реализация позволит нарушителям перенаправлять потоки информации, подменять контент, приводить технику в нерабочее состояние, следить за пользователями и т.д. Существующие средства защиты не способны работать на таких потребительских устройствах, т.к. практически все они в той или иной степени рассчитаны на интерактивное взаимодействие с пользователем, что в данном случае невозможно. Поэтому создание технологий и средств защиты для потребительских устройств в настоящее время является одной из наиболее актуальных задач обеспечения информационной безопасности.

Мошак Н.Н.
Россия, Санкт-Петербург, Главное управление Банка России по Ленинградской области

СИСТЕМЫ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ТЕРРИТОРИАЛЬНЫХ УЧРЕЖДЕНИЯХ БАНКА РОССИИ

Работа Территориального учреждения Банка России в современных условиях характеризуется многообразием функциональных и управленческих задач, требующих постоянного совершенствования системы внутреннего контроля. При этом решение практически всех задач осуществляется с использованием распределенных автоматизированных банковских систем. В этих условиях эффективный внутренний контроль за состоянием информационной безопасности) возможен только при своевременной и адекватной оценке значительных объемов информации.

Анализ существующей практики показывает, что на уровне Территориального учреждения Банка России в сутки в рамках технологического мониторинга регистрируются миллионы различного рода событий, 99,9% из которых являются информацией о штатной работе системных и прикладных процессов, проведении регламентных работ. При этом события информационной безопасности к общему количеству первичных событий составляют лишь сотые доли процента и в основном связаны с регламентными модификациями программного обеспечения.

Главной проблемой процесса мониторинга и анализа событий информационной безопасности при ручной обработке – это невозможность обнаружения деструктивных воздействий на автоматизированные банковские системы и их элементы в реальном времени при визуальном контроле записей в их штатных журналах аудита. Таким образом, выявление реальной угрозы, например, вирусного заражения, комбинированной атаки, с целью несанкционированного доступа к информационным активам, и оперативное принятие управленческого решения возможно только с использованием автоматизированных технологий контроля и, прежде всего, автоматизированного мониторинга информационной безопасности.

В докладе прослеживается эволюция создания и внедрение автоматизированных систем мониторинга информационной безопасности в Территориальных учреждениях Банка России, рассматривается их архитектура и особенности функциональной структуры. На примере единой системы мониторинга информационной безопасности Главного управления Банка России по Ленинградской области описывается процесс формирования коррелированного события информационной безопасности и его обработки. Показан эффект применения системы на примерах формирования различных коррелированных событий информационной безопасности.

Пичугин Ю.А., Кондрашков А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербургский государственный экономический университет

СТАТИСТИЧЕСКИЕ ОЦЕНКИ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ И РИСКА НА ОСНОВЕ АЛЬТМАНОВСКОГО ПОДХОДА

Предложенный Э. Альтманом подход к оценке экономической безопасности предприятий состоит в том, что для пяти основных экономических показателей x1,x2,,…,x5 строится линейная форма $\varphi(X)=CтX$, $Xт=(x1,x2,,…,x5)$, коэффициенты которой $Cт=(c1,c2,…,c5)$ определяются по статистическим данным предприятий за достаточно долгий период. Два значения этой формы φC и φR ($\varphi C>\varphi R$) задают разбиение области G допустимых значений X на три подобласти: $GC=\{X:X\in G,\varphi(X)>\varphi C\}$ – безопасности, $GR=\{X:X\in G,\varphi(X)<\varphi R\}$ – несостоятельности (риска) и GN – неопределенности. Предполагается, что вектор X подчиняется многомерному нормальному распределению $X\sim N(\Theta,\Sigma)$, параметры оцениваются по данным бухгалтерской отчетности. Статистическая проверка безопасности (степени риска) сводится к проверке гипотезы H0: $\Theta\in GR$. Эта задача, в свою очередь, приводит к задаче нахождения точки касания XR гиперплоскости $\varphi(X)=\varphi R$ и эллипсоида риска $WR=\{X:f(X)=fR\}$, где f(X) функция плотности распределения $N(\Theta,\Sigma)$, $fR=f(XR)$. Гипотеза H0 отвергается на уровне значимости α, если вероятностная мера области ограниченной эллипсоидом WR больше выбранного уровня доверия $(1-\alpha)$. Приводится решение задачи нахождения XR и вычисления вероятностной меры WR, приводятся также и вероятностные оценки устойчивой работы предприятия. Предложенная методика может рассматриваться в качестве основы для разработки программного обеспечения оценки экономической безопасности предприятия.

Пойманова Е.Д.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ СОХРАНЕНИЯ ИНФОРМАЦИИ

В настоящее время для любой информационной системы остро стоит проблема сохранения данных. Особенно эта проблема актуальна для данных длительного (до 70 лет) хранения (например, архивы). Речь идет о надежности хранения информации и защиты ее от непреднамеренных угроз. Как правило, непреднамеренные угрозы связаны с человеческим фактором и низкой надежностью программного и аппаратного обеспечения. Примерами информации, нуждающейся в безопасности, могут служить медицинские карточки и медицинские изображения, номера пластиковых карт и социального страхования, сведения, относящиеся к торговле через Интернет и другим транзакциям, системы видеонаблюдения, конфиденциальные юридические документы и корпоративная интеллектуальная собственность.

Поскольку современные информационные системы в основном являются системами с распределенным хранением данных, то возникают проблемы, связанные с ошибками при синхронизации данных, передачей данных по каналам связи, а также связанные с физическим доступом к носителям.

Решением проблем в этой области является организация системы хранения данных (СХД), обеспечивающей сохранение информации на длительное время, или «системы длительного хранения данных». В частности, этому способствуют такие возможности СХД как:

– способность СХД к масштабированию и наращиванию объемов памяти для сохранения данных. Это особенно важно в условиях информационного общества, когда рост информационных ресурсов требует все больших объемов долговременной памяти;

– наличие у СХД развитых интерфейсов с внешним окружением и обеспечение, в том числе и дистанционного взаимодействия через сети связи со многими пользователями в реальном масштабе времени;

– централизация информационных ресурсов в СХД, что позволяет повысить эффективность управления данными и увеличить не только надежность хранения, но и скорость записи и считывания.

Наиболее популярной технологией хранения данных на сегодняшний день является RAID (redundantarrayofinexpensive/independentdisks). Одной из задач RAID массива является повышение надежности хранения информации с помощью специальным образом организованной работы массива из жестких дисков. Однако данные технологии по большей части ориентированы на системы, требующие оперативного доступа к данным. Для информации длительного хранения оперативный доступ не является приоритетной задачей. Наиболее актуальной задачей является именно сохранение.

При организации длительного хранения данных наиболее популярными в настоящее время являются такие виды накопителей как оптические диски, «каменные» диски, стеклянные диски, ленточные накопители. Для реализации доступа к СХД длительного хранения используются роботизированные библиотеки.

Известно, что темпы роста объемов цифровой информации будут расти, а бюджеты на информационные технологии сокращаться, что приведет к росту разрыва между объемами создаваемой информации и количеством приобретенных и установленных ресурсов для управления ею. Данное обстоятельство приводит к возникновению спроса на инструменты и технологии, позволяющие управлять большими объемами информации с меньшими затратами ресурсов.Поэтому помимо выбора надежных накопителей для обеспечения сохранности данных должны использоваться такие технологии как резервирование, зеркалирование, виртуализация.

В зависимости от целей и задач пользователя могут использоваться различные виды систем хранения данных (DAS, NAS, SAN).

В докладе приводится подробная классификация современных систем длительного хранения данных. Рассматриваются модели доступа к СХД, позволяющие оценить важные характеристики качества обслуживания.

Попова Е.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

МНОГОКРИТЕРИАЛЬНЫЙ ОПТИМИЗАЦИОННЫЙ ВЫБОР СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ (СЗИ) ДЛЯ МАЛЫХ ПРЕДПРИЯТИЙ

При оценке сложных систем, приходится иметь дело с несколькими критериями работы системы, которые в совокупности влияют на оценочные показатели и требуют нахождения оптимизационных значений. В экономико–математическом моделировании широко распространены однокритериальные задачи. Многокритериальные задачи часто нивелируются до однокритериальных, используя субъективный выбор доминирующего критерия. При этом искусственно занижается роль остальных критериев, и они используются в виде ограничений. Но для решения задачи сравнения объектов, поиска оптимизационного варианта с учётом всех критериев в условиях неопределённости, связанной с дефицитом информации, наиболее подходит модифицированный метод рандомизированных сводных показателей (ММРСП).

Проблемы информационной безопасности играют всё более значимую роль для малых предприятий. Создатели вредоносных программ давно обратили внимание, что не на всех малых предприятиях уделяют информационной безопасности должное внимание. Вместо того, чтобы взламывать систему крупной компании, можно украсть данные из нескольких малых предприятий и остаться при этом незамеченным. Специально созданные программы сканируют компьютеры в незащищённых системах, поставляя полученные данные. Для сохранения конкурентных преимуществ малым предприятиям нужно охранять свои базы данных, накапливать информацию о возрастных, гендерных, финансовых особенностях клиентов, историю взаимодействия с компанией, причины отказа клиентов от сотрудничества. Круглосуточное интерактивное общение с клиентами через Web-сайты компании позволяет минимизировать издержки, связанные с затратой на рекламу, маркетинговыми исследованиями, тонко подстраиваться под субъективные особенности целевой аудитории. Уделяя должное внимание информационной безопасности, предприятие получает дополнительное конкурентное преимущество и выгодно выделяется на фоне остальных конкурентов. Кроме того, согласно закону ФЗ-152 «О персональных данных» субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и компенсацию морального вреда в судебном порядке. То есть разглашение приватных сведений может привести к судебным искам, юридическим издержкам, ухудшению репутации компании и падению её конкурентоспособности. Организуя комплексную СЗИ для малого предприятия, поэтапно выстраивая её для конкретного предприятия и выбирая оптимизационный многокритериальный вариант, можно добиться значительного повышения информационной безопасности.

После обследования предприятия, предлагается несколько вариантов СЗИ для данного предприятия, каждый из которых можно оценить по определённым критериям, причём по каждому критерию ранжирование объектов не совпадает. Каждый из критериев для нас важен, и нам необходимо выбрать лучший вариант построения СЗИ для данного предприятия в целом, с учётом всех критериев. Например, необходимо построить СЗИ, которая имеет оптимизационные значения по защите предприятия от угроз нарушения доступности, целостности и конфиденциальности информации.

ММРСП основан на экспертных оценках сравниваемых объектов по шкале каждого из критериев. Формируется вектор показателей, каждый из которых является функцией исходных характеристик. Строятся сводные показатели с учётом дефицита информации о значениях весовых коэффициентов. Неопределённость, связанная с дефицитом информации, компенсируется рандомизацией значений весовых коэффициентов, и превращает весовые коэффициенты и сводные показатели в случайные величины. Поэтому задача сравнения сводных показателей сводится стохастическому доминированию рандомизированных сводных показателей. Дефицит информации о весовых коэффициентах приводит к понижению точности расчётов, увеличению дисперсии и небольшой достоверности упорядочивания объектов. Использование нечисловой, неточной и неполной информации (ннн-информации), устраняет эти проблемы.

Сравнивая полученные сводные показатели, мы сравниваем системы защиты информации, и методом рейтингования получаем многокритериальный оптимизационный вариант для данного предприятия, который повышает его информационную безопасность.

Проснеков С.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СВОБОДНОРАСПРОСТРАНЯЕМЫХ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ ДЛЯ ИСПОЛЬЗОВАНИЯ В МАЛОЙ СЕТИ

Системы обнаружения вторжений (англ. - Intrusion Detection Systems, IDS) – одна из главных частей систем информационной безопасности сетей любого современного предприятия. Рост в последние годы количества проблем, связанных с информационной безопасностью, привёл к тому, что системы обнаружения вторжений очень быстро стали важным компонентом любой системы комплексной и сетевой защиты. В настоящее время популярность набирают свободно распространяемые системы обнаружения вторжений, которые предоставляют продукт обладающий хорошими характеристиками и не требующий покупки лицензий. Но так как продукты на данном рынке распространяются по системе as-is (как есть), то никто не несет ответственности если система не справится возложенными на нее задачами. Поэтому очень важно правильно выбрать и протестировать такую свободно распространяемую СОВ, чтобы быть уверенным в том, что в нужный момент она справится со своей задачей.

В данной работе (данном докладе) приводиться сравнительный анализ трех свободнораспространяемых систем обнаружения вторжений: двух сетевых СОВ (Snort, Suricata) и одной хостовой СОВ (OSSEC). Сравнительный анализ базируется на первоначальном тестировании вышеуказанных систем обнаружения вторжений, а затем моделировании их работы на специально созданном макете малой гетерогенной сети. Моделирование работы производилось с использованием специализированного ПО (ShadowSecurityScanner, NessusSecurityScanner, XSpider).

Был создан стенд для реализации модели малой сети с использованием систем обнаружения вторжений.

Состав оборудования: МЭ CISCOASA 5505 и два ПК с виртуальными машинами VmWare и сетевыми картами IntelPRO/1000 Quadport.

С помощью CiscoASA 5505 было создано 4 виртуальных сети (Vlan 10, Vlan 20, Vlan 30, Vlan 40):

- Vlan 10 – Windows Server 2008 (AD, DHCP, DNS)
- Vlan 20 – клиентский компьютер (XP1)
- Vlan 30 – клиентский компьютер (XP2)
- Vlan 40 – «OSSEC»сервер.

Наибольший интерес при тестировании представляли два конкурирующих продукта: сетевые системы обнаружения вторжений «Snort» и «Suricata». Несмотря на то, что системы достаточно близки друг к другу по принципам работы и заявленным характеристикам, «Snort» показал лучший результат как по количеству обнаруженных угроз, так и по удобству эксплуатации. Единственная подходящая по условиям тестирования хостовая СОВ, по результатам подтвердила, что полностью соответствует заявленным характеристикам и выполняет свои функции.

Главной задачей этой работы, был синтез информации о свободно распространяемых СОВ и их тестирование и моделирование в условиях малой сети. Данная работа может быть применена как информационный материал при выборе свободно распространяемой системы обнаружения вторжений. Но следует отметить, что в любой отдельно взятой сети, где планируется внедрение СОВ, необходимо произвести анализ и моделирование работы СОВ, чтобы быть уверенным в том, что данная система сможет выполнять свои функции в данной сети.

Пуха Г.П.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

СИСТЕМЫ ИНТЕЛЛЕКТУАЛЬНОЙ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ – ИННОВАЦИОННОЕ НАПРАВЛЕНИЕ ИССЛЕДОВАНИЙ И ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИТ

1) Современное развитие ЭВТ обеспечило широкие возможности для создания и успешного использования средств обработки данных различного назначения, а, поэтому, одним из актуальных направлений развития современных информационных технологий становится разработка, так называемых, систем интеллектуальной поддержки принятия решения (СИППР) в органах управления (ОУ) предприятиями. Информационные системы данного класса представляют собой системы, максимально приспособленные к решению задач повседневной управленческой деятельности и являются инструментом, призванным оказать помощь лицам, принимающим решения.

СИППР, как правило, являются результатом мультидисциплинарного исследования, включающего теории баз данных, искусственного интеллекта, интерактивных компьютерных систем, методов имитационного моделирования, обеспечивающих выбор решений некоторых неструктурированных и слабоструктурированных задач, в том числе и многокритериальных.

Актуальность разработки и применения подобных систем очевидна. С одной стороны, она обуславливается слишком высокой «ценой» не обосновано принятых, например, экономических решений, а, с другой - сложностью такого обоснования без соответствующих вспомогательных средств.

В то же время, состояние дел в указанном направлении развития современных информационных технологий, особенно в области разработки СИППР для ОУ предприятиями сферы сервиса, нельзя признать удовлетворительным, даже несмотря на появление многочисленных поисковых информационных систем, создаваемых на основе технологий поиска и баз данных.

В связи с этим, возникает необходимость исследовать вопрос о формировании СИППР и технологиях их реализаций именно с методологических позиций.

2) Действительно, исследования процессов принятия решений при управлении в различных сферах человеческой деятельности показывают, что их обоснованность напрямую зависит от корректности той методологии, которая заложена в основу оценки эффективности функционирования объекта управления, а также - выработки целесообразного варианта корректирующих его поведение воздействий, и реализована в соответствующих расчетных методиках [6].

В связи с этим необходимо иметь в виду, что научная проблема, связанная с разработкой СИППР в той или иной области состоит, обычно, не столько в том, как строить их программные средства, а, сколько в том - как оценивать эффективность работы управляемого объекта и как вырабатывать оптимальное решение на изменение его состояния.

Таким образом, необходимо признать, что самым важным условием (методологическим принципом) успешного формирования и функционирования СИППР, в том числе и для предприятий сферы сервиса, является, прежде всего, наличие в их основе комплекса специальных расчетных задач, обеспечивающих анализ (хотя бы) и (еще лучше) синтез структуры управляемого объекта. При этом также очевидно, что все эти задачи должны быть подчинены единой цели их решения, которая предполагает либо определение выбранного показателя эффективности в случае анализа объекта, либо нахождение экстремума показателя эффективности при оптимизации процесса работы объекта. Кроме этого, требуется установить взаимосвязи между частными задачами, по соответствующим показателям и согласовать их по входным и выходным параметрам. Это условие, в первую очередь, предполагает выбор иерархии показателей, необходимых для оценки эффективности принятого решения и разработку методик для их определения.

3) Архитектура программных средств данного класса должна обеспечивать наиболее полную реализацию функциональных возможностей таких методик, их согласование по входным и выходным данным между собой и сопряжения с общей базой данных. Кроме этого она должна позволять централизованное и децентрализованное использование методик, возможность модернизации и наращивания программных средств, а также - интегрирования усилий разработчиков (организаций) при создании сложных систем. При этом реализация таких противоречивых требований к их архитектуре находится в достаточно сильной зависимости от степени научного развития принципов их разработки и обоснованного выбора соответствующей технологии.

И в этом смысле, представляется перспективным организация и проведения в масштабе университета инициативных научно-исследовательских работ, а также открытие в рамках направления «Прикладная информатика в сфере сервиса» магистерской программы «Системы интеллектуальной поддержки принятия решений».

Тихомиров С.А., Богатырев В.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики,
Санкт-Петербургский государственный экономический университет

АГЕНТНО-ОРИЕНТИРОВАННАЯ СИСТЕМА ЗАЩИТЫ ОТ DDOS-АТАК

Одним из эффективных подходов к проектированию систем защиты корпоративных информационных систем (КИС) от DDOS-АТАК, с учетом фактора распределенности узлов вычислительной системы и инфраструктуры системы защиты, клиент-серверной парадигмы, а также динамично изменяющегося профиля трафика, поступающего в КИС, непредсказуемого характера потенциальных атак и их вариативности, является агентно-ориентированный подход. Данный подход к проектированию предполагает декомпозицию общей задачи противодействие ddos-атакам на ряд меньших задач, каждая из которых решается отдельной сущностью системы защиты, называемой агентом (например, задача принятия решения о выборе тактики противодействия атаке). Каждый из агентов в относительной степени автономен от остальных агентов и способен принимать решения самостоятельно на уровне отведенной ему компетенции.

Для агентно-ориентированной архитектуры системы защиты рационально выделить три группы агентов – агенты статистического анализа (address controller agent - ACA), агенты сигнатурного анализа (sensor protocol agent - SPA) и агенты мониторинга файлов состояния системы (system monitor agent - SMA). С учетом различия в ресурсозатратах на тот или иной вид анализа введем несколько уровней жизнедеятельности системы агентов, когда агенты, отвечающие за более ресурсозатратную деятельность (анализ и противодействие) будут активироваться только когда, когда с атакой не справляются агенты, отвечающие за менее ресурсозатратные операции.

На первом уровне системы защиты находятся агенты ACA, отвечающие за контроль над источниками трафика. Они анализируют статистические данные трафика, составляют базовые профили пользователей и подсетей, выполняют блокировку адресов. Агенты статистического анализа должны быть расположены на серверах, подключаемых к каналам связи. Второй уровень системы защиты состоит из агентов SPA, выполняющих сигнатурный анализ трафика, кроме того SPA составляют базовые профили трафика, блокируют вредоносные пакеты. Агенты SPA должны располагаться непосредственно на серверах балансировки нагрузки. Третий уровень защиты представлен агентами SMA. Они выполняют мониторинг состояния КВС, составляют базовые профили пользователей. Агенты SMA должны располагаться непосредственно на серверах, обслуживающих запросы пользователей, т.к. детектируют их активность.

В систему также вводится четвертый управляющий тип агента (supervisor agent - SA), принимающий решения на стратегическом уровне. Агенты SA принимают решения о наличии атаки и выбирают тактику защиты. Агенты SA не работает напрямую с трафиком или иными сервисами КВС, он работает только с данными от других агентов.

Система защиты с предложенной архитектурой способна своевременно обнаруживать атаки, прогнозировать их начало, противодействовать различным типам ddos-атак, выделять легитимные запросы из входящего трафика для продолжения обслуживания лояльных пользователей, учитывать уникальный профиль входящего трафика КИС и его «естественное» краткосрочное и долгосрочное изменение и обеспечивать работоспособность КИС в момент совершения атаки.

Филиппов А.Н., Морозов Ю.С., Кондидатов А.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

ПРИМЕНЕНИЕ ОНТОЛОГИИ В МНОГОАГЕНТНОЙ САПР ТП МЕХАНИЧЕСКОЙ ОБРАБОТКИ ДЕТАЛЕЙ

В статье затронута тема применения онтологии в многоагентной САПР ТП механической обработки деталей.

Многоагентная система — это система, в которой два или более агента взаимодействуют друг с другом, в которой агент — это независимая компьютерная система, находящаяся в некоторой среде, способная автономно действовать в ней для достижения своих целей.

Использование онтологий позволяет отделить семантику используемых в процессе проектирования ТПП понятий от непосредственно данных, которые они представляют.

Онтология может быть представлена в виртуально-строковом пространстве технологических данных (ВСПТД).

Методология ВСПТД предполагает создание единой информационной среды описания технологических данных и знаний.

В ВСТПД онтология реализуется через триплет (основной структурный элемент информационной среды).

Словарь метаданных или онтологический словарь — наиболее универсальное средство, обеспечивающее документирование, хранение и контроль описания данных.

Словарь делится на локальный и глобальный словари данных.

Во время работы над темой исследованы существующие методы применения онтологии.

На основе словаря метаданных САПР ТП ТЕХКОМ была принята базовая структура онтологического словаря.

Для создания словаря планируется разработка редактора, с помощью которого можно будет заносить в него новые данные без большой затраты времени.

Помимо создания самого словаря нужно прорабатывается система импорта/экспорта данных между системами и словарем. Для этого предполагается использовать формат данных XML. Если же система не поддерживает импорт/экспорт в XML, то следует разработать конвертер.

Также планируется продумать взаимодействие агентов с базовым агентом (ВСПТД) и получение информации от них.

Харинов М.В., Заболотский В.П.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ЦЕЛОЧИСЛЕННАЯ ОЦЕНКА КОЛИЧЕСТВА ИНФОРМАЦИИ В ЗАДАЧАХ СТЕГАНОГРАФИИ И РАСПОЗНАВАНИЯ ИЗОБРАЖЕНИЙ

Известно, что в современной информатике и, в частности, в обработке сигналов (изображений) понятие информации недостаточно структурировано и формализовано. При этом понятия «информация», «сигнал» и «смысл» информации не всегда четко разграничиваются между собой, при рассмотрении количества информации обычно обходится вопрос об уточнении понятия самой информации, а также вопрос о верификации расчетных значений количества информации, локализованной в пикселях изображения.

Необходимость уточнения понятия информации и количества информации возникает при обработке сигналов из заранее не ограниченной предметной области, например, при решении задачи «слепой» стеганографии, в которой требуется обратимо встроить один сигнал в другой при условии, что оба сигнала при приеме не известны.

Другим примером является общая проблема распознавания изображения, в которой для унификации выделения или идентификации объектов необходимы общие признаки пикселя, дополняющие яркость. В числе немногочисленных общих подходов к распознаванию изображений известна дескриптивная теория анализа изображений И.Б. Гуревича на основе алгебраического подхода к распознаванию образов Ю.И. Журавлева. Как отмечают авторы подхода, успех применения теории в целом зависит, прежде всего, от предварительного «преобразования изображения к виду, удобному для распознавания без нарушения специфики изображения», которое рассматривается в качестве существенного этапа обработки изображения. При этом условиями подготовки видеоданных для распознавания считаются их иерархическая структуризация и отображения (морфизмы), сохраняющие установленные отношения между пикселями изображения. Вероятно, для строгой формализации указанного этапа обработки полезно уточнить понятие информации и решить проблему единого представления информации изображения при хранении, преобразовании и передаче.

Для уточнения понятия информации и упрощения решения указанных проблем мы разработали модель изображения, в которой оно рассматривается как запоминающая среда и своеобразное средство или устройство для хранения и передачи кодированной информации. Согласно модели атрибутом изображения является цифровая «виртуальная» память, которая подобна памяти компьютера и способна хранить коды информации независимо от предусмотренных преобразований изображения.

В 2008 г. модель сигнала с виртуальной памятью защищена двумя патентами РФ, оформленными СПИИРАН совместно с фирмой Самсунг. В реализованных решениях виртуальная память используется для явной или скрытной передачи встроенных в изображение данных «сообщений». В докладе модель сигнала с виртуальной памятью обобщается для применения в области автоматического распознавания изображений в задаче выделения объектов по информационным признакам.

Основой модели является, так называемое, инвариантное изоморфное представление, которое не зависит от предусмотренных преобразований или искажений изображения и вычисляется без нарушения порядка яркостей пикселей изображения. Указанное представление получается изотоновым преобразованием средних по кластерам яркостей в целочисленные значения результирующего изоморфного представления изображения. Арифметические операции со значениями пикселей инвариантного изоморфного представления (умножение на 2, деление нацело на 2 и на 4, сложение с 1 и др.) порождают последовательность инвариантных представлений изображения и иерархическую последовательность квазиоптимальных кусочно-постоянных приближений изображения. При этом арифметические преобразования инвариантных представлений друг в друга интерпретируются как операции со значениями пикселей в ячейках виртуальной памяти, которая порождается изображением.

В докладе отмечается, что иерархические квазиоптимальные приближения изображения по суммарной квадратичной ошибке аппроксимируют перекрывающиеся оптимальные приближения, но при расчете квазиоптимальных приближений снимается подавляющее большинство вычислительных проблем, характерных для получения оптимальных приближений. В модели сигнала с виртуальной памятью процедура сегментации изображения для автоматического выделения объектов описывается как извлечение кодов информации из инвариантного представления. При этом количество информации обеспечивается прямым подсчетом битов извлеченной информации. Оценка количества информации оказывается целочисленной, но, тем не менее, она согласуется с классическими оценками по Р.В. Хартли и К.Э. Шеннону.

Результаты, представленные в докладе представляют интерес для междисциплинарной области защиты информации и распознавания изображений.

Шаршов А.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОГО ВЗАИМОДЕЙСТВИЯ АВТОМАТИЗИРОВАННЫХ ТРАНСПОРТНЫХ ЛИНИЙ С ПРОМЫШЛЕННЫМ ОБОРУДОВАНИЕМ

Характерной чертой современного этапа развития производства является автоматизация производственных процессов на основе достижений в области электроники, техники и информационных технологий.

Автоматизации подвергаются как технологические процессы, так и процессы транспортировки. На многих предприятиях применяются конвееры, по которым заготовки, детали или материалы последовательно перемещаются между обрабатывающими станциями. В таком случае, в любой момент времени можно определить, местоположение груза на конвеере, и при этом не требуется сложных алгоритмов управления. Но если производство гибкое, и груз может перемещаться между станциями по сложному маршруту, и если груз разнородный, то возникает задача по контролю его местоположения на транспортной линии. Иначе, в случае внештатной ситуации груз может просто потеряться на пути к месту назначения, или будет доставлен не на ту станцию, что в худшем случае приведет к поломке оборудования. В докладе рассмотрен вопрос обеспечения контроля и безопасности взаимодействия транспортной линии и станций на примере гибкой транспортной линии, расположенной в лаборатории автоматизированной сборки микрообъективов на ЛОМО.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ГИДРОМЕТЕОРОЛОГИИ

Александрова Л.В., Попов Н.Н.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет

УЧЕТ И РАСПРЕДЕЛЕНИЕ СЕТЕВОЙ НАГРУЗКИ С ПОМОЩЬЮ СПЕЦИАЛИЗИРОВАННЫХ СРЕДСТВ МОНИТОРИНГА ОБОРУДОВАНИЯ

Любая локальная сеть, в том числе корпоративная, требует постоянного контроля с целью оперативного выявления как уязвимостей и брешей в безопасности, так и проблем в работе серверного и сетевого оборудования с целью их оперативного устранения. В случае большого количества пользователей и значительного трафика появляется также необходимость оптимального распределения нагрузки между каналами и серверами, то есть требуется сегментация сети с учетом локальной нагрузки в каждом из сегментов.

В данном случае была решена задача сегментации сети с управляемыми коммутаторами 2-го уровня.

Одним из наиболее используемых и удобных для отслеживания сети и оборудования является протокол SNMP, поддерживаемый почти любым сетевым устройством и серверами. На использовании данного протокола основаны простейшие средства автоматического мониторинга.

Последние должны предоставлять в удобном для восприятия виде, предпочтительно графическом, постоянно обновляемую информацию о доступности сетевых объектов, а также о разных параметрах систем и сетей.

В работе для определения перегруженного трафиком сегмента с последующей его реструктуризацией использовались такие системы как Cacti и Nagios. Также рассмотрен Zabbix как альтернативное решение для мониторинга сетей.

Cacti является веб-приложением (набором скриптов), которое позволяет наблюдать за загрузкой ЦП сервера, видеть на графике среднюю загрузку памяти за период времени, количество DNS запросов приходящих на сервер, количество писем (спама) приходящих на почтовый сервер. Cacti собирает статистические данные по входящему и исходящему трафику за определённые временные интервалы и позволяет отобразить их в графическом виде. Данная система может быть расширена, так как позволяет использование пользовательских скриптов и темплейтов. Nagios в первую очередь служит для мониторинга сетевых служб (SMTP, POP3, HTTP, SNMP, NNTP, ICMP) и мониторинга состояния хостов (включаю разные параметры, такие как загрузка процессора, использование диска, системные логи, данные с разных системных датчиков) в большинстве сетевых операционных систем, включая коммутаторы. Nagios также позволяет строить онлайн карту-схему сети с маршрутизаторами и коммутаторами.

Анализ графиков, сформированных в Cacti, на узлах постоянного мониторинга, узловых коммутаторах, позволил выделить наиболее загруженный сегмент. Рассматривались графики по аплинковым портам с различным осреднением по времени с целью выявления, в том числе кратковременных пиковых нагрузок.

Далее с помощью Nagios определялась структура исследуемого сегмента, определялись параметры дополнительного мониторинга, а также структуры соседних сегментов на предмет изменения схемы построения исследуемого, а именно включение выбранных нижестоящих коммутаторов в соседние сегменты.

В результате исследований был определен сегмент, обуславливающий критическую загрузку канала в пиковое время. Было признано целесообразным не изменять структуры соседних сегментов, а включить указанный сегмент в отдельный порт вышестоящего коммутатора с расширением доступной пропускной способности канала.

Григорьев Р.С., Калинин В.О., Моргунов М.А.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРИ ПРОВЕДЕНИИ ГИДРОЛОГИЧЕСКИХ И ГИДРОГРАФИЧЕСКИХ ИССЛЕДОВАНИЙ МИРОВОГО ОКЕАНА

На современном этапе развития информационных технологий в освоении Мирового океана, площадь которого составляет около 71% поверхности Земли, особое внимание уделяется обеспечению защищаемой информации при проведении гидрографических и специальных работ.

Экологическая безопасность морских ресурсов является приоритетной задачей. Большую опасность в акваториях представляет загрязнение вод нефтью и нефтепродуктами (основными загрязнителями), некоторыми тяжёлыми металлами и отходами атомной промышленности. Вредные вещества разносятся различными течениями по всем водам Мирового океана. В результате аварий в результате судоходства и других катастроф, экологии наносится непоправимый урон. Для ликвидации последствий и своевременного их предотвращения необходимо решить следующие задачи:

– измерение химических параметров воды;
– ультразвуковое зондирование толщи воды;
– определение точных координат;
– сбор, обобщение, обработка и архивирование информации.

Все эти данные способны быстро ликвидировать негативные последствия, оценить ущерб и даже предотвратить их.

Сумма всех измерительных систем образует универсальный комплекс, который включает в себя: различные зонды, аппаратуры сканирования, GPS навигации, устройства отбора проб, программное обеспечение, геоинформационные системы, различные технологии.

Геоинформационная система(ГИС)- представляет собой систему сбора, хранения, анализа и графической визуализации пространственных данных и связанной с ними информацией о необходимых объектах. Что позволяет иметь удобную возможность работы с данными.

Типичная структура ГИС состоит:

1. Данные (пространственные данные):
   – позиционные (географические): местоположение объекта на земной поверхности;
   – непозиционные (атрибутивные): описательные.
2. Аппаратное обеспечение (ЭВМ, сети, накопители, сканер, дигитайзеры и т.д.).
3. Программное обеспечение (ПО).
4. Технологии (методы, порядок действий и т.д.).

Данные прогноза погоды, штормовые предупреждения, места мелей, опасных подводных объектов, помогут предотвратить катастрофы. А быстрые сборы данных и максимально приближенные прогнозы катастроф, помогут быстро и без лишних затрат ликвидировать последствия.

Для упрощения и улучшения качества работы создаются новые и передовые измерительные системы. И поэтому модернизация и их совершенствование является не только актуальным, но и перспективным делом.

На сегодняшний день в гидрологических и гидрографических измерительных системах идет бурный процесс развитий и новшеств, что значительно улучшает качество и способы работы. Что так же позволяет наряду с обеспечением экологической обстановки, решать задачи информационной безопасности при обеспечении специальных работ в гидрометеорологии.

Завируха В. К., Замятин А. Ю.
Россия, Санкт-Петербург, Арктический и антарктический научно-исследовательский институт, Москва, Федеральная служба по гидрометеорологии и мониторингу окружающей среды

СОЗДАНИЕ И ИСПОЛЬЗОВАНИЕ ОБЪЕКТОВЫХ ПУНКТОВ И СЕТЕЙ МНОГОФУНКЦИОНАЛЬНЫХ РАДИОЛОКАЦИОННЫХ КОМПЛЕКСОВ

За последние десятилетия существенно возросли производительность вычислительных средств и пропускная способность каналов связи, что позволяет значительно повысить информативность, объем и защищенность данных, методов и средств при построении систем дистанционного зондирования. Изменилась и идеология представления ресурсов и сервисов; наблюдается уход от «владения» к «получению по требованию». В работе рассматривается радарный сервис RxaaS (Radar … as a Service), основанный на совместном использовании многофункциональных РЛС. Тремя основными разновидностями RxaaS являются:

1) технические средства радара «по требованию» – RSaaS (Radar System as a Service);
2) «сырые» данные радара «по требованию» – RDaaS (Radar Data as a Service);
3) радиолокационная информация «по требованию» – RIaaS (Radar Information as a Service).

Три вышеперечисленные разновидности сервисов имеют различные уровни «добавленного интеллекта». В первом варианте РЛС на определённом отрезке времени предоставляется заинтересованным потребителям на уровне интерфейсов управления РЛС и интерфейса данных приёмо-передатчика. Таким образом, удалённый или локальный пользователь получает «виртуальную РЛС», поток её «сырых» данных обрабатывает полностью самостоятельно.

RDaaS не предоставляет пользователю возможностей управления радаром, а обеспечивает только доступ к потоку «сырых» данных.

В случае RIaaS пользователю предоставляется тематическая информация, полученная на основе обработки поставщиком услуг «сырых» данных с помощью соответствующих алгоритмов. При этом «сырые» данные могут обрабатываться в интересах различных потребителей:

1) системы контроля за фоно- целевой обстановкой;

2) системы навигационного управления различными видами транспорта (воздушного, надводного, наземного и т.п.);

3) системы оперативного контроля за атмосферными и гидрологическими штормовыми и опасными явлениями погоды и процессами;

4) системы оперативного контроля за технологическими и несанкционированными выбросами (сбросами) загрязняющих веществ в окружающую среду и т.п.

Дальнейшим развитием сервисов многофункциональных радарных комплексов RxaaS является переход к сервисам многофункциональных радарных сетей RNxaaS (Radar Network … as a Service). В случае RNxaaS реализуются как публичные, так и частные (наложенные) сервисы, обеспечивающие закрытый и защищённый доступ к радарным данным и информации определённому сообществу потребителей.

Для RNxaaS тематические направления, территориальная и ведомственная принадлежность радиолокационных пунктов съёма информации, а также системы в целом становятся зачастую объектом ведомственной или коммерческой тайны, а иногда и государственной безопасности. В подобных случаях доступ к системе, к ее исходным данным или обобщенной (комплексной) информации может осуществляться только после прохождения соответствующей аккредитации уполномоченным центром управления доступом. Особое внимание должно быть уделено регламентированному доступу зарубежным потребителям и их агентам на территории России.

Построение сетей многофункциональных радиолокационных комплексов целесообразно начинать с радиолокационных объектовых пунктов принадлежащих различным государственным (или близких к государственным) структурам. В этом случае на ранней стадии реализации проекта может быть достигнут существенный временной и экономический эффект от совместного многофункционального использования развернутых и функционирующих технических и информационных ресурсов различных министерств и ведомств. Дальнейшим развитием сетей радиолокационных комплексов может стать интегрирование в их состав дополнительных средств дистанционного зондирования, а также контактных и бесконтактных датчиков, использующих совместно с радарной системой каналы информации, средства обработки и комплексирования разнородных данных для предоставления тематических сервисов конечным потребителям.

Канаев А.К., Опарин Е.В.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения

МОДУЛЬ СПЕЦИАЛЬНОГО МАТЕМАТИЧЕСКОГО И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ПО АВТОМАТИЗАЦИИ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ УПРАВЛЕНИЯ СЕТЬЮ ТАКТОВОЙ СЕТЕВОЙ СИНХРОНИЗАЦИИ ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЫ ОАО «РЖД»

Одной из основных составляющих любой современной телекоммуникационной системы (ТКС) является сеть тактовой сетевой синхронизации (ТСС), выполняющая функции формирования, передачи и распределения сигналов синхронизации, необходимых для поддержания устойчивого функционирования всех цифровых устройств ТКС. Функционирование такой сложной технической системы как сеть ТСС невозможно без автоматизации процессов принятия решений по её техническому обслуживанию (ТО), что обуславливает необходимость создания автоматизированной системы поддержки принятия решений (АСППР) при системе управления (СУ) ТСС ТКС.

Модуль специального математического и программного обеспечения (СМПО) по автоматизации поддержки принятия решений управления сетью ТСС ТКС ОАО «РЖД» предназначен для обеспечения руководителей различных уровней управления сетью ТСС ОАО «РЖД» своевременной, обоснованной и рациональной поддержкой в принятии решений по управлению сетью ТСС, что позволит обеспечить устойчивость функционирования сети тактовой сетевой синхронизации в телекоммуникационной системе ОАО «РЖД»

Модуль СМПО по автоматизации поддержки принятия решений управления сетью ТСС ТКС ОАО «РЖД» работоспособен с учётом взаимозависимости показателей функционирования телекоммуникационной системы ОАО «РЖД» и сети тактовой сетевой синхронизации, что позволяет формировать своевременные и обоснованные решения по управлению сетью тактовой сетевой синхронизации большого масштаба и высокой сложности при воздействии дестабилизирующих факторов различного характера. База знаний модуля СМПО по автоматизации поддержки принятия решений управления сетью тактовой сетевой синхронизации построена с применением фреймового механизма представления знаний, который наиболее полно удовлетворяет требованиям внутренней интерпретируемости, структурируемости, связности и активности знаний. Указанная база знаний содержит параметры и характеристики оборудования сети ТСС, состояний сети ТСС и стратегии по управлению сетью ТСС, а также процедуры логического вывода стратегий управления сетью ТСС.

Основой выработки стратегий по управлению сетью ТСС ТКС ОАО «РЖД» является классификация состояний, в котором находится сеть. Классификация состояния необходима с той точки зрения, что она позволяет определить основные классы отказов на сети ТСС, что позволит обоснованно выбирать силы и средства на устранение отказа и восстановление сети ТСС. В основе

классификации состояний сети ТСС лежит информация, хранящаяся в базе знаний модуля СМПО по автоматизации поддержки принятия решений управления сетью тактовой сетевой синхронизации.

Для количественной оценки сходства состояний сети ТСС использованы характеристики и параметры, которые находятся в слотах и фреймах базы знаний модуля СМПО по автоматизации поддержки принятия решений управления сетью тактовой сетевой синхронизации.

Анализ различных метрик позволил выявить, что применительно к задаче классификации состояний сети ТСС наиболее рационально использовать метрики типа расстояния и коэффициента корреляции с применением соответствующих алгоритмов. Применение данных алгоритмов классификации является ключевым этапом формирования модуля СМПО по автоматизации поддержки принятия решений управления сетью ТСС. Указанные алгоритмы позволяют своевременно и обоснованно определять класс состояний, в котором находится сеть ТСС, формировать новые классы состояний по результатам классификации в условиях специфики оборудования, масштаба сети, видов дестабилизирующих воздействий и подготовки персонала. Результаты автоматизированной классификации состояний сети ТСС являются исходными данными, на основе которых в последующем решается задача выработки стратегий управления сетью ТСС, что позволит повысить оперативность и своевременность принимаемых решений по управлению сетью ТСС ТКС ОАО «РЖД».

На основе классифицированного состояния сети ТСС производится выработка конкретных стратегий и планов по управлению сетью ТСС. Следует отметить, что выработка стратегий и планов управления сетью ТСС происходит в диалоговом режиме и в тесной взаимосвязи с оператором-экспертом

Модуль СМПО по автоматизации поддержки принятия решений управления сетью тактовой сетевой синхронизации телекоммуникационной системы ОАО «РЖД» входит в состав функциональных подсистем ЕСМА, являющейся базовым блоком системы управления сетью связи технологического сегмента ОАО «РЖД». Модуль СМПО по своей структуре и кругу решаемых задач не имеет аналогов среди существующих систем управления телекоммуникационными сетями.

Митько А.В.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОДВОДНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ В УСЛОВИЯХ АРКТИЧЕСКОГО РЕГИОНА

На современном этапе защита информации, циркулируемой в подводных телекоммуникационных системах, особенно в условиях возросшего интереса к Арктическому региону является актуальной научной задачей. В существующих условиях эскалации террористической деятельности особое место среди задач обеспечения безопасности жизнедеятельности занимает задача предупреждения угроз террористического и криминального характера важным объектам инфраструктуры различных ведомств. Террористические и криминальные угрозы могут приводить к нарушениям функционирования объектов на длительный срок, к большим экономическим потерям и человеческим жертвам. За рубежом, наряду с силами проведения специальных операций, стремительными темпами развиваются технологии, позволяющие создавать роботизированные технические средства и, прежде всего, автономные необитаемые и необслуживаемые малоразмерные аппараты для решения задач специальных операций. В связи с этим, для обеспечения эффективной охраны важных объектов, необходимо в составе ведомственных АСМО предусматривать специальные локальные автоматизированные подсистемы контроля обстановки (АСКО), работающие прежде всего по малым и сверхмалым целям, таким как малое плавсредство, автомобиль, дельтаплан, пешеход, пловец и т.п.

Учитывая, что задача охраны важных объектов достаточно идентична в разных ведомствах, для уменьшения затрат времени и финансов на проектирование АСКО и обеспечение высокой эффективности их функционирования необходимо:

– ввести такие системы в ранг финансируемых и контролируемых государством систем, аналогично системам обеспечения навигационной (эксплуатационной) безопасности, таких как система управления движением судов (СУДС), для чего следует разработать соответствующую нормативную базу АСКО, которая должна быть положена в основу решения задач проектирования, развертывания, сертификации и эксплуатации таких систем;

– под государственным контролем (в рамках государственной программы) разработать типовую АСКО, включающую в себя все необходимые виды оборудования для обеспечения контроля надводной, подводной, наземной и воздушной обстановки, на базе которой будут разрабатываться АСКО для конкретных объектов охраны;

– в нормативной базе АСКО предусмотреть их создание путем адаптации типовой АСКО под конкретные объекты охраны за счет подбора необходимого количества ее различных элементов (оборудования) и привязки их к местности, что обеспечит применение в АСКО только утвержденных

решений и сертифицированного оборудования и существенно сократит затраты на их проектирование.

Таким образом создание таких систем в Арктической зоне на межведомственном уровне в значительной степени позволит решить задачу информационной безопасности в подводных телекоммуникационных системах от существующих и перспективных угроз.

Митько А.В., Авдеенко А.В., Кротенко В.Ю.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет

ПРИНЦИПЫ ЗАЩИТЫ ИНФОРМАЦИИ В ТРЕНАЖЁРНЫХ ОБУЧАЮЩИХ СИСТЕМАХ В ГИДРОМЕТЕОРОЛОГИИ

Государственный стандарт определяет тренажёр как техническое средство профессиональной подготовки гидрометеоролога, предназначенное для формирования и совершенствования у обучающихся профессиональных навыков и умений, необходимых им для управления материальным объектом, путём многократного выполнения обучающимися действий, свойственных процессу управления материальным объектом. Тренажерная подготовка позволяет выработать навыки и умения у обучающихся в процессе одиночной и комплексной подготовки по использованию вычислительной техники.

В тренажерных комплексах предметом несанкционированного доступа является циркулирующая в ней информация сведения о лицах, предметах, событиях, явлениях и процессах системы независимо от формы представления, что само собой является чрезвычайной ситуацией. Объектами несанкционированного доступа выступают информационные технологии и каналы связи, объединяющие их в систему. Защиту от проникновения в тренажерные комплексы злоумышленников необходимо строить с учетом комплексной структуры защищаемых объектов, начиная с информации и программного продукта пользователей санкционированных абонентов тренажеров и заканчивая защитой систем передачи данных (каналов связи).

Система защиты должна иметь иерархическую структуру с наращиванием свойств защищенности информации.

Первый уровень защиты информации пользователя это уровень вычислительной системы, в котором для обеспечения закрытия утечки информации необходим комплекс мероприятий.

Второй по счету, но не по значимости уровень защиты сетевой. Под сетевым уровнем защиты следует понимать комплекс мероприятий, направленных на обеспечение закрытия каналов утечки информации в распределенной вычислительной системе. Это относится как к техническим средствам вычислительных сетей (контроллеры связи, адаптеры канала, серверы и другое сетевое оборудование), так и к программным средствам сетевой поддержки.

Третий уровень защиты системный, включает комплекс мероприятий защиты от несанкционированных воздействий на технические средства и каналы телекоммуникаций.

Каждый из уровней защиты тренажеров наряду с общими методами и способами защиты, приемлемыми для всех уровней иерархии, имеет свои особенности, характерные только для него.

На основе сложившейся иерархии тренажерных комплексов способы защиты целесообразно рассматривать в той последовательности, в которой развивалась структура создания тренажеров, от простого к сложному. Вначале была создана вычислительная система (ЭВМ), которая увеличивала умственные потенции человека; затем сеть ЭВМ, обеспечивающая возможность коллективного решения сложных задач; и как последнее звено эволюции вычислительной системы ИТКС, способная обеспечивать распределенную структуру удаленных пользователей услугами вычислительной системы по обработке гидрометеорологической информации.

Митько А.В., Авдошина А.И., Халзакова А.А.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕЖИМЕ «СЕТЕЦЕНТРИЧЕСКИХ ВОЙН» В ГИДРОМЕЕОРОЛОГИИ

Рассмотрение вынесенной проблематики наиболее эффективно вести в терминологии достаточно общей (в смысле универсальности применения теории управления (ДОТУ), поскольку всякий процесс может быть интерпретирован как процесс управления либо самоуправления. Здесь необходимо подчеркнуть, что ДОТУ и «кибернетика» в её исторически сложившемся виде это содержательно разные вещи. При взгляде с позиций достаточно общей теории управления информационная безопасность это устойчивое течение процесса управления объектом (самоуправления объекта), в пределах допустимых отклонений от идеального предписанного режима, в условиях целенаправленных сторонних или внутренних попыток вывести управляемый объект из предписанного режима. Таким образом, термин «информационная безопасность» всегда связана с конкретным объектом управления, находящимся в определенных условиях (среде). Но кроме того он относится к полной функции управления, представляющей собой совокупность разнокачественных действий, осуществляемых в процессе управления, начиная от идентификации факторов, требующих

управленческого вмешательства и формирования целей управления, и кончая ликвидацией управленческих структур, выполнивших свое предназначение.

Это общее в термине «информационная безопасность» по отношению к информационной безопасности как самого мелкого и незначительного дела, так и информационной безопасности человечества в целом. При более широком взгляде информационная безопасность в определённом выше смысле средство обеспечения безопасности по всем параметрам всякого культурно своеобразного общества в границах северных регионов. Вне разрешения этой проблематики права человека не могут быть гарантированы. Последнее по существу означает, что информационная безопасность в этих аспектах носит двухуровневый характер, обеспечиваемый:

– избранием концепции глобализации (в смысле построения единой культуры человечества, интегрирующей в себя все национально-своеобразные культуры в их лучших проявлениях), гарантирующей безопасность государства;

– качеством управления по избранной концепции глобализации и приведением в соответствии с нею внутренней и внешней политики государства. Одно из наиболее широких определений, которое можно дать термину «сетевая война», война, в которой невозможно однозначное определение противника и линии фронта, разделяющей территории, подконтрольные воюющим сторонам.

Применение обобщённых средств управления оружия реально протекает на основе трёх способов управления: структурное управление, основанное на предварительном создании структур с однозначно определённой функциональной нагрузкой элементов в архитектуре структуры и компетенцией входящих в её состав управленцев и прочего персонала. Бесструктурное управление, основанное на безадресном распространении в среде информации, откликаясь на которую среда сама из своих элементов порождает множество функционально целесообразных структур. По существу бесструктурное управление представляет собой управление статистикой откликов среды на прохождение в ней информации. Управление на основе виртуальных структур. Оно на всяком иерархическом уровне в организации среды, проводящей информацию, представляет собой выражение иерархически высшего по отношению к нему управления, в ходе которого структуры заблаговременно развёртываются в среде, проводящей информацию, но они не видны с того иерархического уровня, в котором развёрнуты. В силу этого управление на основе виртуальных структур с этого уровня среды может восприниматься как «спонтанные процессы», которые носят неуправляемый характер. Сетевая война не битва одиночек. Поэтому субъект, претендующий на реализацию своих целей в режиме «сетевых войн» и не владеющий всеми названными выше средствами, обречён на поражение. Это неизбежное следствие того, что даже если он сам бессознательно эффективно владеет всем названным, то в силу коллективного характера деятельности общества в режиме «сетевых войн», не освоив понятийный аппарат ДОТУ и не распространив его в обществе, он не состоянии выстроить долговременную стратегию ведения такой войны и организовать общество на победу в такой войне с учётом гидрометеорологических условий.

Привалов А.А., Вандич А.П.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения

МОДУЛЬ СПЕЦИАЛЬНОГО МАТЕМАТИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ ЕДИНОЙ СИСТЕМЫ МОНИТОРИНГА И АДМИНИСТРИРОВАНИЯ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ОАО «РЖД»

Железнодорожный транспорт играет важную роль в развитии России в экономическом, социальном и других аспектах. Он позволяет, прежде всего, осуществлять грузовые и пассажирские перевозки на всей территории страны, обеспечивая возможность налаживания деловых отношений между различными субъектами РФ. Не стоит также исключать из поля зрения значение ОАО «РЖД» как военной организации, позволяющей решать средствами существующей инфраструктуры поставленные руководством задачи. Система связи на железнодорожном транспорте, как сложная организационно-техническая система, с одной стороны, является частью системы более высокого уровня – системы управления перевозками, а с другой – включает в себя элементы, также являющиеся системами (узлы связи, линии связи и др.). Система управления перевозками включает в себя автоматизированную систему управления, систему связи, систему разведки и другие специальные системы. Таким образом, система управления перевозками, функционирование которой связано со сбором данных, принятием решения и доведением его до исполнителя, полностью определяется состоянием системы связи. Поэтому чрезвычайно важной является такая организация связи, которая позволяет в любых условиях поддерживать работоспособное состояние системы управления перевозками. Ключевую роль при этом играет достоверная передача информационных сообщений, которая может быть достигнута путем анализа существующей системы управления сетью связи и ее модернизации.

Поэтому актуализируется задача разработки модуля специального математического обеспечения для единой системы мониторинга и администрирования (ЕСМА) телекоммуникационной сети (ТКС) ОАО «РЖД» в целях поддержки принятия решений по управлению функционированием, восстановлением и устранением отказов ТКС ОАО «РЖД».

Модуль специального математического обеспечения, содержащий комплекс математических моделей процессов функционирования сетей связи в прогнозируемых условиях, предназначен для повышения обоснованности принимаемых решений по управлению телекоммуникационными сетями ОАО «РЖД».

Модуль специального математического обеспечения является центральным в структуре специального математического программного обеспечения (СМПО) ЕСМА и предоставляет данные для автоматизированной методики анализа результатов и выдачи рекомендаций должностным лицам дирекции связи по восстановлению работоспособности после возникновения отказов элементов ТКС ОАО «РЖД». Модуль СМПО структурно состоит из согласованных по входным и выходным данным субмодулей:

– мониторинга по видам сетей (SDH, IP-СПД (сеть передачи данных), ОТС/ОбТС (общетехнологическая/оперативно-технологическая сеть), ТСС (сеть тактовой сетевой синхронизации));
– оценки качества предоставления услуг служб электросвязи;
– оценки радиоэлектронной защищенности и безопасности связи ТКС ОАО «РЖД»;
– моделирования распределения потоков информации;
– оценки качества функциональных подсистем;
– блок анализа результатов и выдачи рекомендаций.

Полученные рекомендации и результаты оценки используются для обоснования вырабатываемых решений по управлению телекоммуникационными сетями ОАО РЖД с целью восстановления их работоспособности и адаптации к изменившимся условиям функционирования. Использование модуля специального математического обеспечения в структуре СМПО ЕСМА позволит повысить обоснованность принимаемых решений и сократить длительность цикла управления телекоммуникационными сетями ОАО «РЖД» более чем в два раза. Оценка длительности цикла управления производится на основе моделирования процесса функционирования ЕСМА за счет декомпозиции анализируемого на несколько этапов. Совокупность указанных этапов и частных подпроцессов соответствует алгоритму функционирования ЕСМА, описанному в «Регламенте работы центра управления технологической сетью связи, центров технического управления и центров технического обслуживания. Том 2. Стратегия 1. Управление инцидентами».

Модуль СМПО входит в состав функциональных подсистем ЕСМА и являющегося базовым блоком в системе управления сетью связи технологического сегмента РЖД. Модуль СМПО по своей структуре и кругу решаемых задач не имеет аналогов среди существующих систем управления телекоммуникационными сетями.

Привалов А.А., Рыхлов П.В., Чалов И.В., Евглевская Н.В.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения

ОБ УСТРОЙСТВЕ ПРЕДОТВРАЩЕНИЯ ВЫДЕЛЕНИЯ АКУСТИЧЕСКОЙ ИНФОРМАЦИИ В ПОМЕЩЕНИЯХ, ОСВЕЩАЕМЫХ КОМПАКТНЫМИ ЛЮМИНИСЦЕНТНЫМИ ЛАМПАМИ

Энергосберегающие технологии на сегодняшний день являются очень востребованными. Вопрос о повсеместном внедрении таких технологий, в том числе и осветительных приборов, постоянно поднимается на разных уровнях, включая законодательный. Однако использование широко разрекламированных компактных люминесцентных ламп (далее КЛЛ), приводит к возникновению других проблем, одной из которых является утечка информации. И этот вопрос стоит весьма остро, особенно, если речь идет о конфиденциальной информации.

Внедряемые повсеместно КЛЛ имеют встроенный преобразователь напряжения (далее ЭПРА), предназначенный для преобразования напряжения первичной электрической сети в высокочастотный сигнал с фиксированной частотой, находящейся в коротковолновом диапазоне частот. Это обеспечивает возникновение канала для передачи акустической информации за счет наличия паразитного электромагнитного излучения (ПЭМИ), возникающего во встроенном преобразователе напряжения.

Исследования, результаты которых приведены в настоящем докладе, выполнялись с использованием бытовой энергосберегающей лампы, выбранной в торговой сети.

С целью затруднения съема злоумышленником акустической информации в состав ЭПРА КЛЛ был установлен генератор шума, изменяющий случайным образом частоту преобразования в пределах, обеспечивающих устойчивую работу преобразователя.

По результатам эксперимента было определено, что радиочастота, излучаемая КЛЛ перестала быть фиксированной и съем акустической информации с КЛЛ стал сильно затруднен.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЭКОЛОГИИ

Афанасьев В.П., Камышев И.В., Ломовцев С.В., Орехов Д.Л., Теруков Е.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина),
ООО «НТЦ тонкопленочных технологий в энергетике при ФТИ им. А.Ф. Иоффе»

ПРОБЛЕМЫ ЭКОЛОГИИ И СОВРЕМЕННОЕ СОСТОЯНИЕ ТОНКОПЛЕНОЧНОЙ СОЛНЕЧНОЙ ЭНЕРГЕТИКИ

Прогресс, достигнутый в технологии тонкопленочных солнечных модулей, уже позволил обеспечить паритет в стоимости электроэнергии. Соотношение стоимости «солнечной» и «сетевой» электроэнергии определяет географию экономически эффективной эксплуатации солнечных электростанций в странах с развитыми электросетями. Решить задачу удешевления «солнечной» электроэнергии можно путём перехода на более дешевые тонкопленочные технологии изготовления солнечных элементов. Существует технология производства тонкопленочных солнечных модулей на основе CdTe. Лидером по производству данных модулей является фирма FirstSolar, которая уверенно обосновалась на европейском рынке. Данные модули имеют неплохой стабильный КПД порядка 14%, но при его использовании и утилизации возникают экологические проблемы. Кадмий токсичный материал, поэтому модули в конце срока их службы необходимо специально утилизировать на свалках тяжелых металлов или они должны проходить специальную процедуру переработки. В процессе эксплуатации при разбитии стекла Cd может абсорбироваться и загрязнить почву.

У тонкопленочной технологии на основе кремния нет таких недостатков. По распространённости в земной коре кремний занимает второе место после кислорода и его содержание составляет ~29%. Развитие микроэлектронной промышленности за последний век накопило достаточно мощностей по производству и очистке кремния. Очистка кремния происходит путем ректификации и восстановления силана до металлического кремния, так что о трудности обеспечения поставок силана для массового производства модулей говорить не приходится.

Тонкопленочные кремниевые модули не загрязняют окружающую среду, их не нужно специальным образом утилизировать. Процессы в ходе производства модулей технологичные и энергетически низкозатратные. Осаждение структур приборного качества на большую площадь возможно благодаря технологии плазма-химического осаждения кремния из моносилана в атмосфере водорода. Данная технология безопасна, и не представляет угрозы для окружающей среды, так как отработавшие газы из камеры дожигаются в скруббере и затем нейтрализуются. В качестве серьезного конкурента на рынке тонкопленочных солнечных модулей заявляет о себе технология CIGS (Copper-Indium-Gallium-Diselenide). Модули на основе данного материала уже сейчас имеют ~12% КПД. Проблемы в данной технологии также имеются. Частично селенизированный композитный четырехкомпонентный сплав вступает, при температуре примерно в 500-550oC, в реакцию в течение примерно 30 минут. Высокая температура осаждения делает невозможным использование гибких подложек, а большая толщина получаемого слоя требует использование в достаточных количествах редкоземельных металлов.

Целью данной работы является знакомство с состоянием и развитием тонкопленочной солнечной энергетики в России с позиций ее влияния на экологию окружающей среды. В России запущен ряд крупных проектов по развитию солнечной энергетики. Например, группа компаний «РЕНОВА», приняла решение наладить производство 1 млн. солнечных модулей в год в Чувашии, а также создать в Санкт-Петербурге ООО «НТЦ тонкопленочных технологий в энергетике при ФТИ им. А.Ф. Иоффе», оснащенный современным технологическим и метрологическим оборудованием.

Афанасьев В.П., Бобыль А.В., Иванов Г.А., Ершенко Е.М., Плешков Д.В., Скворцов Д.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина),
Физико-технический институт им. А.Ф. Иоффе РАН

МОНИТОРИНГ ЭФФЕКТИВНОСТИ РАБОТЫ СОЛНЕЧНЫХ МОДУЛЕЙ НА ШИРОТЕ САНКТ-ПЕТЕРБУРГА

Солнечная радиация является эффективным источником возобновляемой энергии на Земле, а фотовольтаические преобразователи обеспечивают экологичность и безопасность ее получения. Однако эффективность генерирования энергии солнечной электростанцией существенно изменяется

в зависимости от расположения модулей и условий окружающей среды таких, как освещенность, температура, время суток и других. Поэтому для объективной оценки энергоэффективности солнечных станций в зависимости от климатических условиях и особенностей эксплуатации необходим мониторинг их работы.

Мониторинг эффективности работы проводился на базе автономной солнечной электростанции на основе тонкопленочных фотопреобразователей, размещенной на крыше 5 корпуса СПбГЭТУ «ЛЭТИ». В ее состав входят фотоэлектрические модули, контроллеры заряда, аккумуляторные батареи, датчики радиации, температуры, имитатор нагрузки, электронный регистратор, характеристики которых будут приведены в докладе.

Электронный регистратор фиксирует в блоке энергонезависимой памяти такие параметры, как: вырабатываемый ток, напряжение и мощность в точке максимальной мощности фотоэлектрических модулей; температуру на тыльной поверхности фотоэлектрических модулей; уровень солнечной радиации, измеренный кремниевым фотоприемником. Для мониторинга метеоданных система комплектуется метеостанцией, которая позволяла осуществлять круглогодичный сбор данных с записью на локальный компьютер. Ко всем получаемым данным обеспечивается доступ через глобальную сеть интернет.

Для установления корреляционной зависимости параметров солнечных модулей в работе проводилось непрерывное измерение мощностных, температурных характеристик двух пар солнечных модулей, установленных под разными углами к горизонту. Отбор энергии от фотоэлектрических модулей обеспечивается системой из контроллера заряда с поиском точки максимальной мощности, аккумулятора и имитатора нагрузки, который включался при достижении верхнего порога зарядки аккумуляторных батарей и отключается при разряде до нижнего порога.

Разработанная система мониторинга позволяет раздельно проводить измерение мощностных, температурных характеристик двух пар солнечных модулей, находящихся в одинаковых погодных условиях, но при разных углах ориентации к горизонту (часть модулей размещена под прямым углом к горизонту, другая ориентируется под углом, оптимальным для широты Санкт-Петербурга).

Введенная в эксплуатацию энергоустановка будет использована как для научных исследований, так и в учебном процессе на кафедре квантовой электроники и оптико-электронных приборов СПбГЭТУ «ЛЭТИ».

На основе экспериментальных данных проведен анализ эффективности работы станции в зависимости от условий эксплуатации и расположения модулей относительно горизонта; рассмотрены особенности эксплуатации солнечных модулей и предложены методики исследования солнечных модулей, которые могут быть использованы для постановки лабораторных работ по дисциплинам «Тонкопленочные солнечные элементы» и «Метрология тонкопленочных солнечных модулей и энергоустановок».

Агафонова Д.С., Сидоров А.И., Колобкова Е.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

ЛЮМИНЕСЦЕНТНЫЕ ОПТИЧЕСКИЕ СТЕКЛА И ВОЛОКНА КАК ЧУВСТВИТЕЛЬНЫЕ ЭЛЕМЕНТЫ ВОЛОКОННО-ОПТИЧЕСКИХ ДАТЧИКОВ ЭЛЕКТРИЧЕСКОЙ ДУГИ, ИСКРЫ И ТЕМПЕРАТУРЫ ДЛЯ ПРЕДУПРЕЖДЕНИЯ АВАРИЙНЫХ СИТУАЦИЙ

Создание чувствительных и надежных датчиков является необходимым этапом при построении информационно-измерительных систем (ИИС). Одной из областей применения ИИС является обеспечение правильной и безопасной работы устройств и оборудования и предупреждения аварий, связанных с возникновением взрывоопасных и пожароопасных ситуаций. Причинами возникновения аварий может быть искренне, короткое замыкание, сопровождаемое электрической дугой, и перегрев оборудования. В условиях высоких электромагнитных помех хорошо себя зарекомендовали волоконно-оптические датчики (ВОД). Разработка чувствительных элементов ВОД электрической дуги, искры и перегрева является важной задачей.

В работе исследованы люминесцентные оптические волокна для детектирования УФ и коротковолнового видимого излучения. В волокнах из силикатных фото-термо-рефрактивных стекол возможно создание люминесцентной оболочки и сердцевины, содержащей молекулярные кластеры серебра. Волокна обладают интенсивной люминесценцией в области 450-800 нм при возбуждении люминесценции в диапазоне длин волн 250-530 нм. Оптическое излучение электрического разряда возбуждает люминесценцию и волноводные моды в чувствительном элементе на основе данных волокон. При этом происходит спектральное преобразование излучения в длинноволновую область, уменьшающее потери полезного сигнала в ВОД. Эффективность преобразования излучения разряда в волноводные моды и величина спектрального сдвига определяет чувствительность датчика. В работе показано, что использование данных люминесцентных волокон позволяет увеличить чувствительность ВОД дуги и искры по сравнению с существующими аналогами. В работе также

исследованы оксифторидные стекла, содержащие молекулярные кластеры серебра. Стекла обладают высокой температурной чувствительностью интенсивности люминесценции. Введение ионов редкоземельных металлов (Sm, Tb) увеличивает температурную чувствительность материала. Значение температурной чувствительности для данных стекол выше на порядок по сравнению с наиболее часто используемыми люминесцентными материалами (на основе Nd, Er и пр.) в ВОД температуры.

Результаты могут быть использованы при проектировании волоконных сенсорных систем для защиты устройств и оборудования от искрения, перегрева и коротких замыканий, сопровождаемых электрической дугой, для предприятий нефтяной и газовой отрасти, химической промышленности, энергетики и на транспорте.

Алексеева-Попова Н.В., Дроздова И.В., Беляева А.И.
Россия, Санкт-Петербург, Ботанический Институт им. В.Л. Комарова РАН

ОЦЕНКА РЕГИОНАЛЬНОГО ФОНОВОГО УРОВНЯ ТЯЖЕЛЫХ МЕТАЛЛОВ В РАСТЕНИЯХ ПОЧВАХ ПРИ МОНИТОРИНГЕ ЗАГРЯЗНЕНИЯ СРЕДЫ В ЛЕНИНГРАДСКОЙ ОБЛАСТИ

Оценка экологической безопасности таких крупных промышленных центров, как Санкт-Петербург, на основании содержания тяжелых металлов в объектах биосферы невозможна без сопоставления с региональным фоновым уровнем. С этой целью в Ленинградской области был проведен фоновый мониторинг особо охраняемых природных территорий: Юнтоловского и Гладышевского заказников и памятников природы: «Парк «Сергиевка» и «Комаровский берег». Для обследования уровня накопления загрязняющих веществ на 12 пробных площадях было взято 27 образцов почв, 122 образца высших сосудистых растений и мхов. Атомно-абсорбционным методом было изучено содержание тяжелых металлов: Fe, Mn, Zn, Cu, Pb, Ni, Cr, Co, Cd в растениях и почвах сравниваемых территорий.

Табл.1 Среднее содержание тяжелых металлов в почвах, мг/кг*

Охраняемые территории	Fe	Zn	Mn	Cu	Ni	Co	Cr	Cd	Pb
ЮЗ	1719	32,3	65,3	11,8	4,73	1,52	0,19	0,30	25,7
ГЗ	1444	5,05	20,3	3,52	1,35	0,45	1,02	0,09	14,2
ПС	1281	13,1	32,0	6,62	3,48	1,27	1,32	0,13	13,7
КБ	2844	7,9	31,9	3,26	1,34	0,45	1,51	0,17	16,6
Среднее	1822	14,6	37,4	6,29	2,73	0,92	1,01	0,17	17,6

Примечание. Здесь и в табл.2 и 3: заказники: ЮЗ – Юнтоловский , ГЗ – Гладышевский; памятники природы: ПС – «Парк «Сергиевка», КБ – «Комаровский берег».

* - 1 н. азотнокислая вытяжка

Полученные данные показывают диапазон изменчивости содержания тяжелых металлов в почвах и индикаторных видов растений в фоновых условиях среды. Наиболее низким уровнем содержания Cd, Ni, Cu, Zn, Co характеризуются почвы Гладышевского заказника и памятника природы «Комаровский берег».

Табл.2. Среднее содержание тяжелых металлов в высших сосудистых растениях, мг/кг

Охраняемые территории	Fe	Zn	Mn	Cu	Ni	Co	Cr	Cd	Pb
ЮЗ	67,5	76,0	855	5,48	1,53	0,33	0,21	0,38	1,29
ГЗ	42,6	48,4	869	5,42	1,80	0,10	1,20	0,16	1,34
ПС	96,3	29,4	520	5,71	2,44	0,34	1,38	0,13	1,97
КБ	55,4	42,4	816	4,89	1,22	0,32	0,64	0,14	1,65
Среднее	65,4	49,1	765	5,38	1,75	0,27	0,86	0,20	1,56

Поскольку в высших сосудистых растениях уровень аккумуляции таких загрязнителей среды, как Ni, Cr, Cd, Co, Pb незначителен, для уточнения региональных фоновых содержаний этих элементов в качестве объектов были использованы листостебельные мхи.

Табл.3 Среднее содержание тяжелых металлов в мхах, мг/кг

Охраняемые территории	Fe	Zn	Mn	Cu	Ni	Co	Cr	Cd	Pb
ЮЗ	334	59,0	258	6,61	1,99	0,49	1,16	0,24	7,36
ГЗ	185	37,6	282	5,07	1,58	0,32	1,09	0,23	4,23
ПС	629	67,0	349	8,70	3,80	1,68	2,56	0,35	7,02
КБ	180	38,1	477	7,50	1,22	0,49	0,56	0,23	5,50
Среднее	332	50,4	342	7,0	2,15	0,75	1,34	0,26	6,03

Показано, что уровень накопления тяжелых металлов в мхах на всех изученных территориях выше, особенно Fe, Pb, Ni, Cu, Co, Cr. Широко распространенные на Северо-Западе листостебельные

мхи являются хорошими мониторами для определения величины почвенного и аэротехногенного загрязнения среды и оценки экологической безопасности.

Наибольшей экологической чистотой отличается территория заказника Гладышевский, уровень аккумуляции тяжелых металлов в растениях и почвах которого можно рассматривать как региональный фон. Средние содержания тяжелых металлов могут быть использованы при фитомониторинге загрязнения среды Северо-Запада.

Бархатов А.В., Веремьев В.И., Ковалев Д.А., Коновалов А.А., Михайлов В.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ИСПОЛЬЗОВАНИЕ СИСТЕМ ПОЛУАКТИВНОЙ РАДИОЛОКАЦИИ В ЭКОЛОГИЧЕСКОМ МОНИТОРИНГЕ ГИДРОСФЕРЫ И АТМОСФЕРЫ

В докладе рассматриваются вопросы использования полуактивной радиолокации (ПАРЛ), особенностью которой является использование сигналов сторонних источников, для экологического мониторинга.

Основные достоинства ПАРЛ системы связаны с отсутствием в ее составе собственного передатчика, роль которого выполняют штатно функционирующие передатчики теле- и радиовещания. Из достоинств отметим меньшую стоимость производства, размещения и эксплуатации, отсутствие необходимости выделения частот, отсутствие вредного воздействия на окружающую среду и помех другим радиотехническим устройствам. Кроме того, достоинством ПАРЛ систем является возможность формирования произвольной зоны наблюдения за счет широкой сети достаточно мощных передатчиков подсвета и оптимального выбора местоположения.

Система ПАРЛ в общем случае состоит из нескольких разнесенных в пространстве передающих и приемных позиций. Местоположение стороннего передатчика ПАРЛС известно. Зная координаты передатчика и приемных позиций, измеряя задержку между временем приема прямого и переотраженного целью сигналов, можно рассчитать дальность цели. Кроме дальности, ПАРЛ система измеряет бистатический доплеровский сдвиг частоты отраженного сигнала и угловые координаты цели. В мультистатической системе ПАРЛ при наличии синхронных измерений несколькими приемниками возможно одномоментное измерение полного вектора скорости цели.

Как и в системах активной радиолокации, системы ПАРЛ могут использоваться для решения задач исследования и мониторинга природных сред: для водной среды – составление карт поверхностных течений и оценка параметров волнения, освещение ледовой обстановки, отслеживание уровня воды с целью прогнозирования наводнений и пр.; для воздушной среды – обнаружение турбулентных областей, обнаружение, слежение и оценка степени опасности (грозовой, градовой) облачных систем; а для обеих этих сред – обнаружение различного рода загрязнений, оценка их интенсивности и прогнозирование их распространения.

В качестве частного случая использования полуактивной локации можно предложить концепцию построения систем мониторинга в труднодоступных районах, например, в Арктической зоне, с применением сигналов КВ-диапазона, которые в состоянии обеспечить обнаружение и оценку характеристик объектов на дальностях до нескольких сотен и даже тысяч километров.

Бузников А.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ДИСТАНЦИОННАЯ СПЕКТРОМЕТРИЯ РАСТИТИЕЛЬНОГО ПОКРОВА ОДИН ИЗ МЕТОДОВ ОЦЕНКИ ЭКОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ РЕГИОНА

Переход на путь устойчивого развития общества, провозглашенный ООН и принятый Россией, предусматривает применение дистанционных методов исследования, на основе которых может производиться диагностика состояния природных экосистем на больших территориях. В этой связи актуальным является установление и изучение признаков, характеризующих состояние экосистем, и разработка имитационных моделей, адекватно отображающих их эволюцию под влиянием антропогенных воздействий.

Одним из основных загрязнителей атмосферы и почвенного покрова являются тяжелые металлы. Причем наиболее заметный вклад в ухудшение экологического состояния региона вносят металлургическая и химическая промышленность, а также автомобильный транспорт, численность которого за последние годы стремительно возрастает. Целями настоящей работы являлись теоретические и экспериментальные исследования влияния тяжелых металлов на спектральную отражательную способность растений. В результате установлены корреляционные связи и регрессионные зависимости между оптическими параметрами листьев и концентрациями тяжелых металлов в растениях. Установлены индикаторные виды городской растительности для дистанционной экспресс-оценки загрязнения территорий тяжелыми металлами с помощью спектральной аппаратуры. В результате корреляционно-регрессионного анализа установлены

спектральные индексы для индикаторных видов растительности, характеризующие уровни содержания в них тяжелых металлов. Составлены таблицы зависимостей спектральных индексов индикаторных видов от уровней концентраций тяжелых металлов и экологического состояния окружающей среды, являющихся основой метода дистанционной диагностики загрязнения. Разработан метод дистанционной оценки загрязнения индикаторных видов растительности тяжелыми металлами с помощью спектральной аппаратуры.

Бунина Ю.Е., Готюр И.А., Костромитинов А.В.
Россия, Санкт-Петербург, Военно-космическая академия имени А.Ф.Можайского

МЕТОДИКА ВЫЯВЛЕНИЯ И УСТРАНЕНИЯ ИСКАЖЕНИЙ ЭКОЛОГИЧЕСКОЙ ИНФОРМАЦИИ

Вопрос информационной безопасности при решении задач гидрометеорологического обеспечения является одним из актуальных. Это связано с тем, что поступающая по каналам связи гидрометеорологическая информация может подвергаться искажениям различного характера, устранение которых может достигаться путём применения существующих методов контроля гидрометеорологической информации при обработке данных. Однако, несмотря на наличие множества подходов, задача устранения искажений в полной мере не решена.

Исходя из оперативной практики, к серьёзным последствиям может привести искажение полей геопотенциала, которые чаще всего используются в оперативной работе метеорологических подразделений. Предлагаемая методика позволяет выявлять и устранять искажения полей геопотенциала за счёт привлечения в качестве дополнительной информации данных, поступающих от метеорологических искусственных спутников Земли (МИСЗ).

Разработанная методика позволяет использовать информацию о поле облачности при объективном анализе поля геопотенциала и основывается на сплайн-аппроксимации. При такой аппроксимации не используются сведения о статистической структуре поля, и обеспечивается получение глобальных непрерывных полей диагностируемых величин. Кроме того, существует возможность привлекать при аппроксимации не только значения величин, но и их производные по направлениям. В качестве информации, используемой нами при анализе поля геопотенциала, используется информация о координатах центров циклонов и значения зональных и меридиональных составляющих векторов скорости ветра. Эта информация получается в результате обработки данных уровня 1В (географически привязанные и радиометрически калиброванные изображения), поступающих от спутников космических комплексов NOAA и Метеор-3М. На первом этапе этой обработки формируется маска облачности. На втором этапе определяется наличие облачности, идентифицируемой логарифмической спиралью. Третий этап заключается в определении координат и параметров спирали, позволяющих определить координаты центра циклона, а также направление и скорость ветра в различных точках спирали.

Наличие облачности, идентифицируемой логарифмической спиралью определяется методом корреляционно-экстремальной идентификации. Набор эталонных спиралей и связанные с ними характерные значения направлений и скоростей ветра в ее различных точках получены статистически.

Полученная информация используется для выявления и устранения искажений полей геопотенциала следующим образом. В исходной задаче минимизации, положенной в основу построения аппроксимационного сплайна, в качестве ограничений используются значения геопотенциала, полученные от сети аэрологического зондирования, и значения производных по направлениям, определяемые по данным от МИСЗ. В свободной атмосфере для полей геопотенциала в качестве такой информации можно использовать зональные и меридиональные составляющие векторов скорости ветра. Возможность их использования обусловливается тем, что в первом приближении в атмосфере выше пограничного слоя режим движения определяется градиентом геопотенциала и силой инерции Кориолиса. В центрах циклонов значения производных по направлениям принимают нулевые значения.

Проведенные численные эксперименты показали хорошую согласованность уточненных полей геопотенциала, полученных по разработанной методике, и полей облачности, видимых на снимках, получаемых от МИСЗ, что говорит о возможности ее использования при выявлении и устранении искажений метеорологической информации.

Василевский А.М., Коноплев Г.А., Степанова О.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ОЦЕНКА СТЕПЕНИ ЗАГРЯЗНЕНИЯ ВОДЫ ПО УФ СПЕКТРАМ ПОГЛОЩЕНИЯ

Абсорбционный спектральный анализ в УФ области является одним из перспективных методов экспресс контроля степени загрязнения воды. Данный метод позволяет проводить интегральную оценку содержания примесей в пробах воды, а в ряде случаев и определять концентрацию отдельных загрязняющих компонентов. Преимуществами метода являются оперативность, высокая

воспроизводимость, возможность реализации мониторинга в проточном режиме, сравнительно невысокая стоимость используемой аппаратуры, отсутствие необходимости в использовании реактивов, низкая трудоемкость и возможность автоматизации.

Цель исследования – оценка степени загрязнения воды из различных источников, а также оценка эффективности бытовых фильтров, предназначенных для дополнительной очистки питьевой воды.

Спектральные измерения проводились на автоматизированном спектроанализаторе на основе ПЗС фотоприемника в диапазоне длин волн 200...400 нм с разрешением 0.5 нм. Эталоном сравнения служила дистиллированная вода, в ходе измерений были использованы кварцевые кюветы толщиной 5 мм.

Исследовались пробы воды, взятые в искусственных открытых водоемах, колодезной воды, а также воды в водопроводной сети общего пользования в нескольких районах города Санкт-Петербурга. Водопроводная вода подвергалась дополнительной очистке с помощью бытового фильтра с угольным сорбентом.

Результаты исследований показывают, что в спектральной области 200...350 нм уровень поглощения проб взятых из различных источников значительно различается, при этом на спектрах проявляются как селективные полосы поглощения, обусловленные растворенными веществами, так и неселективное рассеяние вызванное взвесями. Большее поглощение соответствует большей концентрации загрязняющих компонентов.

По нашим данным наиболее загрязнена вода в искусственных водоемах (прудах), при этом на спектрограммах имеются интенсивные полосы поглощения в коротковолновой части спектра 200...250 нм, обусловленные комбинацией различных загрязнителей. В спектрах проб водопроводной воды Московского и Фрунзенского районов проявляется достаточно выраженная полоса поглощения с максимумом вблизи длины волны 280 нм. С большой степенью вероятности можно предположить, что данная полоса обусловлена белковыми компонентами, что говорит о наличии биологического загрязнения. В спектрах поглощения колодезной воды нет селективных полос, но ярко выражено рассеяние, что указывает на большое содержание взвесей.

Исследования показали, что после доочистки воды с помощью фильтров со свежим сорбентом уровень поглощения в УФ области существенно падает, что свидетельствует об уменьшении концентрации загрязняющих компонентов. В то же самое время, после прохождения фильтра с сорбентом, который предварительно эксплуатировался в течение 6 месяцев, уровень поглощения возрос, т.е. степень загрязнения увеличилась. Таким образом, использование фильтров позволяет заметно повысить качество питьевой воды, но в процессе эксплуатации фильтра сорбирующие модули должны своевременно заменяться.

Веремьев В.И., Коновалов А.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ ЭКОЛОГИЧЕСКОГО КОНТРОЛЯ ОКРУЖАЮЩЕГО ПРОСТРАНСТВА НА БАЗЕ МНОГОПОЗИЦИОННЫХ РАДИОЛОКАЦИОННЫХ КОМПЛЕКСОВ

В докладе рассматривается вопросы построения перспективных интеллектуальных систем контроля окружающего пространства на базе многопозиционных многодиапазонных радиолокационных комплексов. Предлагается использование многоуровневых методов объединения информации, осуществляющих оценку ситуации, уровня угроз и возможных последствий от принятия тех или иных управленческих решений.

Одним из перспективных направлений развития радиотехнических средств контроля окружающего пространства является разработка и создание интеллектуальных систем на основе радиолокационных средств наблюдения с использованием всего арсенала современных методов совместной обработки информации. Подобного рода системы могут быть наземного, морского или авиационного базирования и применяться при решении задач дистанционного экологического мониторинга гидросферы и атмосферы.

Основными функциями этих систем являются сбор данных, их обработка с целью получения сведений об объектах наблюдения, оценка ситуации в целом путем логического вывода или интеллектуальных методов, прогнозирование развития ситуации, принятие решения о реагировании. Ядром такой системы, ответственным за сбор первичной информации, должен стать многопозиционный радиолокационный комплекс, осуществляющий мгновенное и всепогодное обнаружение и измерение параметров объектов, появляющихся и перемещающихся в его зоне ответственности.

Для описания структур систем объединения данных, поступающих от отдельных датчиков радиолокационной системы, и методов объединения предлагается модель JDL (Joint Directors of Laboratories). Она включает в себя набор взаимодействий процессов в ходе объединения данных, а также интерфейсы взаимодействия с набором датчиков, базами данных и человеком-оператором. Набор информационных взаимодействий в модели JDL представлен в виде совокупности пяти уровней: 0 (обработка сигналов и признаков), 1 (оценка объекта), 2 (оценка ситуации), 3 (оценка воздействия), 4 (оценка процесса объединения).

Викторов С.В.
Россия, Санкт-Петербург, Санкт-Петербургский научно-исследовательский центр экологической безопасности РАН, Санкт-Петербургский государственный университет

ЭФФЕКТИВНОСТЬ ДИСТАНЦИОННЫХ МЕТОДОВ ОБНАРУЖЕНИЯ НЕФТЯНЫХ ЗАГРЯЗНЕНИЙ (НА ПРИМЕРЕ БАЛТИЙСКОГО МОРЯ)

На основе данных Хельсинкской комиссии по безопасности Балтийского моря обсуждаются результаты авиационных и спутниковых наблюдений нефтяного загрязнения Балтийского моря. Затрагивается проблема достоверности обнаружения нефтяных пятен методом радиолокации со спутников типа RADARSAT и ENVISAT. Приводятся сведения о количестве идентифицированных нарушителей. Сделаны выводы о невысокой эффективности существующей международной системы дистанционных методов обнаружения нефтяных загрязнений в регионе.

Горохов В.Л., Витковский В.В., Бузников А.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный архитектурно-строительный университет, Специальная астрофизическая обсерватория РАН, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

КОГНИТИВНЫЕ ОБРАЗЫ МНОГОМЕРНЫХ РАСПРЕДЕЛЕННЫХ БАЗ ДАННЫХ ЭКОЛОГИЧЕСКОГО И КОСМИЧЕСКОГО МОНИТОРИНГА, КАК ИНДИКАТОРЫ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГО ВТОРЖЕНИЯ В ИХ КОНТЕНТ

Концепция когнитивной компьютерной графики в настоящее время получила достаточно эффективное развитие в рамках научного направления интеллектуальных интерфейсов для поддержки принятия решений и бизнес аналитики. Однако, использование свойств когнитивных образов радикально меняться при изменении хотя бы одного из параметров в многомерном пространстве характеристик может быть использовано для задач диспетчеризации и контроля за несанкционированными воздействиями на терабайтные базы данных. Если речь идет о распределенных базах данных, то здесь возможны пентабайтные массивы и дополнительные механизмы несанкционированного доступа. Такого рода базы данных используются в международных проектах по космическому дистанционному зондированию и международному экологическому мониторингу. Между тем способность представлять весь объем и состояние терабайтных массивов в виде образных наглядных когнитивных «картинок» и при этом индицировать малые изменения в данных в виде радикального изменения вида «картинки» представляется крайне полезным с точки зрения технологий защиты информации. В работе приводится пример многомерной совокупности данных астрофизического мониторинга (RCJ –каталог), представленной в виде когнитивного образа для проверки и иллюстрации описанной выше способности к радикальному изменению когнитивного образа при незначительном изменении одного из 12-ти параметров в тысячах объектов. Показывается радикальное изменение этого образа при незначительном изменении масштаба лишь одного параметра.

Горохов В.Л., Витковский В.В., Бузников А.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный архитектурно-строительный университет, Специальная астрофизическая обсерватория РАН, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

КОГНИТИВНАЯ ВИЗУАЛИЗАЦИЯ ИНДИКАЦИИ ОПАСНОСТЕЙ ВЫЯВЛЯЕМЫХ НА ОСНОВЕ ДИСТАНЦИОННОГО ЗОНДИРОВАНИЯ

В работе проведены исследования по изучению влияния тяжелых металлов на оптические характеристики растений для разработки метода дистанционной оценки загрязнения. Когнитивная машинная графика позволяет оперативно просматривать многомерные таблицы данных мониторинга с целью выявления опасных или экстремальных ситуаций. Приводится наглядный пример использования когнитивной графики иллюстрирующий возможности ее применения.

В 2006 году была проведена серия полевых экспериментов, по результатам которых выявлены индикаторные виды растительности Санкт-Петербурга: мать-и-мачеха, одуванчик и трава. Кроме того, была проведена серия лабораторных экспериментов для установления ПДК тяжелых металлов индикаторных видов растений и градации изменения спектральных характеристик в зависимости от уровня загрязнения. Полученные данные представляют многомерные данные. Один массив представляет измерения концентрации тяжелых металлов в различных типах растений отобранных в зонах мегаполиса, которые представляют различные уровни загрязнения. Второй массив представляет корреляционную связь между различными типами спектральных измеряемых индексов и типами загрязнителей (тяжелых металлы).

Средствами и методами когнитивной визуализации удалось для первого массива выявить и классифицировать отдельные группы видов растений по способности выявлять уровень загрязнений. Для второго массива методами когнитивной визуализации удалось классифицировать спектральные индексы по степени их «чувствительности» к различным тяжелым металлам в растениях.

Горяинов В.С., Бузников А.А., Черноок В.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ВОЗМОЖНОСТЬ ПРИМЕНЕНИЯ ЛИДАРНЫХ СИСТЕМ ДЛЯ КОНТРОЛЯ СОСТОЯНИЯ ВОДНЫХ РЕСУРСОВ

История использования лазеров для исследования окружающей среды начинается с середины 1960-х годов, когда были опубликованы первые работы, посвящённые зондированию атмосферы при помощи лазерных систем], а также предложен метод лазерного зондирования для локации подводных объектов и картирования рельефа]. В дальнейшем подобные системы получили название лидарных, от слова «лидар» (транслитерация LIDAR – англ. Light Identification, Detection and Ranging).

С развитием лазерной техники, вычислительной техники и программного обеспечения, а также постепенным удешевлением компонентной базы, сфера применения лидарных систем несравненно расширилась Лидары успешно используются в метеорологических исследованиях атмосферы, океана, для картографирования земной поверхности и береговой линии, для измерения параметров движения разнообразных объектов, в качестве органов зрения автоматизированных систем, также во многих других областях науки и техники. Одна из причин такого широкого применения в том, что лидарные системы нередко являются единственным средством получения детальной информации об исследуемой среде, при этом сочетая высокие быстродействие и разрешение с отсутствием деструктивного воздействия на объект зондирования.

Среди множества упомянутых выше направлений использования лидарных систем можно выделить следующие, имеющие непосредственное отношение к дистанционному зондированию природной среды:

– Измерение концентрации как основных, так и малых составляющих атмосферы (контроль загрязнений).

– Определение термических, структурных, динамических характеристик атмосферы, океана и подстилающей поверхности.

– Пороговое обнаружение некоторых составляющих (контроль аварийных ситуаций).

– Получение карт параметров рассеяния шлейфами выбросов и их эволюции во времени.

– Распознавание определённых мишеней (нефтяные пятна) по спектральным характеристикам.

Всё вышесказанное показывает эффективность лидарных систем при решении задач исследования водных ресурсов. В современный период наблюдаются две устойчивых тенденции: с одной стороны, расширяется осознание роли Мирового океана в существовании человечества; с другой – продолжается рост экологической нагрузки на земную гидросферу, увеличивается степень использования её биоресурсов, влияние загрязняющих факторов. В данных условиях развитие методов лидарного зондирования и нахождение новых применений для них, несомненно, является одной из первостепенных задач среди технологий обеспечения экологической безопасности региона.

Готюр И.А., Кулешов Ю.В., Маков А.Б, Суворов С.С., Щукин Г.Г.
Россия, Санкт-Петербург, Военно-космическая академия имени А.Ф.Можайского

КОНЦЕПЦИЯ СОЗДАНИЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ МЕТЕОРОЛОГИЧЕСКОГО И ЭКОЛОГИЧЕСКОГО ОБЕСПЕЧЕНИЯ КОСМОДРОМА «ВОСТОЧНЫЙ»

Метеорологическое обеспечение (МО) космодромов, и, в частности, создаваемого в настоящее время космодрома «Восточный», направлено на достижение требуемого уровня безопасности и эффективности пусков ракет космического назначения (РКН). К важнейшим требованиям, предъявляемым к метеорологическому обеспечению, относятся своевременность (оперативность), полнота и достоверность этого вида обеспечения. В связи с этим предъявляются высокие требования к системе сбора (получения), обработки и представления метеорологической информации для принятия решений по выполнению всех этапов подготовки к пуску (транспортировка, разворачивание на позиции и др.) и пуска РКН.

К настоящему времени в нашей стране накоплен большой опыт разработки автоматизированных систем (АС) подобного типа. Однако во всех этих проектах отсутствует комплексная система оперативного сбора, обработки и представления метеорологической информации.

Несмотря на кажущуюся очевидность, построение комплексной системы оперативного сбора, обработки и представления метеорологической информации космодрома сопряжено с рядом проблем. Основной задачей, решаемой при создании АС МО, является выбор совокупности методов, реализующих информационные процессы МО, из множеств методов $\{M\}$, которые могут быть реализованы в системе.

Задачу структурного синтеза АС, обеспечивающую требуемое значение вероятности достижения цели обеспечения, можно свести к оптимизационной задаче. Структура АС МО космодрома $\Omega_i \in \Omega$ должна представлять собой ориентированный ациклический граф. При этом задача оптимизации иерархической структуры может быть записана следующим образом:

необходимо найти $\arg\max P_{эф}(\Omega)$, где Ω – множество иерархических структур – возможных вариантов построения АС МО. Синтез АС МО заключается в последовательности операций выбора из множества вариантов описания $\Omega_i \in \Omega$ и операций оценивания эффективности и совместимости подсистем, образующих синтезированный целостный вариант. Здесь же определяется соответствие варианта требованиям к искомой функциональной системе – от понятия «подходящее решение» до понятия «оптимальное» или «рациональное решение».

Предлагаемый подход позволяет синтезировать АС МО с заданными требованиями к составу и точности метеорологической информации, заблаговременности прогнозов значений метеорологических величин, численности и квалификации обслуживающего персонала, ограничениям на временные и технические ресурсы. При этом синтез можно осуществлять в несколько этапов. Вначале строится система на базе уже имеющихся программных и технических средств и оцениваются ρ_k – «степени близости» реально достигнутых показателей характеристик подсистем $x_{\text{ф}}^{k}$ к требуемым $x_{\text{тр}}^{k}$. В дальнейшем каждую из подсистем можно дорабатывать или заменять, тем самым переходя от «подходящего» к «оптимальному» или «рациональному» решению.

Анализ технологии проведения специальных работ на примере одной из типичных РКН, которой является РКН типа «Зенит», показал, что на космодроме необходимо реализовать все информационные процессы метеорологического обеспечения: производство метеорологических измерений с помощью различных технических средств; сбор измеренной информации; усвоение полученной и собранной информации; диагностика метеорологических условий в районе космодрома; прогнозирование метеорологических условий в районе космодрома, а также выработка рекомендаций по их учету при подготовке и пуске РКН; доведение рекомендаций, диагностической и прогностической информации до органов управления космодромом.

Рассмотрены существующие автоматизированные системы и технические средства, наиболее полно отвечающие предъявляемым требованиям. В результате было найдено «подходящее» решение по созданию АС МО космодрома, которое в дальнейшем должно быть доведено до «оптимального» путем доработки отдельных АС.

Гришканич А.С., Бузников А.А., Редька Д.Н., Жевлаков А.П., Кащеев С.В.
Россия, Санкт-Петербург, ОАО «НПК «Государственный оптический институт им С.И. Вавилова», Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

МОНИТОРИНГ МЕТАНОВЫХ ВЫБРОСОВ В АРКТИКЕ ДЛЯ ОЦЕНКИ ИЗМЕНЕНИЯ КЛИМАТА МЕТОДОМ ЛАЗЕРНОГО ЗОНДИРОВАНИЯ

Арктика является важнейшим компонентом в экосистеме Земли, влияющим на её энергетический баланс, атмосферную и океаническую циркуляцию, запасы пресной воды, уровень моря, хранение и высвобождение большого количества парниковых газов, экономику, инфраструктуру, здоровье, культуру и идентичность, а также жизни миллионов людей.

В настоящее время Арктика драматично изменяется из-за глобального потепления, кроме того, на нее оказывают влияние глобализация и трансграничное загрязнение. Механизм обратной связи между арктической поверхностью и климатической системой будет способствовать усилению эффекта потепления, в то время как наземный лед Арктики все больше способствует глобальному повышению уровня моря. Необходимо следить за всеми изменениями, происходящими в Арктике, документировать их, чтобы смоделировать изменения в криосфере и их последствия. Температура вечной мерзлоты и толщина ее активного слоя, несмотря на некоторое различие по отдельным регионам, в целом увеличились по всей Арктике.

За последние 100 лет темпы повышения температуры в Арктике почти вдвое превысили среднюю скорость потепления на планете (МГЭИК, 2007 г.). С 1954 по 2003 гг. среднегодовая температура воздуха в приземном слое атмосферы Арктики повысилась с 2°C до 3°C в Аляске и Сибири и почти до 4°C в зимний период (ACIA, 2004 г.). Потепление в Арктике сопровождается более ранним началом весеннего таяния, увеличивающейся продолжительностью периодов таяния, а также изменениями в массовом балансе ледниковых покровов Гренландии (Строув и др., 2006 г.; Зуолли и др., 2002 г.). Помимо того, с 1979 по 2006 гг. каждый месяц отмечалось сокращение поверхности ледовых покровов арктических морей (Серрезе и др., 2007 г.). В течение периода таяния 2007 г. общая площадь поверхности морского льда Арктики сократилась до самых низких величин, когда-либо отмечавшихся со времени начала спутникового наблюдения в 1979 г., впервые за всю известную историю полностью открыв для навигации Северо-Западный проход Северного морского пути (NSIDC, 2007 г.).

По предварительным прогнозам к 2100 г. будет наблюдаться широкая деградация вечной мерзлоты по всей Арктике с многочисленными последствиями (например, оползание земли, осушение водно-болотных угодий в одних областях, заболачивание других, увеличение выбросов метана и разрушение инфраструктуры, особенно вдоль береговой линии). Ярким примером является

Ямальский регион: экономическая значимость региона в сочетании с его чувствительностью к глобальному потеплению, проявляющаяся через динамику вечной мерзлоты, и взаимодействие между добывающей промышленностью и средствами существования коренных народов требует наличия исследовательской станции и постоянного мониторинга уровня выброса парниковых газов, для информирования всех заинтересованных лиц о возможном экологическом будущем региона.

Действительно, расконсервация менее 0,1% количества органического углерода, захороненного в верхнем 100-метровом слое мерзлоты (примерно 10000 Гт углерода в форме CH4) может привести к удвоению содержания атмосферного метана, радиационная активность которого примерно в 20 раз выше, чем у CO2.

Выявление метановых аномалий пешеходными маршрутами в условиях арктики требует больших людских трудозатрат и потому малоэффективно. Также малоэффективным является визуальное наблюдение с использованием воздушного транспорта и проботбора.

Несмотря на очевидную актуальность проблемы в настоящее время практически отсутствуют методы выделения, локализации и дистанционной диагностики метановых аномалий, хотя технически такая возможность вполне реализуема. Лидарная аэросъемка, отличается высокой мобильностью и позволяет на значительном расстоянии (сотни метров) обнаруживать признаки наличия на Земной поверхности ничтожных концентраций метана. (не менее 0,0001%).

Развитие и внедрение новых физических методов нелинейного увеличения чувствительности детектирования позволяет реализовать богатейшие и практически неисчерпаемые информационные возможности лазерного зондирования для создания высокоэффективной и конкурентоспособной технологии аэрогеохимического поиска метановых выбросов в условиях Арктики.. Его преимущества по сравнению с традиционными (косвенными), например, физико-химическими, - следующие: дистанционность, бесконтакность, возможность непрерывного площадного и профильного сканирования с одновременным определением широкого набора химических элементов и соединений, а также высокая чувствительность и скорость детектирования (10-6сек).

Автоматизированный бортовой лидар позволит устанавливать мощность метановых выбросов, качественные и количественные параметры аномалий. По данным аэрогеохимической съемки можно будет определять места скопления метана, оперативно отслеживать уровни изменения концентрации, тем самым получая необходимые данные для моделирования климата и прогнозирования степени «глобального потепления». Кроме того возможна оценка экологических и инженерных условий проектирования, строительства и эксплуатации скважин, прокладки трубопроводов и др.

Гришканич А.С., Бузников А.А., Елизаров В.В., Жевлаков А.П., Кащеев С.В.
Россия, Санкт-Петербург, ОАО «НПК «Государственный оптический институт им С.И. Вавилова», Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ЛИДАРНЫЕ КОМПЛЕКСЫ АВИАЦИОННОГО БАЗИРОВАНИЯ С УЛЬТРАСПЕКТРАЛЬНЫМ РАЗРЕШЕНИЕМ

Среди различных экологических бедствий лидирующее место по тяжести последствий занимают чрезвычайные происшествия на атомных объектах («Селлафилд» – Великобритания,1957; Чернобыль – Украина,1986; Фукусима – Япония, 2011 и т.д.). В таких случаях определяющим фактором радиоактивного загрязнения среды являются изотопы инертных газов, цезия, йода, стронция, кобальта.

Современные методы радиационной разведки и радиационного мониторинга достаточно успешно справляются с поиском и локализацией радиоактивных загрязнений гамма-излучающими нуклидами. Однако вопрос дистанционного обнаружения чистых бета-радиоактивных (например, стронций-90) и большинства альфа-радиоактивных выбросов не может быть решен ядерно-физическими методами.

На текущий момент лучшие образцы серийных спектрометров, производимые отечественными и зарубежными фирмами, имеют дальность не более 50 м вследствие фундаментальных ограничений пассивных методов диагностики. Для обнаружения ультрамалых концентраций радионуклидов (1010÷1012 см-3) в атмосфере на больших расстояниях (более 100 м) необходимо применение активных методов дистанционного зондирования, а именно лидаров, размещенных на подвижных платформах. В этой связи дистанционная лазерная спектроскопия может служить высокоэффективным методом поиска и обнаружения как гамма-, так и чистых альфа- бета-активных радионуклидов. Ее преимущества по сравнению с традиционными, например, физико-химическими (забор проб), либо стандартными радиометрическими (радиометры и γ-спектрометры) - следующие: дистанционность, возможность непрерывного площадного и профильного сканирования с одновременным определением широкого набора радиоактивных элементов и соединений, а также высокая чувствительность и скорость детектирования.

Как известно, спектры радионуклидов характеризуются частотными сдвигами, при этом каждая изотопическая структура отличается соответствующими массовыми числами и числом нейтронов. Например, изотопам стронция Sr86, Sr90 и Sr84 соответствуют частотные сдвиги относительно стабильного Sr88, равные 5.8•10-3 см-1, 11.4•10-3 см-1 и 12.4•10-3 см-1. Следовательно, идентификация дозообразущих нуклидов возможна лишь с помощью измерительных средств, обладающих высоким спектральным разрешением. Использование гипер/ультра-спектральной аппаратуры ($\lambda/\Delta\lambda>>100$) позволяет исключить перекрытие спектральных линий искомых радионуклидов при лазерном зондировании зараженных территорий и объектов и идентифицировать тот или иной изотоп. Перечисленные свойства были реализованы в разработанном бортовом лидаре с ультраспектральным разрешением ($\lambda/\Delta\lambda>1000$).

Отличительная особенность лидарной системы состоит в способности дистанционно обнаруживать источники радиационных утечек и выбросов в атмосферу, а также работать с большими зараженными территориями. Таким образом, достигается полная безопасность операторов при проведении радиационного контроля.

Гришканич А.С., Бузников А.А., Елизаров В.В., Жевлаков А.П., Кащеев С.В.
Россия, Санкт-Петербург, ОАО «НПК «Государственный оптический институт им С.И. Вавилова», Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

АЭРОПОИСК МЕСТОРОЖДЕНИЙ УГЛЕВОДОРОДОВ МЕТОДОМ ЛАЗЕРНОГО ЗОНДИРОВАНИЯ

Минеральные ресурсы, прежде всего углеводородные, представляют собой крупнейший реальный, хотя и труднодоступный, резерв для наращивания запасов и развития топливно-энергетического комплекса России и мирового сообщества в целом. Основным геофизическим методом поисков залежей нефти и газа была и остается сейсмическая разведка. Но достоверность прогноза только по материалам одного этого метода остается недостаточно высокой и в благоприятных условиях составляет, в лучшем случае, 30%. Особенно низка эффективность сейсморазведки при поисках неантиклинальных и сложно построенных ловушек, что характерно для районов Восточной Сибири. Поэтому на современном этапе развития нефтепоисковых работ необходим более широкий комплекс методов, имеющих различную физическую основу.

Применение аэрогеохимических и наземных геохимических съемок для поисков месторождений углеводородов базируется на установленном факте миграции из залежей нефти и газа углеводородных и других многокомпонентных флюидов (H2S, CO, CO2, H2, He), что приводит к изменению физических свойств пород над залежью и формированию ореолов метана, пропана и других углеводородов в приповерхностных отложениях и приземном слое атмосферы. В результате, по контуру залежи наблюдаются аномальные концентрации углеводородных газов.

В районе водонефтяного контакта и газонефтяного контакта наблюдаются аномальные, а над залежью повышенные концентрации тяжелых углеводородов.

Особо остро стоит задача повышения эффективности поисков нефти и газа в частности, в практике использования аэрогеофизических съемок. В настоящее время в России разработано достаточно большое количество дистанционных диагностических средств для задач эколого-метеорологического мониторинга, исследовательского, технического, бытового и специального назначения. Однако с учетом множества факторов, действующих на измерительную аппаратуру в реальных условиях, а также требований соответствующих нормативно-технических документов, большинство хорошо зарекомендовавших себя в лабораторных условиях авиационных геологоразведочных и поисковых комплексов оказывается непригодным для эксплуатации в реальных условиях. Для многих направлений дистанционного диагностирования, в частности, с использованием дистанционных оптических газоанализаторов (ДОГА), повышение чувствительности и точности детектирования углеводородных газов в приземных слоях атмосферы остается наиболее важным и проблемным.

Развитие и внедрение новых физических методов нелинейного увеличения чувствительности детектирования позволяет реализовать богатейшие и практически неисчерпаемые информационные возможности лазерного зондирования для создания высокоэффективной и конкурентоспособной технологии аэрогеохимического поиска нефтегазоносных месторождений.

Лазерное зондирование может служить высокоэффективным методом геологоразведочных работ на региональных и поисковых этапах для прогноза нефтегазоносности, оценки зон нефтегазонакопления и выявления локальных структур под глубокое бурение. Его преимущества по сравнению с традиционными (косвенными), например, физико-химическими, - следующие: дистанционность, бесконтакность, возможность непрерывного площадного и профильного сканирования с одновременным определением широкого набора химических элементов и соединений, а также высокая чувствительность и скорость детектирования (10-6 сек).

Автоматизированный бортовой лидар позволит устанавливать прогнозируемую мощность нефте- и газоносных пластов, содержание в них нефти и газа, качественные и количественные параметры углеводородного сырья. По данным аэрогеохимической съемки можно будет определять места бурения

нефтяных и газовых скважин, сложность условий бурения по вертикальному профилю, горно-геологической характеристики нефте- и газоносных пластов. Кроме того возможна оценка экологических и инженерных условий проектирования, строительства и эксплуатации скважин, прокладки трубопроводов и др. Тем самым значительно уменьшатся сроки проведения исследований объектов нефтяной и газовой промышленности, будут исключены загрязнения, сократятся расходы, связанные с разведочными работами.

Гришканич А.С., Лобанова Е.Г., Редька Д.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ЭКОЛОГИЧЕСКИЕ ОСОБЕННОСТИ СОЗДАНИЯ ЛАЗЕРНЫХ СИСТЕМ ДИСТАНЦИОННОГО ПИТАНИЯ ФОТОЭЛЕКТРИЧЕСКИХ ПРЕОБРАЗОВАТЕЛЕЙ

В последние годы особое внимание уделяется поиску, производству и использованию возобновляемых источников энергии, одним из которых являются преобразователи солнечной энергии в электричество. Помимо исследования возможностей повышения эффективности фотоэлектрических и термоэлектрических преобразователей солнечной энергии также в настоящее время активно развивается беспроводная передача энергии на открытых атмосферных трассах для подзарядки различных электронных устройств (например, беспилотных летательных аппаратов – БПЛА). Для решения этой задачи используется лазерное излучение, поскольку благодаря своей высокой направленности и интенсивности оно может обеспечить требуемую величину энергетического потока. Для работы в приповерхностном слое атмосферы целесообразно использовать источник излучения ближнего инфракрасного диапазона, попадающий в окна прозрачности атмосферы, например, с длиной волны 1,06 мкм. Также необходимо обеспечить обратное преобразование лазерного излучения в электрическую энергию с минимально-возможными потерями.

Целью данной работы является создание и исследование лазерной системы дистанционной подпитки электронных устройств, способной обеспечить необходимые эксплуатационные параметры, а также их стабильность, обеспечив при этом минимальный негативный эффект воздействия данных систем на окружающую среду.

Основные элементы такой системы – это источник лазерного излучения, система наведения, фотоэлектрический преобразователь и контроллер заряда, обеспечивающий требуемые электрические выходные параметры системы. Исследуемая нами система включает в себя лазерный источник на базе активной среды YAG:Nd с длиной волны 1,06 мкм и кремниевый фотодиод в качестве приемника излучения. Такой тип фотоприемника был выбран ввиду своей доступности и невысокой стоимости таких устройств. Кроме того, принималась в расчет и высокая чувствительность кремниевых фотодиодов на рабочей длине волны 1,06 мкм (не менее 0.1 А/Вт). Для других рабочих длин волн могут быть использованы другие материалы.

В ходе проведенных исследований разработанной системы дистанционной подпитки при выбранных параметрах (площади приемника, требуемых значениях тока и напряжения) были измерены и рассчитаны вольт-ваттная и ампер-ваттная характеристика фотопреобразователя, и его температурная стабильность. Кроме того, были рассчитаны оптимальная геометрическая структура приемника с учетом профиля распределения интенсивности по сечению пучка, расходимость лазерного излучения на различных расстояниях, а также распределение энергии по сечению пучка. Характер рассчитанных зависимостей хорошо согласуется с полученными экспериментальными данными. Для согласования площади приемной площадки и сечения пучка может понадобиться введение оптической системы, позволяющей управлять геометрическими размерами пучка.

С экологической точки зрения немаловажным моментом является безопасность использования подобных систем. Она может быть обеспечена: снижением уровней передаваемой мощности до минимальных, достаточных для обеспечения требуемых выходных характеристик либо установкой дополнительных систем мониторинга канала передачи энергии с автоматическим прерывателем передачи при появлении на пути следования луча различных объектов биологического происхождения.

Проведенные расчеты и измерения показали, что, хотя на данном этапе система лазерного дистанционного питания не удовлетворяет полностью заданным параметрам, дальнейшие работы, направленные на совершенствование системы, могут принести положительные результаты.

Захаров И.С., Величко А.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ ТЕМПЕРАТУРНЫХ ПОПУЛЯЦИОННЫХ РЕАКЦИЙ ИНФУЗОРИЙ КАК ИНФОРМАТИВНЫХ ПОКАЗАТЕЛЕЙ ВРЕДНЫХ ФАКТОРОВ В СРЕДЕ

В 1980-1990 гг. выделилась область приборостроения микробиотестирование, использующая организмы малых размеров в качестве первичного биохимического преобразователя интегрального химического состава и малые объемы проб. Данное направление динамично развивается за рубежом

(Wells,1998). В микробиотестировании широко используется реакция популяции одноклеточных организмов на внешнее воздействие. В области биотестирования широкое применение получили реакции хемотаксиса, геотаксиса и гальванотаксиса инфузорий. Одной из важнейших реакций живого является температурная регуляция в виде термотаксиса – перемещение инфузорий под действием градиента температуры.

В рамках конкурса грантов для студентов и аспирантов г. Санкт-Петербурга 2013 г. проводилось исследование актуальности применения термотаксиса в качестве экологической тест-реакции с учетом достижений современных зарубежных ученых-протозоологов и разработка концепции биотехнической системы для контроля информативных параметров температурно зависимой тест-реакции.

Термотаксис инфузорий как тест-реакция был предложен в работе (Захаров, Голядкин, 2008), но проведенный анализ источников конца XIX в. – начала XXI в. позволил выявить новые аспекты применения температурных эффектов у популяции инфузорий. В результате литературного обзора было выделено несколько этапов исследований температурных эффектов у популяции инфузорий:

Конец XIX в. – первая половина XX в. – обнаружение популяционных эффектов, зависящих от температур среды одноклеточных, исследование условий возникновения температурных эффектов, диапазона температурных оптимумов, разработка первых приборов для их поиска (Herter, 1923).

1970-1980-е гг. – разработка методов и технических средств для искусственного формирования температурных реакций (Tawada, 1972,1973).

1990-2000-е гг. исследование возможностей управления температурными тест-реакциями с помощью биохимическими и химических механизмов.

Современные зарубежные исследования температурных эффектов популяции инфузорий показали их зависимость от целого ряда вредных факторов водной среды. Простейшие, не обладая нервной системой, образуют плавающие структуры, способные находить зону температурного оптимума. Не имея температурных рецепторов, эти организмы способны реагировать на остро опасные воздействия, чтобы обеспечить выживание.

К ним относятся биоцидные вещества такие, как азид натрия (Gordon, 2005), инфекции, гипоксия, ингибиторы метаболизма азота (Malvin, 2003) морфины, такие, как налоксон (Karami, 2013). Данные вредные факторы изменяют диапазон температурного оптимума популяции инфузорий. Выявлено сходство между воздействием ряда биохимических соединений и химических веществ на температурные эффекты многоклеточных и одноклеточных организмов, что позволяет использовать их в качестве биотестовых моделей. Процессы терморегуляции популяции простейших могут выявлять нарушение этих процессов тепловым загрязнением, которые приводят к гипоксии. Существуют методы биологического контроля температурных загрязнений, обусловленных подогревом воды в ТЭС и АЭС, основанных на ферментативных реакциях, отражающих температурную резистивность. Температура является важным лимитирующим фактором. Повышение температуры воды оказывает воздействие на все звенья в водном биоценозе, изменяя его качественный и количественный состав.

Обзор источников показал, что, несмотря на большое количество лабораторных исследований, отсутствуют аппаратурные микробиотесты, которые были бы основаны на базе термоэффектов популяции одноклеточных организмов.

В рамках исследовательской работы на основе литературных данных и собственных исследований были выявлены биологические и технические факторы, влияющие на возникновение тест-реакции. В качестве наиболее важных факторов определены: возраст культуры, температура окружающей среды, вид температурного градиента, термодинамические аспекты его формирования .

Для экспериментальных исследований был создан макет установки с формированием одностороннего и двухстороннего градиента и цифровой регистрации реакции, а также программный пакет в среде MATLAB, позволившей зарегистрировать и выделить информативные параметры тест-реакции популяции инфузорий.

Новиков А.В., Летучий Ю.А., Тимощук А.С.
Россия, Санкт-Петербург, Военно-космическая академия имени А.Ф.Можайского

СХЕМА ФУНКЦИОНИРОВАНИЯ КОСМИЧЕСКОГО КОМПЛЕКСА ПРИ РЕШЕНИИ ИНФОРМАЦИОННЫХ ЗАДАЧ МОНИТОРИНГА ЭКОЛОГИЧЕСКОЙ ОБСТАНОВКИ В КОСМОСЕ И ИЗ КОСМОСА

Космический мониторинг обладает рядом важных преимуществ по сравнению с другими методами наблюдения и контроля загрязнений природной среды, обеспечивая высокий уровень обобщения данных о загрязнении окружающей среды, глобальный охват антропогенных эффектов, оперативность получения информации по экологической ситуации в различных областях земного шара. Космический мониторинг существенно дополняет наземные, самолетные и корабельные средства наблюдений и контроля природной среды и позволяет объединить данные о состоянии окружающей среды на основе информации, полученной из космоса.

Для повышения эффективности использования космического комплекса в задачах экологического мониторинга Земной поверхности и космического пространства, необходимо разработать схему его функционирования, которая бы позволяла при минимальных ресурсных затратах получать максимум информации о состоянии экологической обстановки в обследуемых районах Земли и вести учет космического мусора, находящегося на орбитах.

Общая схема использования космического комплекса включает в себя как составные элементы частные схемы использования по группам задач. Задачи, решаемые космическим комплексом, можно классифицировать по трем группам:

1. Основные.
2. Дополнительные.
3. Эпизодические.

Каждая группа задач имеет как общие, так и отличительные черты.

При решении указанных задач следует учитывать необходимость придерживаться (в полном объеме или частично) общей методической схемы проведения работ, включающей следующие этапы:

1. Анализ архивных материалов данных дистанционного зондирования земной поверхности и космического пространства.
2. Сбор обобщенной информации.
3. Первичная обработка материалов космической съемки и их предварительный анализ.
4. По результатам оперативного анализа полученных материалов уточняются наилучшие ситуационные условия для детального сбора информации (метеорологические, аппаратные, временные).
5. Проведение детальной съемки выбранных участков земной поверхности или космического пространства.
6. Первичная и вторичная обработка полученных материалов дистанционного наблюдения.
7. Углубленная комплексная тематическая обработка информации, полученной во всех спектральных диапазонах. Определение границ и пространственно-временных координат загрязнений, их характеристик. Составление цифровых карт областей изменения экологической обстановки.
8. Выявление динамики, прогнозирование и оценивание изменения экологической обстановки или траекторий перемещения космического мусора.
9. Представление структурной схемы функционирования разрабатываемого космического комплекса.

На борту космического аппарата происходит первичная обработка полученных изображений земной поверхности и космического пространства, накопление данных изображений, и передача их по радиоканалам в наземный центр обработки информации, где производится ее обработка, анализ и выработка прогноза изменения экологической обстановки.

Парфенов В.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ПРОБЛЕМЫ ТОЧНОСТИ ИЗМЕРЕНИЙ И СОЗДАНИЯ ЭЛЕКТРОННЫХ 3D-МОДЕЛЕЙ ПРИ МОНИТОРИНГЕ ЭКСТЕРЬЕРНЫХ СКУЛЬПТУРНЫХ ПАМЯТНИКОВ МЕТОДОМ ТРЕХМЕРНОГО ЛАЗЕРНОГО СКАНИРОВАНИЯ

В настоящее время в различных областях науки и техники все более широкое применение получает технология лазерного 3D-сканирования. Данная технология основана на принципах лазерной дальнометрии и будучи разновидностью методов лазерной локации, является составной частью новейших методов геоинформатики и цифровой фотограмметрии. Она находит применение при решении различных задач топографирования и картографирования местности, инженерного проектирования, строительства, земле- и лесоустройства, добычи полезных ископаемых и экологического мониторинга. В последние годы трехмерное лазерное сканирование стало активно применяться в области сохранения объектов культурно-исторического наследия, в том числе, для создания обмерных чертежей исторических зданий, электронных паспортов и физических копий памятников. Другое важное применение лазерного 3D-сканирования в данной сфере это мониторинг состояния сохранности экстерьерных памятников. Периодическое (например, 1 раз в 2-3 года) повторение работ по лазерному 3D-сканированию одного и того же памятника позволяет проводить контроль размеров имеющихся на его поверхности трещин и сколов, увеличения площади биообрастаний и гипсовых корок, очагов коррозии и т.д.

Вместе с тем, несмотря на активное внедрение технологии лазерного 3D-сканирования в сферу реставрации и искусства, сегодня остается открытым ряд актуальных вопросов, связанных с обеспечиваемой сканерами точностью измерений, а также степенью соответствия создаваемых 3D-моделей исходным объектам. Проведенные нами исследования показали, что для сканирования

скульптурных памятников необходимо использовать 3D-сканеры, обеспечивающие максимально-высокую точность измерений (по крайней мере, не хуже 0,05-0,1 мм) и разрешение (не хуже 200-300 мкм). Помимо правильного выбора типа используемого для измерений сканера (т.е. учета его точностных характеристик), в работах по лазерному сканированию необходимо использовать многофункциональное программное обеспечение, которое должно обеспечивать высокую точность совмещения отдельных сканов на этапе сборки 3D-модели и проведение необходимых количественных измерений при анализе состояния поверхности памятника.

Цыганкова И. А.,Заболотский В.П.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ПРОГРАММНЫЙ КОМПЛЕКС ПОДДЕРЖКИ ПРИНЯТИЯ ВРАЧЕБНЫХ РЕШЕНИЙ

Современный уровень развития общества характеризуется ростом требований к качеству жизни, поэтому оказание квалифицированной медицинской помощи становится все более и более дорогостоящим. Это резко обостряет проблему оптимизации затрат на лечение и профилактику заболеваний, как для отдельных пациентов, так и для медицинских структур различного уровня. Решение этой проблемы может быть получено только современными методами оптимизации и прогнозирования результатов лечения, учитывающими медико-биологические и социальные особенности пациентов.

Реализация этих методов невозможна без внедрения в повседневную врачебную практику современных информационных систем поддержки принятия решений. Системы поддержки принятия врачебных решений относятся к классу специализированных программных (компьютерных) систем, обладающих средствами ввода, хранения и анализа медико-биологических данных, и предназначены для оказания поддержки пользователю в принятии решений. Использование в работе врача таких систем позволяет повысить качество медицинских услуг, облегчить работу медицинского персонала, улучшить качество жизни пациентов, а также существенно сократить затраты на лечение и профилактику заболеваний.

В докладе рассматривается программный комплекс поддержки принятия врачебных решений для прогнозирования результатов лечения и выбора тактики лечебного процесса. При обработке медико-биологической информации используется разработанный авторами метод поиска внутренних связей в многомерных разнотипных плохо формализованных данных, который базируется на эволюционном подходе к решению экстремальных задач функции многих переменных.

Метод позволяет подобрать веса параметров биологических объектов, не снижая размерности признакового пространства, что, в свою очередь, позволяет исключить потерю значимой информации и учесть слабые связи в рассматриваемых информационных массивах.

Программный комплекс ориентирован на работу в среде ОС Window.

Комплекс состоит из базы данных, пакета программных модулей. Программные модули реализованы в среде объектно-ориентированного языка программирования C++Builder.Программный пакет включает в себя:

– модуль предобработки исходных данных;
– модуль обучения, обеспечивающий расчет весов входных параметров;
– модуль прогнозирования выходных параметров нового пациента по его известным входным характеристикам.

База данных представляет собой массивы медико-биологической информации о пациентах, методах и результатах лечения. Массивы данных хранятся в электронных таблицах формата Excel. Таблицы, с описанием входных и выходных характеристик пациентов, представляют собой данные типа «объект-свойство». Обмен данными между электронной таблицей и программными модулями осуществляется с помощью механизма автоматизации технологии OLE.

Пользовательский интерфейс комплекса разработан с учетом специфики лечения больных псориазом, и обеспечивает ввод исходных данных и представление результатов расчета в понятном и принятом в профессиональной среде пользователей виде.

Доступ к комплексу настраивается в соответствии с пользовательской ролью. Предусматривается защищенный иерархический доступ к информационным базам данных и программным модулям следующим категориям пользователей: врач, администратор, разработчик.

Предлагаемый программный комплекс позволяет:

– обеспечить поддержку в принятии врачебного решения о выборе тактики лечения;
– прогнозировать результаты лечения у новых пациентов;
– проводить анализ лечебного процесса с использованием базы данных.

Программный комплекс может быть достаточно быстро адаптирован для решения широкого круга задач, при условии, что рассматриваемые объекты представляют собой выборки большого объема, описываются в протоколах «вход-выход», и для них справедлива гипотеза о монотонности принятия решений в локальной области.

Шилин Б.В.
Россия, Санкт-Петербург, Санкт-Петербургский центр экологической безопасности РАН

ВИДЕОСПЕКТРАЛЬНЫЙ МЕТОД РЕГИСТРАЦИИ АНТРОПОГЕННОГО СТРЕССА РАСТИТЕЛЬНОСТИ

Хорошо известна методика исследования стресса растительности по изменениям спектральных характеристик с использованием спектрорадиометров. Однако эти приборы регистрируют спектральные характеристики «в точке», что резко ограничивает информационные возможности метода при изучении растительных ансамблей, в том числе и из-за временных изменений в процессе, например, полевых измерений. Видеоспектральная съёмка позволяет регистрировать спектральную информацию с авиакосмических носителей и в наземных условиях в виде информационного параллелепипеда, данные по вертикальной (горизонтальной при полевых измерениях) координате которого представляют спектр уходящего излучения объекта в пределах мгновенного поля зрения видеоспектрометра, а информация по горизонтальному «срезу» паралеллепипеда является монохромным узкоспектральным изображением конкретной фоноцелевой ситуации. При полевых исследованиях видеоспектрометр устанавливается на платформе на базе киноустановки, при вращении которой в горизонтальной плоскости формируется информационный параллелепипед конкретной сцены. В пределах сцены (газон в обрамлении кустарника) были организованы тест-площадки 1м$_x$1м с различным уровнем антропогенного загрязнения: на площадки выливались растворы и различной концентрации. Спектры фона и тест-объектов регистрировались на третий день после полива. На всех спектрах уверенно регистрируется стресс от каждого типа загрязнителей.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОЦИОКОМПЬЮТИНГЕ

Азаров А.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ФОРМАЛИЗАЦИЯ КОСПЛЕКСА «ИНФОРМАЦИОННАЯ СИСТЕМА — ПЕРСОНАЛ — КРИТИЧНЫЕ ДОКУМЕНТЫ» В ПРОБЛЕМЕ АНАЛИЗА ЗАЩИЩЕННОСТИ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ ОТ СОЦИО-ИНЖЕНЕРНЫХ АТАК

Доклад посвящен нескольким видам формализации моделей комплекса «информационная система – персонал – критичные документы». К рассмотрению представлены следующие виды формализаций: с помощью информационных моделей, с помощью реляционно-алгебраических моделей, представление комплекса в виде SQL-базы данных, представление комплекса с помощью вероятностных графических моделей. Рассмотрение представленных видов формализаций обусловлено следующими предпосылками. Рассмотрение информационных моделей позволяет формализовать рассматриваемую область и выделить основные сущности, играющие ключевую роль в процессе обеспечения безопасности пользователей информационных систем. Представление с помощью реляционно-алгебраических моделей с легкостью позволяет перейти к SQL-представлению комплекса «ИСПКД», что в дальнейшем позволяет использовать имеющиеся программные решения оптимизации запросов в таких базах данных, как, например, MySQL или Oracle. Наконец, представление комплекса «ИСПКД» в виде вероятностных графических моделей обусловлено перспективностью использования данных подходов в силу бурного развития этой области в настоящее время. Также представлены примеры имитации социо-инженерных атакующих действий злоумышленника на пользователей информационной системы к некоторым из представленным подходам.

Бродовская Е.В.
Россия, Москва, Московский государственный гуманитарный университет им. М.А. Шолохова

ОСОБЕННОСТИ ИССЛЕДОВАНИЯ ПОЛИТИЧЕСКОГО ПРОТЕСТА В РУНЕТЕ: КОГНИТИВНЫЕ КАРТЫ, МАТАФОРЫ, МЕМЫ

Российская гуманитарная наука переживает очередную волну актуализации интереса к исследованию теоретических и прикладных аспектов политического протеста. В отличие от предыдущих периодов развития данной темы, для которых свойственно внимание, прежде всего, к социальным факторам и движущим силам протеста, в настоящий период осуществляются попытки подобрать адекватные методики и технологии для измерения влияния коммуникативных факторов на протестную активность россиян. Решение данной проблемы предполагает исследование политического протеста в таком специфическом коммуникативном пространстве, как Интернет.

В российской социологии Интернета наблюдаются три основные тенденции. Первая тенденция воплощает стремление исследователей использовать традиционные, преимущественно количественные методы и инструменты прикладной социологии, применяемые для измерения и объяснения тех или иных процессов в реальной практике. Вторая тенденция заключается в попытке сочетать количественные и качественные методы эмпирических социологических исследований. И, наконец, поиск специальной, работающей только с объектами виртуального пространства, методики и техники исследования – характерен для третьей тенденции.

Для каждого из этих подходов свойственны те или иные методологические возможности и ограничения.

Применение традиционных социологических методов и процедур позволяет выявлять количественные параметры Интернет-активности, отслеживать динамику потребления Интернет-контента, описывать связи между различными сетевыми сообществами и т.д.. Вместе с тем, нерешенными остаются проблемы идентификации пользователей, обеспечения репрезентативности результатов исследования. Дискуссионным является вопрос относительно идентичности социальных процессов, протекающих в реальной и виртуальной средах.

Комбинирование количественных и качественных методов отчасти лимитирует недостатки подхода, рассмотренного выше, акцентируя внимание на исследовании оснований и форм дифференциации стратегий поведения в глобальной сети. Однако, в условиях слабой структурированности ролей и идентичностей пользователей Интернет, применение качественных методов нуждается в новых подходах к рекрутированию респондентов.

Позиция, согласно которой, поведение в Интернете как объект социологического исследования целесообразно изучать с помощью уникальных методик, не связанных с прямым запросом информации у респондента, претендует на преодоление недостатков сложившейся практики исследований в рамках социологии Интернет. Необходимо отметить, что, наблюдение за поведением в сети, как минимум, серьезно ограничено коммуникативным пространством, доступным для взгляда социолога (иными словами, мы можем наблюдать только то, что открыто демонстрирует пользователь). Помимо этого, решение проблемы обеспечения достаточного масштаба выборочной совокупности требует разработки и апробации системы автоматизированного сбора данных.

Одним из перспективных направлений исследования поведения в виртуальном пространстве является анализ ценностных репрезентаций пользователей и сетевых сообществ, выраженных в дискурсе протеста. Развитие данного направления может опираться на ряд апробированных методик.

Спецификой настоящего исследования является сочетание методов когнитивного картирования, интент-анализа метафор и мемов протеста. Выбор комбинации методов обусловлен следующими причинами. Во-первых, когнитивное картирование позволяет определить «набор ценностей» (список основных понятий) протестных сообществ. Во-вторых, анализ метафор позволяет уточнить модальность дискурса протеста. В-третьих, анализ мемов позволяет выявить устойчивые смыслы, отражающие ценностные основания протестных настроений в сети.

Верт Н.С., Маховенко Е.Б.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

ДОКАЗУЕМОЕ ХРАНЕНИЕ КОПИЙ ДАННЫХ НА ОБЛАЧНОМ СЕРВЕРЕ

Использование облачного хранилища данных является удобным, простым и экономичным способом хранения файлов, не требующим от владельцев данных поддержки и обслуживания собственной инфраструктуры по хранению данных. Безопасность при хранении является одним из основных вопросов в процессе работы с облачным сервером. Конфиденциальность данных может быть обеспечена путем шифрования информации. В настоящее время актуальной задачей является разработка схем контроля целостности данных, хранимых на недоверенном удаленном сервере.

Рассматриваются схемы доказуемого хранения нескольких копий данных на основе хэш-деревьев и на основе таблицы версий. Представлено доказательство безопасности криптографических протоколов, обеспечивающих контроль целостности файлов, хранимых на облачном сервере.

Модель облачного хранения данных состоит из трех основных сторон:

– владелец данных, помещаемых на хранение в облако;

– поставщик облачных услуг (CSP, от англ. cloud service provider), управляющий облачным сервером и предоставляющий оплачиваемое пространство для инфраструктуры хранения пользовательских файлов;

– авторизованные пользователи – множество клиентов владельца данных, которые имеют право на доступ к удаленным данным и знают закрытый ключ владельца данных, используя его для расшифрования файла.

Конфиденциальность данных, отправляемых на облачный сервер, обеспечивается шифрованием исходного файла. Создание уникальной копии данных – главная задача при проектировании схемы доказуемого хранения нескольких копий данных. В рассматриваемых схемах для генерации различимых копий предлагается использовать свойство рассеивания схем шифрования. В соответствии со свойством рассеивания зависимость выходных бит зашифрованного текста от входных битов исходного текста сложно выразить. Взаимодействие между авторизованными пользователями и CSP осуществляется по указанному методу создания уникальных копий. Авторизованный пользователь может расшифровать и получить доступ к копии файла, полученной от CSP. В рассматриваемых схемах для расшифрования копии файла авторизованные пользователи должны иметь только секретный ключ, полученный от владельца данных, нет необходимости определять индекс полученной копии.

Владелец данных разбивает исходный файл на блоки. Каждый блок шифруется отдельно. Помимо контроля числа копий данных, хранимых на облачном сервере, разбиение на блоки позволяет владельцу данных производить следующие действия над данными, помещенными на облачный сервер:

– изменение блока;

– добавление нового блока;

– удаление блока;

– параметрами схем хранения данных являются:

– F – файл данных, передаваемый серверу, состоит из m блоков F = {b1, b2, … bm};

– πkey() – псевдослучайная перестановка: key × {0, 1}log(m) → {0, 1}log(m). Размер ключа – 128 бит;

– ψkey() – псевдослучайная функция: key × {0, 1}log(m) → ℤp. Размер ключа – 128 бит;
– билинейное отображение/спаривание – основная составляющая рассматриваемой схемы.
– h – криптографическая хэш-функция;
– () – функция отображения битовой последовательности в точку эллиптической кривой: {0, 1}* → 1;
– EK – алгоритм шифрования, обладающий рассеивающим свойством, например AES.

Предложенные схемы включают в себя семь полиномиальных алгоритмов. Безопасность схем основана на сложности решения задач Диффи–Хеллмана и дискретного логарифмирования. При доказательстве того, что CS формирует верные ответы на запросы проверяющего только в том случае, если на сервере действительно хранятся все копии данных, они корректны и не изменены, использованы свойства билинейного отображения *ê.*

Долгоруков А.М.
Россия, Москва, Московский государственный университет им. М.В. Ломоносова,
Московский государственный гуманитарный университет им. М.А. Шолохова

МЕТОДЫ ИССЛЕДОВАНИЯ ON-LINE СЕТЕЙ В Е-ЭТНОМЕТОДОЛОГИЧЕСКОЙ ПЕРСПЕКТИВЕ

1. Для понимания и прогнозирования динамики сложных социальных систем любого уровня мы должны изучать и выдвигать правдоподобные гипотезы по трем основаниям: «человек», «культура», «структуры».

2. Человек в сети. В отношении категории «человек», новизна, видимо, состоит в появлении новых видов «приписанных и достигнутых статусов» в интернет-сообществах. В ofline-сообществах, к примеру, близкие отношения, устойчивая социальная иерархия и соответствующие паттерны поведения; наборы ценностей и культурных символов и т.д., все это приобретается преимущественно благодаря общности территории и социального времени – приписанный статус. Тогда как достигнутый статус – это скорее личные достижения, часто связанные с эмансипацией от приписанного статуса. Но что такое «территория» и «социальное время» в online-сообществах? Ответ предстоит найти. Это позволят определить понятия: «приписанный online-статус»; «достигнутый online-статус»; «online-проактивность»; «online-реактивность». Операционально определив эти и другие понятия можно содержательно описать новые типы «on-line-акторов» Их статусы (роли) в сети; степень и особенности влияния; источники власти; ценностные системы; паттерны; типичные значимые действия.

3. Сетевые структуры. Новое в структурно-функциональном «срезе» online-сообществ обнаруживается в ином качестве социального морфогенеза – «кристаллизации» новых (более гибких и видимо менее долговечных) структур.

Структуры (проявленные и латентные) - это не только результат взаимосвязей между «узлами»- отдельными акторами (индивидами и, к примеру, организациями), как это принято считать в устоявшейся теории сетей.

Более важными, вероятно, окажутся сложные (латентные) узлы, состоящие из «пар» и некоторых типов «троек» акторов и так называемых клик - плотно связанных скрытой от «большой» сети повесткой дня малых групп – террористов, силовиков, экономических игроков и т.п.. Они заполняют пространство между online-общностями (размер которых по разным оценкам колеблется от 50 до 600 человек), составляя специфический иерархический уровень в сетевой популяции. Можно обосновать предположение, что именно такие разновидности узлов уже в ближайшее десятилетие будут определять скрытую повестку дня в сети интернет.

4. Культура. Один из существенных признаков интернет-культуры, вызревающий у нас на глазах, позволяет говорить о номадическом культурном типе. Люди опять становятся кочевниками (мобильные идентичности; случайные связи в сети; прозрачные границы сообществ; ролевая вседозволенность; эксперименты по конструированию и деконструкции себя и т.д.) – все это создание нового мира, а не описание старого с помощью средств Интернета.

Реальные социальные трансформации в ближайшее время можно ожидать не от Интернета, но от мобильного Интернета.

Как исследовать «человека», «структуры» и «культуру», порождающие динамику online-сетей? Ответ, на мой взгляд, лежит в е-этнометодологической перспективе.

Укажем некоторые важные черты этнометодологии».

Этнометодология – буквально «методы людей». Она изучает повседневные знания людей, которые они называют «здравым смыслом».

Основные установки этнометодологов можно сформулировать так.

Социальная реальность это эндогенно порождаемое практическое дело, осуществляемое «здесь и сейчас».

Это в основном действия относительно рутинные и не обдуманные.

Повседневные разговоры составляют естественный фундамент для других форм межличностных отношений, выливающихся в действия.

Сложные взаимосвязи можно обнаружить, вызывая к жизни «объяснения», работая с ними в рефлексивной позиции люди, тем самым, понимают и иногда изменяют свою жизнь, делая избыточными «рекомендации» и внешние предписания.

Ключом для обнаружения и понимания «структур», «культуры» и «ценностей, а также действий человека» должны выступать оценки самих участников жизненных ситуаций.

Задача этнометодолога анализировать как сами «объяснения», так и реакцию других участников ситуации на эти объяснения.

К выше сказанному надо добавить следующее:

Данные и средства их сбора в интернет уже есть. Поэтому, надо больше наблюдать то, что есть, нежели собирать новые данные.

Очень важной становится способность генерировать новые данные, приписывая «свежий» смысл тому, что спонтанно порождает сеть.

Завируха В. К., Байгутлина И.А., Замятин А.Ю., Цыпанов С.А.
Россия, Санкт-Петербург, Арктический и антарктический научно-исследовательский институт,
Болгария, Несебр, ООД «Синергия Инвест»

ИСКАЖЕНИЕ ИСТОРИИ РОССИИ В РЕЗУЛЬТАТЕ ИНФОРМАЦИОННОЙ ВОЙНЫ

Широкое проникновение доступа к Интернет и развитие различных информационных сервисов создало нашим традиционным противникам беспрецедентные возможности для массированных акций по искажению истории России в рамках информационной войны.

К сожалению, в настоящий момент практически все наиболее популярные информационные сервисы и системы управления их содержимым находятся на территории и под юрисдикцией враждебных государств. Значительную опасность представляют также новые и перспективные зарубежные разработки в области больших данных (BigData). Прежде всего, это можно отнести к технологической новинке IBM – суперкомпьютеру Watson, с помощью которого может в широких пределах осуществляться трансформация ранее существовавших представлений в любой области знаний. И, в том числе, в области истории и культуры государств и народов.

Одним из активно атакуемых в последнее время направлений является история Великой Отечественной войны 1941–1945 годов, а также роль и заслуги РККА и СССР в разгроме гитлеровской Германии и её многочисленных союзников. За рубежом всё больше в свободное обращение поступают очевидно нацистские издания, описывающие события того времени в извращённом виде (зачастую, с героизацией Вермахта и СС). На прилавках книжных магазинов России появляется огромное количество переводной литературы, написанной теми, кто находился на стороне нацистской Германии. Интернет наполнен (в том числе, через «Википедию») огромным количеством недостоверной информации с перекрёстными ссылками. Недалеко ушел и отечественный кинематограф (здесь невозможно не упомянуть в крайне негативном смысле фильм «Белый тигр», снятый на госбюджетные деньги).

Авторами совместно с поисковым отрядом «Наследники» (при общеобразовательной средней школе №1968 ЮВАО Москвы) детально исследован вопрос проведения силами 55-й Армии Ленинградского фронта второй фазы наступательной операции на Красноборском направлении, которая началась 19 марта 1943 года. По материалам германских архивов было определено количество боеприпасов, выпущенных противником для отражения наступления 55-й Армии в полосе нескольких километров. В переводе на вес это составило 754 тонны или 38 вагонов боеприпасов. В процентном отношении это соответствовало 15% от среднесуточного количество боеприпасов, израсходованных немцами в марте 1943 года на всём Восточном фронте. Примерно такой же расход боеприпасов у Красного Бора наблюдался 20 и 21 марта. Также следует отметить, что у Красного Бора на стороне Германии воевало значительное число европейских наёмников: испанцы, голландцы, бельгийцы, норвежцы, латыши и эстонцы (в том числе, в отдельных укомплектованных по национальной принадлежности легионах СС).

В существующих на настоящий момент публикациях Красноборская операция рассматривается крайне однобоко; на основании ограниченного количества данных делается заключение о слабости подготовки и бездарности проведения наступления 55-й Армии Ленинградского фронта. Однако, колоссальный расход боеприпасов немцев говорит в этом случае сам за себя.

Ранее подобная работа была выполнена применительно к наступательной операции группы полковника Андреева (52-я Армия Волховского фронта) у населённых пунктов Крутик и Копцы Новгородского района Ленинградской области 2 апреля 1942 года. Результат исследования, как и в случае с Красноборской операцией, дал результаты, диаметрально противоположные тем, которые излагаются в современной печати.

Говоря об историко-культурном наследии России, следует отметить, что сегодня очень остро стоит вопрос создания российских национальных электронных банков знаний, которые могли бы обеспечить целостность и непротиворечивость хранящейся в них информации. Применительно же к зарубежным информационным системам (например, IBM Watson) уже сегодня необходимо

разрабатывать стратегические программы, направленные на обеспечение контроля загружаемого содержимого и его использования (в том числе, в различных образовательных целях). Вероятно, на законодательном уровне необходим запрет использования определённых очевидно «враждебных» ресурсов в любых образовательных целях. От проведения этих мероприятий в значительной степени будет зависеть то, в какой информационной среде будут жить последующие поколения россиян.

Корт С.С., Евдокимов Д.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

ДИНАМИЧЕСКАЯ БИНАРНАЯ ИНСТРУМЕНТАЦИЯ. ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ

В докладе рассматриваются программные средства, работающие во время выполнения исследуемой программы, основанные на инструментации.

Инструментацией называют процесс модификации исследуемой программы путем вставки в нее дополнительного кода, выполняемого с целью анализа поведения модифицируемой программы. За вставку дополнительного кода обычно отвечают инструментирующие процедуры, которые и модифицируют целевую программу. Инструментация бинарного приложения может быть выполнена на разных уровнях гранулярности представления программы, в том числе на уровне инструкции, базового блока, процедуры, секции бинарного файла, бинарного образа.

Добавленный код обычно представляет собой анализирующие процедуры. Эти процедуры отвечает за проведение необходимого анализа, модификации и мониторинга исследуемой (целевой) программы и вызываются каждый раз при достижении определенного участка кода. Анализирующие процедуры обычно реализованы в виде процедур обратного вызова, которые вызываются при достижении определенного участка кода, или когда происходит определенное событие в программе.

Такой подход может использоваться для решения целого ряда задач по анализу программного обеспечения, включая эмуляцию, анализ производительности, автоматической отладки и т.д. Можно отметить, что функциональные возможности, предоставляемые инструментированием программ, хорошо подходят и для решения различных задач информационной безопасности.

Динамическая бинарная инструментация (DBI, Dynamic Binary Instrumentation), рассматриваемая в настоящей статье, выполняется во время работы программы и состоит из нескольких базовых процедур: получение управления от приложения, сохранение состояния программы, выполнение задач, восстановление состояние программы, возвращение управления приложению. Получение анализирующей процедурой управления от приложения обычно происходит с помощью технологии сплайсинга, реализующего перезапись текущих инструкций, с их сохранением в определенном месте, на инструкцию передачи управления (jmp) и функциональный фрагмент кода.

На сегодняшний день существует два основных пути работы DBI для представления кода и его инструментации:

– Disassemble-and-resynthesise (D&R): машинный код конвертируется в промежуточное представление. Это промежуточное представление инструментируется (за счет добавления новых инструкций), и затем обратно конвертируется в машинный код;

– Copy-and-annotate (C&A): входящие инструкции в точности копируются, за исключением тех, что связанны с потоком управления. Каждая инструкции аннотируется с описанием ее воздействия, через структуры данных или instruction-querying API. Инструменты используют аннотацию для выполнения своей инструментации. Добавленный код анализа чередуется с исходным кодом без какого влияния на него.

В докладе рассмотрено применение библиотеки PIN (которая представляет собой бесплатную разработку компании Intel, поставляющуюся с частично открытыми исходными текстами в виде SDK) для решения таких задач, как оценка покрытия кода при динамическом анализе, мониторинг исключений обнаружение уязвимостей переполнения буфера в стеке.

Приведенные примеры показывают достоинства использования динамической бинарной инструментации для исследования безопасности программного обеспечения, основанные на контроле выполнения программы на уровне ассемблера.

Лаврова Д.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

ПАРАЛЛЕЛЬНАЯ ОБРАБОТКА СЕТЕВОГО ТРАФИКА ДЛЯ АНАЛИЗА БЕЗОПАСНОСТИ ПЕРЕДАВАЕМЫХ ОБЪЕКТОВ

Для поддержания безопасности информации при работе в сети Интернет для государственных и коммерческих целей необходимо наличие систем эффективного анализа и обработки сетевого трафика. Вследствие низких скоростей обработки сетевого трафика понижается вероятность обнаружения несанкционированной активности в трафике, что критично для безопасности информации и также может привести к повышению расходов на обслуживание и обеспечение сетевой

инфраструктуры. Недостаток вычислительной мощности не позволяет производить глубокий анализ безопасности сетевого трафика, что в свою очередь повышает риск пропуска несанкционированной активности.

Для эффективного решения задачи проведения анализа безопасности больших объемов сетевого трафика следует проводить анализ на многопроцессорном кластере.

Исследование особенностей функционирования современных средств и систем обработки сетевого трафика показало, что для проведения эффективного анализа безопасности больших объемов сетевого трафика следует делать это на многопроцессорном кластере. Использование высокопроизводительных кластерных платформ для процессинга сетевого трафика позволяет распределять задачи между несколькими компонентами кластера. Это дает возможность параллельно осуществлять анализ сетевого трафика и обеспечивать безопасность передаваемой информации, сохраняя при этом высокую пропускную способность.

Идея эффективной параллельной обработки больших объемов сетевого трафика на предмет безопасности заключается в сокращении дублирующихся действий по обработке трафика как маршрутизирующим и коммутационным оборудованием, так и средствами сетевой безопасности, достигающемся за счет выделения компонента анализа сетевого трафика в отдельную подсистему.

Предлагается архитектура системы параллельной обработки сетевого трафика для анализа безопасности, включающая в себя:

а) балансировщик нагрузки;

б) анализаторы сетевого трафика, функционирующие на узлах вычислительного кластера;

в) компонент принятия решений;

г) выходной фильтр;

д) интеграторы системы со средствами сетевой безопасности;

е) средства сетевой безопасности, интегрированные с системой.

Каждое средство сетевой безопасности формирует список задач для представленной системы. С учетом параллельности архитектуры данной системы, очевидно, что каждый анализатор может выполнять задачи, полученные от каждого из средств. Таким образом, схема взаимодействия системы со средствами безопасности может быть представлена как связь вида «многие ко многим». Взаимодействие происходит через базу данных, в которую каждое средство записывает задачи для системы. Сетевой трафик поступает в систему на балансировщик нагрузки, балансировщик выделяет сетевой трафик каждому узлу кластера, и далее трафик, приходящий на узел, поступает на анализатор. Каждый анализатор обращается к базе данных и «забирает» оттуда задачи, оставляя запись в таблице базы данных. Далее, в соответствии с задачей, анализатор выполняет действия по обработке трафика. При успешном завершении задачи, анализатор обращается к базе данных, записывая результаты по выполнению данной задачи. Каждое средство сетевой безопасности имеет свой интегратор, который обеспечивает связь с базой данных и выполняет функцию датчика, принимающего сигналы о готовности выполнения задачи и записи результатов ее решения в базу данных. После того, как задача выполнена анализатором, интегратор получает сигнал о выполнении, забирает результаты решения задачи из базы данных и запускает своё средство сетевой безопасности. Далее средства сетевой безопасности проводят параллельный анализ безопасности, используя результаты работы анализаторов, и собирают все результаты вместе. Компонент принятия решений обрабатывает результаты анализа безопасности и выносит вердикт о безопасности/небезопасности сетевого трафика и сообщает о своем решении выходному фильтру, который либо блокирует трафик, либо пропускает.

Параллельная обработка сетевого трафика с выделением компонента анализа позволит существенно повысить скорость обработки сетевого трафика на предмет безопасности, сократить дублирующиеся действия по обработке трафика, обеспечить одновременное использование нескольких средств сетевой безопасности, как одного, так и различных типов, а также снизить расходы на обеспечение сетевой инфраструктуры.

Маховенко Е.Б., Кольцова Е.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

ПРАКТИКУМ ПО АНАЛИЗУ ДАННЫХ И ЕСТЕСТВЕННО-ЯЗЫКОВЫХ ТЕКСТОВ

Методы анализа данных и естественно-языковых текстов, применительно к сфере информационной безопасности, позволяют устанавливать авторство, бороться со спамом, разрабатывать поисковые системы, системы защиты от флуда и захвата аккаунтов, классифицировать данные сетевого взаимодействия.

Обработку естественно-языковых текстов можно разделить на два основных этапа.

1. Первичная обработка (уровень сообщения), под которой подразумевается выявление ключевых элементов сообщения и выполнение следующих задач:

- поиск в тексте сообщения известных объектов;
- поиск в тексте возможных ошибок и опечаток;

– поиск в тексте новых объектов.

Первая задача решается методами морфологического и частотного анализа. Для поиска ошибок и опечаток применяется нечеткое сравнение строк. Последняя задача решается с использованием регулярных выражений.

2. В состав вторичной обработки (уровень почтового ящика) входят:

– классификация сообщений;

– кластеризация сообщений.

В обоих случаях собственно сообщение заменяется результатом его первичной обработки, т.е. списком найденных в нем объектов.

Анализ данных включает в себя анализ сетевых пакетов, данных, хранящихся на жестком диске, флэш-накопителе или любых других накопителях информации, анализ программного кода, анализ и разработку средств защиты от спама и флуда.

Для изучения таких методов в рамках дисциплины «Методы анализа данных и естественно-языковых текстов» предлагается цикл из восьми лабораторных работ, включающих изучение методов первичной и вторичной обработки естественно-языковых текстов и анализа данных.

Первые четыре работы направлены на изучение методов первичной и вторичной обработки текста. В первой работе необходимо с помощью алгоритма шинглов определить степень похожести текстов. Алгоритм используется поисковыми системами для борьбы со спамом и позволяет исключать из поисковой выдачи тексты, похожие друг на друга или полностью идентичные. Во второй работе необходимо научиться определять авторство текста на основе частотного анализа данных. В третьей работе рассматриваются возможности метода латентно-семантического анализа по решению задач кластеризации. Необходимо научиться находить тексты одной тематики, определять, есть ли взаимосвязь между документами и терминами, в них встречающимися. Результатом работы является разделение заголовков статей по тематике. Четвертая работа предполагает изучение возможности нейронных сетей по решению задач классификации. В результате работы с помощью программы Neural Analyzer необходимо обучить нейронную сеть так, чтобы она по частоте встречаемости букв в тексте (также можно использовать другие характеристики текста, например частоту встречаемости слов, заглавных и прописных букв, количество знаков препинания и т.д.) могла определить, к какому языковому жанру данный текст относится.

В следующих четырех работах рассмотрены основные методы и алгоритмы анализа данных. В пятой работе необходимо научиться распознавать CAPTCHA с помощью преобразования Хафа и нейронных сетей. Результатом работы является распознанные цифровые значения. Шестая работа предполагает изучение основных способов восстановления данных и алгоритмов надежного удаления данных без возможности их восстановления. Седьмая работа предполагает изучение основных методов обфускации программного кода. В результате работы необходимо получить деобфусцированный код и определить, какие функции он выполняет. В последней работе рассматриваются методы классификации данных с помощью системы анализа данных Weka и ее графического интерфейса Explorer: наивный байесовский метод, метод C 4.5, метод Random forest.

Нечаев В.Д.
Россия, Москва, Московский государственный гуманитарный университет им. М.А. Шолохова

ГРАНИЦЫ СВОБОДЫ И БЕЗОПАСНОСТИ В ПРОСТРАНСТВЕ ИНТЕРНЕТ В ОЦЕНКАХ РОССИЙСКИХ ПОЛЬЗОВАТЕЛЕЙ (ПО РЕЗУЛЬТАТАМ ИССЛЕДОВАНИЯ WORLD INTERNET PROJECT IN RUSSIA - 2012)

На сегодняшний день Мировой Интернет-Проект (World Internet Project или сокращенно WIP) - это основная международная площадка, объединяющая исследователей со всех континентов. Старт проекта был осуществлен еще в 1999 году в Центре политических коммуникаций Лос-Анджелеса, США (в настоящее время – Центр цифрового будущего). Основатели WIP исходили из того, что растущее влияние цифровых технологий и интернета является кросс-национальным феноменом, трансформирующим социальную, политическую, экономическую жизнь индивидов, сообществ, наций и глобального мира в целом. Была поставлена амбициозная задача – ежегодно наблюдать, фиксировать и анализировать изменения, которые связаны с расширением интернет-коммуникации в различных точках глобального пространства. Очевидно, что решить такую масштабную задачу силами одного научного центра было бы невозможно, и на протяжении последних 12 лет представители более 30 стран (среди них Канада, Китай, Япония, Великобритания, Германия, Италия и т.д.) включились в совместную работу. 2012 год стал рекордным по количеству привлеченных в WIP партнеров (их число достигло 37) и знаковым для российского научного сообщества, так как исследователи из РФ, впервые за всю историю существования проекта, приняли в нем участие.

Базой проведения исследования WIP-2012 в России стал Институт гуманитарных технологий в сфере социального компьютинга (Institute for High-Hume Technologies in Social Computing) Московского государственного гуманитарного университета им. М. А. Шолохова.

В ходе исследования мы измерили три группы переменных, отражающих восприятие личной безопасности пользователями Интернета:

– ощущение комфорта и безопасности/дискомфорта и незащищенности от открытости политического сегмента пространства Интернет;

– представления о необходимости наличия/отсутствия границ при реализации свободы слова в пространстве Интернет;

– отношение к контролю над действиями пользователей Интернет со стороны властей, Интернет-корпораций, поисковых систем и др.

В результате анализа группы переменных, отражающих особенности восприятия россиянами границ свободы и безопасности в пространстве Интернет, мы пришли к следующим выводам.

Во-первых, глобальная сеть воспринимается россиянами, прежде всего, как пространство свободы, в связи с чем, в качестве нормы рассматриваются такие его параметры и функции, как «открытость для выражения позиций», «неограниченная критика властей и политиков». Данное понимание основывается на ощущениях комфорта и безопасности и обладает большим консолидационным потенциалом, интегрирующим представителей разных возрастных групп.

Во-вторых, в ходе исследования основных индикаторов группы переменных, отражающих представления россиян о необходимости наличия/отсутствия границ при реализации свободы слова в пространстве Интернет, мы зафиксировали «эффект абсолютизации свободы слова», свойственный для респондентов, ориентированных на «политические функции» глобальной сети. Это обстоятельство позволяет нам предположить, что критика власти (включая ее радикальные формы) является одной из доминирующих форм реализации политической субъектности россиян в Интернете.

В-третьих, изучение данных об отношении россиян к контролю над действиями пользователей Интернет со стороны властей, Интернет-корпораций, поисковых систем, позволило выявить противоречие в позициях респондентов, которые, с одной стороны, абсолютизируют свободу слова, а, с другой стороны, считают необходимым усилить контроль над глобальной сетью со стороны властей. Результаты исследования демонстрируют зависимость обозначенных позиций от оценки достоверности информации, представленной в Интернете. Запрос на усиление контроля со стороны властных структур коррелирует с низким уровнем доверия к достоверности контента в глобальной сети.

Торопова А.В., Фроленков К.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ЗАДАЧА МОДЕЛИРОВАНИЯ РАСПРОСТРАНЕНИЯ МНЕНИЙ НА ОСНОВЕ КОМПЛЕКСНОГО АНАЛИЗА ЭЛЕКТРОННЫХ СОЦИАЛЬНЫХ СЕТЕЙ

Постоянно увеличивающийся темп развития телекоммуникационных технологий на данный момент приводит к ситуации, при которой о каждом агенте исследуемой социальной среды в открытом доступе находятся огромные количества информации. К такой информации, однако, не могут быть применены стандартные методы исследования, так как часто она не может быть приведена к числовому формату.

В связи с этим были предприняты попытки анализа отдельных электронных социальных сетей с целью выявить тенденции распространения мнений как с учетом только связей (т.е. анализ графовой/гиперграфовой структуры), так и на основе анализа текстов. Последняя категория представлена исследованиями моделей сетевых игр и имитационных вероятностных моделей.

Существенным недостатком этих подходов является необходимость выбора графовой структуры социальной сети, которая в реальной ситуации не является наблюдаемой, так как один и тот же агент может и зачастую участвует во множестве социальных сетей, представленных в интернете; при этом каждая из таких сетей может являться одним из узлов сети более высокого порядка, образованной ссылками. Основной по мнению авторов задачей на данный момент является синтез общего графа социального взаимодействия, составленного с использованием знаний, извлеченных из множественных источников. Для этого могут быть применены существующие на данный момент модели синтеза графовых структур с заданными параметрами, такие как exponential random graphs.

Такое моделирование поможет при определении того, каким образом может распространяться информация того или иного вида, что в свою очередь будет очень полезно при исследованиях по информационной безопасности.

Тулупьев А.Л., Абрамов М.В., Азаров А.А., Тулупьева Т.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ЗАЩИТА КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ НА ИНТЕРНЕТ-ПОРТАЛЕ РЕДАКЦИИ ЭЛЕКТРОННОГО НАУЧНОГО ЖУРНАЛА

М.В. Абрамов как активно использует на портале современные, наиболее эффективные технологии защиты информации, так и вносит вклад в развитие новых систем информационной безопасности в сфере веб-программирования. Необходимость столь пристального внимания к вопросам безопасности конфиденциальных данных обусловлена развитием программного комплекса,

расширением аудитории его пользователей, ростом интереса к проекту. Благодаря заблаговременному анализу предметной области уже до начала работы программистов было понятно, что безопасности данных будет уделено особое внимание на всех этапах разработки. Пренебрежение этой деятельностью может вести к очень серьёзным последствиям. Здесь этого удалось избежать, вопрос защиты конфиденциальных данных проработан блестяще и предусматривает несколько уровней. Первый уровень – это работа с пользователями, информирование их о нежелательных действиях, которые могут привести к утери информации, второй уровень – это отслеживание нетипичных действий пользователей и блокировка таких пользователей в случае необходимости и, наконец, третий уровень – это непосредственная защита базы данных от прямой SQL-инъекции. Благодаря тщательной проработке каждого уровня система по праву может считаться максимально защищённой от атак злоумышленников.

Тулупьев А.Л., Тулупьева Т.В., Азаров А.А., Фильченков А.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
АЛГОРИТМЫ АНАЛИЗА ЗАЩИЩЕННОСТИ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ ОТ СОЦИО-ИНЖЕНЕРНЫХ АТАК

Представляемый доклад посвящен рассмотрению алгоритмов имитации распространения социо-инженерных атак злоумышленника на графе социальных связей пользователей информационных систем и алгоритма имитации социо-инженерной атаки, зависящей от степени выраженности уязвимостей пользователя. Первый набор алгоритмов построен на основании реляционно-алгебраического подхода, также разработанного коллективом авторов. Представленные алгоритмы имеют различную вычислительную сложности, что существенно влияет на скорость работы комплекса программ при анализе больших информационных систем со множеством связей. Второй алгоритм это модификация и адаптация алгоритма деревьев атак, применяемого для автоматизированного анализа защищенности программно-технических компонент информационной системы. Представлено несколько вариантов такого алгоритма. Основным отличием данных алгоритмов является использование профиля уязвимостей пользователя при моделировании дерева социо-инженерных атак на пользователей информационной системы.

Тулупьев А.Л., Тулупьева Т.В., Михайлов Н.Ю., Азаров А.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
РАЗГРАНИЧЕНИЕ ДОСТУПА К ИНФОРМАЦИОННЫМ РЕСУРСАМ С ЦЕЛЬЮ ЗАЩИТЫ КРИТИЧНЫХ ДОКУМЕНТОВ ПОЛЬЗОВАТЕЛЕЙ ОТ СОЦИО-ИНЖЕНЕРНЫХ АТАК

Доклад посвящён информационной безопасности, а именно разграничению доступа пользователей к информационным ресурсам компании с целью защиты критичных документов от социо-инженерных атак. Приведены психологические теории относительно природы социо-инженерных атак, типы атак, а также теория об избыточности прав пользователей при работе с информационными ресурсами и методы выделения групп пользователей по правам доступа в соответствии с возложенными на них задачами и с учётом структуры связей между ними.

Фильченков А.А., Суворова А.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
РАЗЛИЧИЕ В ГРАФАХ РАСПРОСТРАНЕНИЯ ВИРУСОВ И ВИРУСНЫХ МАТЕРИАЛОВ В СОЦИАЛЬНЫХ СЕТЯХ

Некогда казавшаяся незначительной проблема распространения вирусов в социальных сетях за последние 5–8 лет стала одной из наиболее острых в вопросах борьбы с компьютерными вирусами. В 2005 году компьютеры более миллиона пользователей MySpace были заражены вирусом Samy. К 2008 году число появляющихся вирусов стало исчисляться десятками, а их среда обитания стала включать в себя все крупные социальные сети. В нее вошли и русскоязычные социальные сети: вирус Rovud заразил более десяти миллионов пользователей сети ВКонтакте, Несколько позже этот вирус затронул также сеть Одноклассники.

Модели распространения компьютерных вирусов в социальной сети аналогична модель распространения вирусного контента (из-за чего и было получено такое название) — различного рода видео, картинок или ссылок, — обобщая, контента, который передаются между пользователями, причем побудительным мотивом передачи служит именно содержание контента (юмор, эстетическое, скандальное, познавательное, шокирующее и т.д.). Сами вирусы также распространяют себя под видом вирусного материала — жертва получает сообщение от одного из своих контактов с контентом, содержащим вредоносное ПО. Затем этот же контент рассылается по контактам зараженной жертвы, продолжая распространение вируса.

Таким образом, отличить вирусный материал от вируса достаточно сложно, поскольку модели их распространения похожи. Различие можно обнаружить в графах распространения. В простейшем случае вирус рассылает контент по всем контактам жертвы, тогда как множество адресатов вирусного

материала зачастую является собственным подмножеством множества контактов, к тому же обычно значительно меньше последнего. Другим отличием является то, что даже если вирус, мимикрируя под вирусный материал, рассылает свои репликации лишь по части контактов, среди них могут оказаться неперсонализированные страницы/профили — т.е. страницы/профили, ведущиеся от лица какой-либо организации (примерами могут служить профиль Аэрофлот, профиль группы Любэ, профиль кинопоказов в кинотеатре Родина и т.д.). Таким контактам вирусные материалы не отправляют.

Анализ профилей пользователей социальных сетей позволит выявить маркеры, которые являются критичными при распространении именно вирусов. В частности, это позволит выявлять вершины, которые при распространении вирусного материала являются тупиками, т.е. не передают материал дальше. Соответственно, если в графе распространения такие вершины имеют исходящие ребра, это является свидетельством в пользу того, что граф отражает распространение именно вируса. Также выявление внимательных пользователей, которые менее подвержены вероятности заразиться, позволит в случае, если такой пользователь распространил контент, сделать вывод в пользу того, что этот контент не содержит вирус. Важно также отметить, что описанный подход носит вероятностный характер и требует построения соответствующей вероятностной модели классификации.

Чиркин Е.С.
Россия, Тамбов, Тамбовский государственный университет им. Г.Р. Державина

ОПАСНОСТЬ ИСПОЛЬЗОВАНИЯ ОРИГИНАЛЬНЫХ ФАЙЛОВ В СИСТЕМАХ АВТОМАТИЗИРОВАННОЙ ПРОВЕРКИ НА ПЛАГИАТ

К настоящему времени в мире идёт усиление борьбы с неправомерным использованием чужой интеллектуальной собственности. Проникновение широкополосного интернета, удешевление доступа к нему, рост количества сервисов и услуг, которые можно получить удалённо, доступность систем электронной коммерции стимулируют нарушения в области авторского права.

Под плагиатом подразумевают умышленное присвоение авторства чужой работы или её части. Правовое поле ответственности за плагиат регулируется авторским и смежными правами.

Немалое внимание привлекает плагиат в работах чиновников, учёных, работников высшей школы, других лиц. Согласно мнению подавляющего большинства (согласно опросам, например, см. опрос «Левада-Центра» от августа 2013 г.), плагиаторы должны немедленно лишаться своих должностей и званий.

До недавнего времени борьба с плагиатом в научных работах носила эпизодический характер, общественный резонанс получали лишь самые громкие случаи. Связано это, отчасти, с дороговизной проведения лингвистической экспертизы и несовершенством нормативной базы. К настоящему времени существуют и, не смотря на все их недостатки, функционируют системы автоматизированной проверки на плагиат, которые способны в корне изменить ситуацию по борьбе с плагиатом в сфере образования и науки – они упрощают начало процедуры лингвистической экспертизы и вынуждают совершенствовать связанные юридические процедуры.

Согласно утверждённой Министерством образования и науки «Стратегия развития системы подготовки рабочих кадров и формирования прикладных квалификаций в Российской Федерации на период до 2020 года» ожидается:

1) создание базы экземпляров всех работ: квалификационных работ обучающихся, кадров высшей квалификации и современных учебников, её интеграция с ЕИС ВАК (за 2013 г.);

2) обеспечение доступа частных производителей программного обеспечения к базе контрольных экземпляров работ и их текстам, предоставление образовательным и научным учреждениям доступа к системам контроля заимствований на любых приемлемых, в том числе коммерческих условиях, при этом право выбора соответствующих информационных систем должно остаться исключительно за самим учреждением (за 2014 г.);

3) уточнение правового определения термина «недобросовестное заимствование» (плагиат) в контексте проверки квалификационных работ; создание организационно-методической базы для построения системы антиплагиата в научных и образовательных учреждениях; разработка методик установления фактов неправомочного заимствования, регламентов процедур рассмотрения спорных вопросов неправомочного заимствования, системы моральных и административных санкций (к 2014 г.);

4) изменение требований к промежуточной и итоговой аттестации в образовательных учреждениях; изменение процедуры регламентированного контроля качества образования в части обязательных требований к использованию систем контроля заимствований (к 2016 г.).

С появлением централизованных баз с контрольными, курсовыми, дипломными, диссертациями существует следующая опасность автоматизированной проверки работ на наличие плагиата. Дело в том, что работы, логично предположить, должны храниться в их оригинальном виде – в том виде, в котором они создавались. Вероятно, это будет один из пяти самых распространённых форматов (т.н.

«форматы» файлов .doc, .docx, .rtf, .pdf, .odt или специально предназначенный для архивного хранения документов формат PDF/A). Общеизвестно, что в файлах форматов PDF (в т.ч. PDF/A), а также DjVu хранимый текст отделён от его представления, аналогичного назначения манипуляцию можно произвести и с другими форматами (но в них это несколько сложнее). Таким образом, не представляет особой сложности создание специальных документов, имеющих разное видимое (и напечатанное) и текстовое (анализируемое) представления. Более того, учитывая поведение программ для распознавания символов, а именно, документы, при наличии текстового слоя, обычно перестают распознаваться и берётся готовый текст из текстового слоя, вероятно предположить, что этот же специальный текстовый слой и будет использован для проверки документа системой антиплагиата вместо распознанного со страницы.

Решения данной проблемы:

1) проверять только отсканированные печатные работы (что категорически ресурсо- и трудоёмко);

2) проверять извлекаемый текст, но программами, форсировано его извлекающими из представления документа (таких пока нет);

3) требовать сдачу работ как оригинальными файлами, так и виде текста (plain-text) и учитывать разницу между ними.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект №12-07-00512).

Шаповалов В.Л., Бубнов А.Ю.
Россия, Москва, Московский государственный гуманитарный университет им. М.А. Шолохова

ОСНОВНЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ АУДИТОРИИ РУНЕТА (ПО РЕЗУЛЬТАТАМ ИССЛЕДОВАНИЯ WORLD INTERNRT PROJECT IN RUSSIA - 2012)

Изучение социальных взаимодействий в Интернете предполагает раскрытие интенсивности и особенностей использования Интернета как пространства досуга, коммерции и образования, а так же описание традиционных интернет-ролей и характера потребляемого контента. Параметры, анализируемые в исследовании отражают частоту обращения пользователей Рунета к его различным сегментам, разную степень интереса к информационной составляющей интернет-пространства и способам организации досуга.

Во-первых, использование Интернета как пространства и сервиса досуговой деятельности в целом отражает общие тенденции развития Рунета. Портрет активного пользователя интернет-сервисов, представленный в исследовании, соответствует общей тенденции по вхождению российского сегмента всемирной сети в фазу насыщения. Наряду с сохранением ядра активных пользователей с высшим образованием в возрасте 14-33 года, проживающих в крупных городах, нарастает процесс вовлечения в интернет-коммуникацию ранее незатронутых групп: лиц старшего возраста, пенсионеров, жителей малых городов и деревень, людей без высшего образования. Анализ данных показывает, что такие общераспространённые виды досуга как просмотр новостей, чтение блогов, поиск информации о путешествиях и здоровье существенно увеличивает присутствие в сети возрастных групп 43-53 и 54-63 года.

Во-вторых, обращает на себя внимание демографическая тенденция на преобладание женщин в сети. Так к 2012 году традиционная мужская доминация в интернете уступила место женской (48% и 52% соответственно, согласно последним данным). Женщины, очевидно, являются более активными пользователями досугового сегмента сети по многим показателям (в первую очередь здоровье, самообразование, поиск информации о товарах и услугах).

В-третьих, согласно исследованию Высшей школы экономики и Российской ассоциации электронных коммуникаций, экономика Рунета находится на подъеме и демонстрирует неплохие показатели в абсолютных цифрах: она составляет уже 4,5% ВВП России и около 11% интернет-экономики США. Из сопоставления этих данных с интенсивность использования коммерческих сервисов сети, становится ясно, что процесс роста экономики Рунета находится далеко от фазы насыщения.

В-четвёртых, сегментация пользователей по типичному потреблению информации, представленная в исследовании, коррелирует с проведенными ранее измерениями. Так принято выделять типичные роли шопперов (14% пользователей), блоггеров (15%), меломанов (17%) и геймеров (14%). Наше исследование так же показывает, что эти роли преобладают в досуговом секторе Рунета, характеризуя интернет-поведение значительной части пользователей сети. Согласно анализу переменных, среди респондентов насчитывается 24% активных (раз в день и чаще) геймеров из 60% играющих, 14% активных (раз в месяц и чаще) шопперов из 58% интересующихся товарами и услугами, 9% активных (несколько раз в день) потребителей музыки (меломанов) из 80% слушающих музыку в сети. К этим типичным ролям следует добавить также ищущих информацию о понятиях и фактах в сфере самообразования – условно, ресечерах, которых насчитывается 15% (активных, один раз в день и чаще) из 60%.

В-пятых, российские пользователи очень активно потребляют аудио и видеоконтент (в районе 80% пользователей). Особенности распространения контента в Рунете во многом связаны с опережающим ростом социальных сетей. Так по данным Международного союза электросвязи Россия находится на пятом месте в мире по вовлечённости пользователей в социальные сети (65% пользователей). Интегральные сервисы на базе социальных сетей позволяют одновременно удовлетворить потребности в общении, самовыражении, поиске и потреблении разнообразной информации, в первую очередь аудио-визуальной.

Щедрин П.О.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ СТАНЦИИ ОКОНЧАТЕЛЬНОЙ СБОРКИ МИКРООБЪЕКТИВОВ

Кафедрой ТПС осуществляется учебно-научный проект по созданию автоматизированной линии сборки микрообъективов, которая состоит из восьми станций. На каждой станции установлено оборудование компании Festo, которое имеет либо пневмопривод, либо электропривод. На станции окончательной сборки микрообъективов установлены робот-перекладчик, робот-манипулятор (декартовый робот), лифтовый склад, завинчивающее и переворотное устройства, а также устройство нанесения эмали. На станции десять управляемых координат. Для программирования роботов и устройств используется специальный язык STL, предназначенный для управления оборудованием Festo. Поскольку транспортная линия и все компьютеры в лаборатории изолированы от сети Интернет, все программы находятся в безопасности.

Целью данной работы является разработка унифицированных алгоритмов и управляющих программ на данной станции для последующего их применения на других станциях автоматизированной линии, которые к настоящему времени не имеют материального исполнения.

Алгоритм работы станции следующий: по транспортной линии приезжают шаттлы с тарами, в которых находятся незмеряемые предварительно детали МО. Робот-перекладчик переносит тары на станцию, а именно, в лифтовый склад. В дальнейшем, когда на станцию доставляется узел «Корпус», начинается окончательная сборка МО. Узел «Корпус» помещается в зону сборочных устройств, а робот-перекладчик переносит необходимую тару в зону работы робота-манипулятора, который в свою очередь переносит нужные детали в завинчивающее устройство. По мере необходимости робот-перекладчик переносит тары из лифтового склада в зону доступа робота-манипулятора, а также подпитывает лифтовый склад тарами с деталями пустой тарой, которые закончились при сборке, и выгружает тару с готовыми микрообъективами на транспортную линию.

Результатом работы являются унифицированные управляющие программы для сборки микрообъективов.

ПОДГОТОВКА И ПЕРЕПОДГОТОВКА КАДРОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Абрамян Г.В.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена

ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ НЕЛИНЕЙНОГО РАЗВИТИЯ СОВРЕМЕННОГО РЕГИОНАЛЬНОГО ОБРАЗОВАНИЯ И ПОДГОТОВКИ КАДРОВ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Традиционные научные подходы и технологии прогнозирования последовательного развития региональных образовательных систем в сфере информационной безопасности (РОСвСИБ) основываются на рассмотрении объектов детерминированных либо стохастических систем и процессов. Наши исследования показали, что, изучая текущее состояние детерминированных РОСвСИБ, можно установить, что произойдет с системой лишь в ближайшем будущем.

Для преодоления ограничений в области традиционных технологий прогнозирования и описания развития РОСвСИБ как объектов и процессов функционирующих в условиях глобализации и информационной среды, предлагается воспользоваться средствами информационно-коммуникационных технологий, синергетикой и описательным аппаратом нелинейной динамики:

1. Технологией (принципом) перехода и взаимодополняемости нелинейных логик описания РОСвСИБ на этапе их взаимного насыщения (с точки зрения синергетики достигается технологией-аттрактором вхождения-притягивания профессиональной, образовательной и информационной региональных сред друг к другу в зоне их оптимального функционирования).
2. Технологией (принципом) фрактальности или поэтапности нелинейного отражения промежуточных состояний эволюции РОСвСИБ.
3. Технологией (принципом) нелинейной распределенности инновационных РОСвСИБ, информационных и образовательных ресурсов во времени и среде. Технология определяет логику и зависимость конкретной образовательной ситуации в области подготовки специалиста для сферы ИБ от особенностей и специфики региональной среды (определяется интервалами времени между неопределенными состояниями (бифуркациями) РОСвСИБ.
4. Технологией (принципом) хаотичности и случайности регионально-образовательного диалога и информационного взаимодействия как переходного временного процесса реализации инновационных технологий и РОСвСИБ.
5. Технологией (принципом) не прогнозируемости инновационных последствий информационного взаимодействия субъектов РОСвСИБ по отношению к их образовательным результатам на достаточно длительных временах после бифуркаций в сфере регионального образования.
6. Технологией (принципом) глобальной, положительной линейности или однозначности в развитии инноваций предполагает, что ведущей тенденцией описания РОСвСИБ является однозначная (положительная или развивающая инновационную сферу регионального образования, сервиса и услуг) по смыслу логика.

Данный подход, технологии и принципы позволяют выявить общность закономерностей нелинейного инновационного развития РОСвСИБ разного уровня организации. Таким образом, положительные результаты прогнозирования нелинейного инновационного развития РОСвСИБ могут быть достигнуты изменением лишь значений основных переменных (параметров порядка) информационной или образовательной систем при подготовке кадров для сферы информационной безопасности регионов. А сходство описываемых процессов развития в различных нелинейных системах позволит в дальнейшем описывать структурный и временной изоморфизм инновационных процессов самоорганизации будущих РОСвСИБ.

Барабаш П.А.
Россия, Санкт-Петербург, Смольный институт Российской академии образования

ОСОБЕННОСТИ ПРЕПОДАВАНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ «ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ»

Создание и совершенствование информационных систем обработки персональных данных, использование в них новых информационных технологий объективно приводят к необходимости

совершенствования законодательной и нормативной базы, организационных методов и технических средств, направленных на обеспечение безопасности персональных данных.

Одним из серьезных препятствий на пути реализации ФЗ «О персональных данных» является отсутствие квалифицированных кадров. В рейтинге сложности реализации требований закона операторы на первое место ставят нехватку кадров, а на второе – недостаток средств.

Учитывая эти обстоятельства, на факультете информационных технологий Смольного института Российской академии образования для студентов специальности 090105 (075500) «Комплексное обеспечение информационной безопасности автоматизированных систем» в разделе «Специальные дисциплины» в течение ряда лет читается учебная дисциплина: «Защита информации в информационных системах персональных данных».

Целью дисциплины является формирование у студентов знаний по основам защиты персональных данных (ПДн) в информационных системах персональных данных (ИСПДн), навыков и умения в применении знаний для конкретных условий, а также развитие в процессе обучения системного мышления, необходимого для решения задач инженерно-технической защиты информации с учетом требований системного подхода.

В результате обучения студенты должны иметь представление об угрозах безопасности информации в ИСПДн, знать теоретические, физические и организационные основы инженерно-технической защиты информации, уметь составлять Модель угроз для заданной ИСПДн, выбирать необходимые и достаточные средства инженерно-технической защиты информации, иметь навыки применения технических средств и методов защиты информации при проектировании и эксплуатации систем защиты персональных данных.

Трудоемкость этой учебной дисциплины составляет 102 часа, из которых 36 часов – лекционных. Она включает следующие основные разделы:

– Обработка персональных данных. Основные понятия и определения.
– Проведение классификации информационных систем персональных данных.
– Основные мероприятия по организации обеспечения безопасности персональных данных.
– Мероприятия по техническому обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.
– Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных.
– Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
– Типовые модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
– Система защиты персональных данных.

Целью лекций является изложение нового теоретического материала и иллюстрация его примерами и задачами. Целью практической работы студентов является построение Модели угроз для заданной ИСПДн, нахождение актуальных угроз, создание системы защиты персональных данных с использованием сертифицированных средств защиты информации.

В помощь студентам при изучении этой учебной дисциплины автором написано и издано учебное пособие «Безопасность персональных данных», допущенное УМО вузов России по университетскому политехническому образованию в качестве учебного пособия для студентов вузов, обучающихся по направлению подготовки 230400 Информационные системы и технологии.

Данное учебное пособие содержит новый актуальный материал по обеспечению безопасности обработки персональных данных в информационных системах.

Оно адресовано студентам вузов в дополнение к учебникам по дисциплинам: «Инструментальные средства информационных систем», «Методы и средства проектирования информационных систем и технологий», «Архитектура информационных систем», которые входят в базовую часть цикла профессиональных дисциплин ФГОС подготовки бакалавра по направлению 230400 «Информационные системы и технологии», а также студентам, обучающимся по профилю «Безопасность информационных систем».

Учебное пособие состоит из 9 глав, введения и заключения, в приложении 1 представлен краткий словарь терминов и определений, а в приложении 2 – список используемых в учебном пособии обозначений и сокращений.

Барабаш П.А.
Россия, Санкт-Петербург, Смольный институт Российской академии образования

О НЕОБХОДИМОСТИ РАЗДЕЛА ПО ИНФОРОМАЦИОННОЙ БЕЗОПАСНОСТИ В УЧЕБНОЙ ДИСЦИПЛИНЕ «ИНФОКОММУНИКАЦИОННЫЕ СИСТЕМЫ И СЕТИ »

Новая совокупность требований, обязательных при реализации основных образовательных программ бакалавриата по направлениям подготовки в соответствии с федеральными государственными образовательными стандартами высшего профессионального образования, в

значительной мере изменила подход к формированию примерных учебных программ дисциплин и методики преподавания.

В соответствии с федеральным государственным образовательным стандартом высшего профессионального образования по направлению подготовки 230400 Информационные системы и технологии (далее ФГОС ВПО) область профессиональной деятельности бакалавров включает: исследование, разработку, внедрение и сопровождение информационных технологий и систем.

Объектами профессиональной деятельности бакалавров являются: информационные процессы, технологии, системы и сети, их инструментальное (программное, техническое, организационное) обеспечение, способы и методы проектирования, отладки, производства и эксплуатации информационных технологий и систем.

В учебной программе каждой дисциплины (модуля) должны быть четко сформулированы конечные результаты обучения в органичной увязке с осваиваемыми знаниями, умениями и приобретаемыми компетенциями.

Компетентностный подход ФГОС ВПО требует, чтобы выпускник обладал, в частности, следующими профессиональными компетенциями:

– способность поддерживать работоспособность информационных систем и технологий в заданных функциональных характеристиках и соответствии критериям качества (ПК-32);

– готовность обеспечивать безопасность и целостность данных информационных систем и технологий (ПК-33)

На факультете информационных технологий Смольного института Российской академии образования ведется подготовка бакалавров по направлению подготовки 230400 Информационные системы и технологии.

Структурой основной образовательной программы ФГОС ВПО в базовой (общепрофессиональной) части профессионального цикла предусматривается дисциплина «Инфокоммуникационные системы и сети».

Согласно Примерному учебному плану трудоемкость дисциплины составляет 5 зачетных единиц, 180 часов, из которых 90 часов отводится на аудиторные занятия и также 90 часов - на самостоятельную работу.

Дисциплина посвящена изучению современных сетевых технологий. В процессе изучения студенты приобретают знания и навыки по основам устройства и функционирования инфокоммуникационных систем и сетей.

Примерная основная образовательная программа по этому направлению подготовки, равно как и Примерная программа по данной дисциплине не предусматривают изучение вопросов информационной безопасности и защиты информации.

Это упущение решается нами путем введения в структуру дисциплины раздела «Безопасность инфокоммуникационных систем и сетей», на который отводится 20 часов, в том числе 8 часов для самостоятельной работы.

Такое решение позволяет дать студентам в сжатой форме:

– основы информационной безопасности;

– понятие и источники угроз безопасности информации;

– структуру, классификацию и основные характеристики технических каналов утечки информации;

– методы и средства защиты от утечки по техническим каналам;

– методы и средства защиты от угроз, связанных с несанкционированным доступом к информации;

– назначение и особенности функционирования устройств защиты;

– организационные основы инженерно-технической защиты информации.

Таким образом, выпускники могут получить знания и необходимые профессиональные компетенции в соответствии с требованиями ФГОС ВПО.

Белая Т.И.
Россия, Санкт-Петербург, Северо-Западный институт печати Санкт-Петербургского государственного университета технологии и дизайна

ЧЕЛОВЕК КАК ОСНОВНОЙ ЭЛЕМЕНТ СИСТЕМЫ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Широкое использование информационных технологий во всех сферах человеческой деятельности приводит к появлению новых потенциальных каналов утечки информации, значительная часть которой относится к конфиденциальной или является коммерческой тайной и не подлежит разглашению третьим лицам. Защита и использование такой информации регламентируется соответствующими федеральными законами Российской Федерации.

Как показывает практика, основным каналом утечки информации в организации является её сотрудник. Утечка коммерческой информации со стороны сотрудника может быть как преднамеренной, так и непреднамеренной. Непреднамеренная утечка чаще всего обуславливается следующими причинами:

– низкая информированность сотрудника о возможных каналах утечки информации;
– низкий профессионализм сотрудников, непосредственно отвечающих за безопасность;
– низкая мотивация в сохранении конфиденциальной информации;
– высокая потребность общения в социальных сетях в рабочее время;
– низкая корпоративная культура в организации;
– недопонимание важности повышения лояльности и обучения основам безопасности руководством организации;
– экономия средств на развитие технической базы по обеспечению информационной безопасности.

Для повышения уровня обеспечения информационной безопасности организации прежде всего необходима реализация руководством планомерной политики и мероприятий по повышению уровня информированности, мотивации и систематическому обучению сотрудников основам информационной безопасности. В докладе обсуждается содержание дополнительных образовательных программ, направленных на повышение уровня информированности в области обеспечения информационной безопасности сотрудников и повышение эффективности системы безопасности организации в целом.

Залещанский Б.Д., Свиридов А.П., Павлова О.А., Шалобина Е.А.
Россия, Москва, Московский государственный технический университет радиотехники, электроники и автоматики

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СОЦИО-ТЕХНИЧЕСКИХ СИСТЕМ ЭКОНОМИЧНЫМИ СТРАТЕГИЯМИ УПРАВЛЕНИЯ ПОДГОТОВКОЙ ПЕРСОНАЛА

Современные предприятия и организации являются социо-техническими системами. Безопасность и надёжность их функционирования определяются не только надёжностью технических и программных средств, но и деятельностью персонала. Безопасность и надёжность технических и программных средств обеспечивается в настоящее время по средствам контроля, диагностики и последующих профилактических и восстановительных работ.

В докладе предлагается подобный подход к обеспечению надёжности действий персонала. Рассматриваются периодические стратегии управления качеством профессиональной подготовки обучаемых (персонала) с учётом интенсивности забывания и экономических показателей (затрат на обучение, контроль и потерь из-за ошибок персонала и др.). Они основаны на оптимальном планировании во времени повторений или предупредительных восстановлений знаний, умений, навыков и компетенций.

В качестве критерий оптимальности управления используются:

1. Максимум коэффициента профессиональной готовности обучаемого (персонала);
2. Минимум средних удельных затрат (потерь) и др.

Требуемая профессиональная готовность обучаемого (персонала) обеспечивается путем контроля и последующего управления качеством подготовки. Приводятся результаты применения рассматриваемых стратегий.

Касаткин В.В., Советов Б.Я., Цехановский В.В.
Россия, Санкт-Петербург, Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ПРОФИЛЬ ПОДГОТОВКИ БАКАЛАВРОВ «БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ» В СОСТАВЕ НАПРАВЛЕНИЯ «ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ»

Целесообразность включения в номенклатуру профилей подготовки бакалавров «Безопасность информационных систем» в составе направления «Информационные системы и технологии» обосновывается следующими соображениями.

В настоящее время сложилась уникальная ситуация, когда сначала проектируются и внедряются информационные системы, а затем они дополнительно оснащаются средствами защиты информации в зависимости от поставленных целей.

Такой подход, как с позиций системной инженерии, так и с позиций экономики не всегда является неэффективным. Вместе с тем, пример отраслей, достигших высокого уровня технологий, например, автомобилестроения, демонстрирует четкое разделение: безопасность, обеспечиваемая в процессе проектирования автомобиля, и безопасность, обеспечиваемая в рамках организации дорожного движения. Именно на такой характер деятельности ориентирован бакалавр по профилю подготовки «Безопасность информационных систем».

Проектирование информационных систем является коллективным процессом и специалист в области информационной безопасности должен участвовать во всех стадиях создания конечного продукта. Этим достигается решение двух важных проблем:

– обеспечение высоких показателей проектируемой информационной системы;

– оптимальное использование ресурсов – финансовых, материальных и трудовых.

ИТ-специалисты могут принести пользу своим компаниям только понимая основополагающие принципы, положенные в основу разработки, внедрения и эксплуатации информационных систем по всем основным показателям, включая и информационную безопасность.

Структура организации профиля является модульной с выделением базовых дисциплин и дальнейшим их раскрытием в вариативной части. Курсы, составляющие программу профиля, учат студентов, как применить технологию для создания решений и достичь требуемых результатов с большей эффективностью.

В докладе приводятся варианты ПООП для бакалавров по профилю подготовки «Безопасность информационных систем» в составе направления подготовки «Информационные системы и технологии», дается оценка программ учебных дисциплин как базовой, так и вариативной части, а также приводятся рекомендации вузам по дальнейшему использованию ПООП.

Куватов В.И., Пантиховский О.В., Примакин А.И., Синещук Ю.И.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России, ВУНЦ ВМФ «Военно-морская академия имени Адмирала Флота Советского Союза Н.Г. Кузнецова»

ПРИМЕНЕНИЕ БЛОЧНО-МОДУЛЬНЫХ ТЕХНОЛОГИЙ ДЛЯ ОПТИМИЗАЦИИ УЧЕБНЫХ ПЛАНОВ И ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ПОДГОТОВКИ КУРСАНТОВ ПО СПЕЦИАЛЬНОСТИ 090915.65 – «БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРАВООХРАНИТЕЛЬНОЙ СФЕРЕ»

Причинами, послужившими использованию блочно-модульных технологий к построению образовательных стандартов, учебных планов и образовательных программ являются:

– повышение гибкости образовательных программ;

– облегчение определения «точек» входа и «точек» выхода курсанта в его индивидуальной образовательной траектории;

– необходимость увязки всех компетенций к конкретным дисциплинам, практикам, модулям и циклам (вместе с тем, необходимо отметить, что существует некоторое подмножество компетенций, которое формируется самой средой образовательной организации в период пребывания в ней обучающегося);

– минимизация трудозатрат при оперативной модификации различных видов модулей, включаемых в учебные дисциплины, внесение новых или удаление устаревших модулей, в соответствии с требованиями ФГОС ВПО «высшие учебные заведения должны ежегодно обновлять основные образовательные программы с учетом развития науки, культуры, экономики, техники, технологий и социальной сферы»;

– необходимость реализации требований о текущем контроле и обеспечении оценки достижений обучаемых с учетом системности работы;

– возможность оперативно формировать содержательно новые курсы из модулей, как части одно-, или многосеместровой дисциплины;

– необходимость реализации концепции непрерывного образования и связанные с ней программы повышения квалификации и переподготовки специалистов также требуют более компактных, но информативных и логически завершённых дидактических единиц со своей достаточно совершенной системой контроля знаний обучающихся, чем и являются модули семестровой дисциплины.

Поэтому можно утверждать, что блочно-модульное построение учебных планов и образовательных программ учебных дисциплин является одним из основных принципов развития образования и повышения эффективности подготовки специалистов, в том числе, по специальности 090915.65 – «Безопасность информационных технологий в правоохранительной сфере».

Вместе с тем, из триады, характеризующей инновационный характер нового поколения образовательных стандартов: компетенция – модуль – зачетная единица, понятие модуля наименее методически разработано и наиболее сложно для понимания, по нему не выработано достаточно согласованных документов.

В основе методики формирования модулей, а так же последовательности изучения их курсантами лежат следующие положения.

Все дисциплины учебного плана можно поделить на группы взаимосвязанных дисциплин или модулей. Существует три типа отношений между дисциплинами (модулями) учебного плана: отношения следования, отношения взаимной независимости и отношения взаимной зависимости.

Если две дисциплины (модули) связаны отношением следования, то изучение одной из них можно начинать только после окончания изучения другой дисциплины (или определенных тем другой дисциплины). Так, например, изучению физики должно предшествовать изучение определенных разделов математики.

Если между двумя дисциплинами существует отношение взаимной независимости, то их изучение может вестись произвольно по отношению друг к другу, в том числе, они могут изучаться параллельно. Так, например, взаимно независимыми являются дисциплины информатика и история.

Последний, третий тип отношений означает, что изучение дисциплин должно вестись параллельно, с учетом зависимости между темами. Такое отношение встречается редко, как правило, оно свидетельствует о том, что деление области знаний между дисциплинами проведено неверно. Поэтому мы взаимную зависимость между дисциплинами учитывать не будем.

Одно из важнейших свойств памяти человека – ассоциативность. В группе из двух дисциплин связанных отношением следования, чем больше ассоциаций возникает у курсантов при изучении последующей дисциплины, тем эффективнее ее изучение. Другое важнейшее свойство памяти – забывание. Если временной интервал между дисциплинами, связанными отношениями следования велик, то большая часть предшествующей дисциплины забыта и количество ассоциаций, возникающих у курсантов при изучении последующей дисциплины меньше. Поэтому, учебный план тем оптимальнее, чем меньше временные интервалы между дисциплинами (модулями) связанными отношением следования.

В докладе предлагаются модули (блоки) изучаемых дисциплин, а так же изменения в последовательности изучения дисциплин учебного плана специальности 090915.65 – «Безопасность информационных технологий в правоохранительной сфере», по которой проходят подготовку курсанты Санкт-Петербургского университета МВД России.

Морозов В.Е., Дрозд А.В.
Россия, Москва, ООО «Новые поисковые технологии»

ОБУЧЕНИЕ СПЕЦИАЛИСТОВ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВОПРОСАМ ПРАКТИЧЕСКОГО ИСПОЛЬЗОВАНИЯ DLP-СИСТЕМ

Информация сегодня является одним из критически важных факторов успеха деятельности любой организации. В этой связи стоит отметить, что средняя стоимость одной утечки информации в мире составляет около 5,3 млн. долларов, а в качестве основных причин инцидентов, связанных с утечками, отечественные и зарубежные исследователи всё чаще называют «человеческий фактор» и деятельность инсайдеров. Для предотвращения утечек данных на корпоративном уровне, как правило, используются так называемые Data Leak Prevention (или DLP) системы. Работа DLP-систем строится на перехвате и последующем анализе потоков данных, пересекающих периметр в направлении «вовне» либо циркулирующих внутри защищаемой корпоративной сети. Перехваченная информация анализируется с помощью различных поисковых алгоритмов, а при обнаружении данных, соответствующих выбранным критериям, срабатывает активная компонента системы, оповещая об инциденте сотрудника службы информационной безопасности. При этом в ряде случаев передача сообщения (пакета, потока, сессии) может блокироваться. Существующие на данный момент DLP-системы обладают широкими функциональными возможностями и демонстрируют достаточно высокую эффективность при условии их грамотного применения.

Компания SearchInform является разработчиком DLP-системы «Контур информационной безопасности SearchInform» (далее «КИБ SearchInform»), которая позволяет эффективно защитить бизнес от убытков, связанных с утечками информации. На сегодняшний день «КИБ SearchInform» -- признанный лидер на рынках информационной безопасности России и стран СНГ. Данное решение используется во многих крупных организациях, работающих в самых разных отраслях – от банковского дела до машиностроения. Работа продуктов SearchInform на многих тысячах компьютеров красноречиво свидетельствует о доверии пользователей к ним.

Для обучения сотрудников служб информационной безопасности российских предприятий и организаций основам использования современных DLP-систем компанией SearchInform создан учебный центр, в деятельности которого важное место принадлежит реализации программы «Практика применения DLP-систем». Указанная программа, созданная на основе многолетнего опыта взаимодействия компании с более чем 1200 предприятий и организаций, не только знакомит специалистов с соответствующей категорией средств защиты информации, но и способствует выработке у них навыков решения различных проблем, которые могут возникнуть в их собственной профессиональной деятельности. В содержании программы нашли свое отражение следующие вопросы: типовые задачи, стоящие перед сотрудниками службы информационной безопасности; методы их решения; характеристика представленных на рынке программных продуктов, используемых для анализа и контроля передаваемой информации в масштабах предприятия или организации; основы работы DLP-систем на примере «КИБ SearchInform»; юридические аспекты использования DLP-систем; автоматизация контроля нерационального использования времени и ресурсов организации и многие другие. Подобное обучение позволяет не только существенно расширить кругозор специалистов в области информационной безопасности, но и сформировать у них новые профессиональные компетенции, во многом определяющие успешность деятельности.

Сегодня уже ни у кого нет сомнений в том, что высокий уровень современных средств незаконного получения информации, а также ценность данных для компаний и их клиентов делают защиту информационных активов чрезвычайно важной. Внедрение специализированных решений (таких как DLP-системы и «КИБ SearchInform», в частности) позволяет существенно уменьшить риски,

связанные с эксплуатацией ИТ-систем, оптимизировать затраты на обеспечение информационной безопасности, повысить управляемость процессов движения информации в организации. Однако широкое распространение названных средств защиты информации сдерживается целым рядом факторов, одним из которых является отсутствие достаточного количества специалистов, обладающих навыками их эффективного применения. Решение этой проблемы, на наш взгляд, невозможно без наличия соответствующих образовательных программ, реализуемых имеющими государственную аккредитацию учреждениями высшего профессионального образования.

С точки зрения компании SearchInform, для преодоления возникшего противоречия необходимо: во-первых, наличие взаимной заинтересованности учреждений образования и вендоров DLP-систем; во-вторых, бесплатное предоставление DLP-систем для нужд учреждений образования, обеспечивающих подготовку и переподготовку специалистов по направлению «Информационная безопасность»; в-третьих, разработка соответствующих учебных и методических материалов; в-четвёртых, внесение соответствующих изменений в учебные программы профильных дисциплин. Выполнение всех перечисленных условий приведет к тому, что руководители организаций и лица, обеспечивающие информационную безопасность, будут не только иметь техническую возможность, но и обладать необходимыми профессиональными компетенциями для контроля и анализа всей информации, которая циркулирует по каналам связи, используемым в организации.

Пантюхин О.И.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного

ПРЕПОДАВАНИЕ СОВРЕМЕННЫХ ДИСЦИПЛИН В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В современных условиях сформировался новый вид трудовой деятельности, связанный с получением, распространением и хранением информации. Информатизация ведет к созданию единого мирового информационного пространства, к унификации информационных технологий различных стран.

Новые технологии сулят грандиозные перспективы. Вместе с тем, катастрофически возрастает цена потерь в случае нештатного функционирования или снижения надежности систем обработки и передачи информации. Следует признать, что все более зримо проявляется зависимость экономики от качества систем защиты информации, в том числе криптографических.

Использование подобных технологий приводит к необходимости применения ЭВМ для решения специфических задач, таких как обеспечение уверенности в гарантиях ответственности лиц, отдающих распоряжения, ответственности исполнителей за своевременное выполнение распоряжений и т.д. Возник ряд новых задач, имеющих практическое значение, например, задача принятия нотариальных решений в автоматическом режиме, электронный обмен в банковских системах. Для решения подобных задач необходимо наличие специфических алгоритмов.

Принципы построения соответствующих алгоритмов разработаны в криптологии, науке изучающей методы построения и анализа систем защиты информации, основанных на математических преобразованиях данных с использованием секретных параметров. Такие системы называются криптографическими. Применение криптографических систем защиты информации позволяет обеспечить надежность электронного документооборота.

В настоящее время высшие учебные заведения предлагают новые дисциплины для подготовки специалистов и магистров, например, «Математические методы защиты информации», «Криптографические алгоритмы и средства», «Методы криптоанализа» и другие.

Предметом учебных дисциплин обычно являются:

– общие принципы построения систем криптографической защиты информации;

– ключевые системы, криптоалгоритмы и криптопротоколы, составляющие основу криптографической защиты информации в современных компьютерных сетях и их криптографические свойства;

– подходы относительно выбора параметров криптосистем, алгоритмы их построения и тестирования;

– методика организации подсистем криптографической защиты информации в компьютерных системах и сетях.

Основными задачами учебной дисциплины является формирование навыков:

– уметь предоставлять рекомендации относительно использования стандартных криптоалгоритмов и криптопротоколов для обеспечения надлежащего уровня защиты информации;

– уметь определять существенные параметры и потенциальные слабости типичных криптографических алгоритмов и протоколов;

– уметь использовать и реализовывать стандарты в области криптографической защиты информации;

– уметь применять и разрабатывать новые методы и средства в области криптографической защиты информации.

Программы дисциплин, как правило, предназначены для подготовки специалистов и магистров в области математического и программного обеспечения защиты информации в компьютерных системах и сетях связи.

Раскин А.В., Фральцова Т.А.
Россия, Москва, Войска воздушно-космической обороны, Институт повышения квалификации ТЭК

ОСОБЕННОСТИ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В СФЕРЕ ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

В современном обществе информационные ресурсы играют важную роль. По мнению экспертов, их значение нередко больше, чем ресурсы материальные. Информация о том кому, когда и где продать товар может оцениваться соразмерно самому товару. Динамика развития мирового общества показывает, что информационные ресурсы начинают преобладать над материальными ресурсами.

В экономической деятельности любой организации (предприятия, фирмы) присутствует информационный ресурс. К нему можно отнести документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных и других информационных системах). Проблемы защиты информации занимают одно из ведущих мест в ряду приоритетных проблем, которые приходится разрешать субъектам хозяйственной деятельности.

Необходимость в защите информации в сфере экономики обусловлена следующими причинами:

– формирование открытого информационного общества;

– информация имеет непосредственную ценность в силу ее неизвестности третьим лицам, т.е. является товаром и подлежит защите;

– формирование информацией нового уровня знаний, которые в виде умений и навыков сотрудников выступают основным фактором, обеспечивающим организации получение прибыли;

– распространение информации по формальным и неформальным каналам.

Исходя из вышесказанного, в настоящее время появилось новое понятие - информационно-экономическая безопасность. По нашему мнению, ее можно определить как составную часть экономической безопасности, которая обеспечивает защиту субъектов хозяйственной деятельности от внешних и внутренних информационных угроз.

Современная система подготовки кадров предусматривает обучение специалистов в области информационной защиты и экономической безопасности. Однако сегодня в программах обучения ни один ВУЗ не имеет специальности «информационно – экономическая безопасность».

Предполагается, что данные специалисты должны иметь представление:

– об основах экономической деятельности организации (предприятия, фирмы);

– об основах финансовой деятельности организации (предприятия, фирмы);

– об основах производственной деятельности организации (предприятия, фирмы);

– о современных и перспективных сетевых интернет - технологиях;

– о современных коммуникационных технологиях;

– о современных и перспективных программно – аппаратных комплексах обработки информации;

– об основах документоведения.

Знать:

– теоретические основы информационной безопасности в экономике;

– нормативно – правовую базу обеспечения информационной безопасности в экономике;

– основы построения системы обеспечения информационной безопасности в организации и принципы ее применения;

– формы и способы организационно – технической и программно – аппаратной защиты информации.

Уметь:

– создать систему обеспечения информационной безопасности экономической и производственной деятельности и организовать ее применение;

– практически применять правовую практику в области обеспечения информационной безопасности;

– применять организационно – технические и программно – аппаратные средства защиты информации.

Превращение закрытой национальной экономики в открытую систему - закономерный, но весьма противоречивый процесс. Наша страна находится в начале сложной работы по интеграции в мировое экономическое пространство. В этой связи вопрос подготовки высококвалифицированных кадров способных обеспечить информационно-экономическую безопасность организации является весьма актуальной.

Рябова А.А.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова

ИСПОЛЬЗОВАНИЕ СИСТЕМЫ ДИСТАНЦИОННОГО ОБУЧЕНИЯ «ФАРВАТЕР» В ПОДГОТОВКЕ КВАЛИФИЦИРОВАННЫХ КАДРОВ

В настоящее время существуют проблемы в подготовке квалифицированных кадров во многих областях. Эти проблемы связаны не только с бюджетом и временем, но еще и местом жительства до учебного заведения. Решением подобных проблем является дистанционное обучение.

Основными преимуществами дистанционного обучения являются:
– обучение без отрыва от производственной деятельности;
– резкое сокращение накладных расходов;
– неограниченное число обучаемых;
– ускорение процесса обучения;
– свободный график обучения;
– доступность изложения учебного материала;
– возможность компьютерного тестирования;

В рамках создания и внедрения системы электронного обучения, развития и оценки обучающих важной компонентой является учебный контент.

Методика создания электронного контента позволяет с равной степенью создавать электронные курсы.

Даже обладая начальными навыками работы на компьютере, преподаватель может легко разработать электронные учебные курсы, включая:
– создание структуры курса, разделов, занятий, описание целей обучения;
– структурированное изложение материала с возможностью повторного изучения;
– опросы и анкетирование;
– создание контрольных заданий и тестов, промежуточного и итогового тестов;
– разбиение курса на смысловые части, сформировать глоссарий, связывать учебные материалы гипертекстовыми ссылками.

Для работы с электронными курсами требуется только персональный компьютер, подключенный к сети Интернет. Ваше электронное издательство – это не просто «разовое мероприятие», это всерьез и надолго, т.е. на весь период, когда Вы рассчитывает заниматься электронным обучением.

В государственном университете морского и речного флота имени адмирала С.О. Макарова (до реорганизации – Санкт-Петербургском государственном университете водных коммуникаций) успешно развивается система дистанционного обучения (СДО) «Фарватер» на платформе Moodle «Modular Oject-Oriented Dynamic Learning Environment» (модульная объектно-ориентированная динамическая среда обучения). Moodle представляет собой автоматизированную, основанную на компьютерных и Интернет-технологиях, систему управления обучением – Learning Management System (LMS).

Система дистанционного обучения «ФАРВАТЕР» имеет интуитивно понятный интерфейс. При создании электронного курса не возникает никаких проблем, а в случае вопросов можно обратиться к вспомогательным инструкциям.

Основное назначение СДО «Фарватер» – учебная внеаудиторная самостоятельная работа обучающихся (студентов, курсантов, аспирантов и т.д.).

Важной составляющей процесса создания и внедрения системы электронного обучения, оценки и развития преподавателей является подготовка персонала учебной группы к работе в соответствующей платформе. Именно поэтому в ГУМРФ были созданы курсы повышения квалификации, занятия по которым ведутся с февраля 2013 года. С осени 2013 планируется включить дистанционное обучение на курсах в СДО «ФАРВАТЕР», по причине отсутствия на очных занятиях.

Салтыков Е.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

ПОИСК И АНАЛИЗ УЯЗВИМОСТЕЙ В ПРОГРАММЕ «АВЕРС: ЭЛЕКТРОННЫЙ КЛАССНЫЙ ЖУРНАЛ»

Внедрение информационных технологий в классическую систему школьного образования ведет к постепенному переходу от стандартных бумажных форм обеспечения учебного процесса на электронные: организация ведения электронного дневника учащегося, электронного журнала успеваемости. Это, безусловно, положительный момент. Однако реализация программного продукта с точки зрения информационной безопасности оставляет желать лучшего.

Автором было проведено исследование указанного приложения на предмет несанкционированного доступа к его базе.

В процессе исследования были произведен анализ веб-ресурса – «Электронного классного журанала» (ЭКЖ), в котором были найден и протестирован ряд уязвимостей. К слабым местам данного продукта относятся следующие: уязвимость к SQL-инъекциям, возможность подмены сессии пользователя, выполнение запросов к базам данных от имени администратора сервера.

При выполнении работы были использованы следующие программные продукты: Charles Web Debuggin Proxy для анализа, перехвата и корректировки трафика, последние версии браузера Google Chrome для непосредственного обращения к ресурсу через web-интерфейс.

В результате использования найденных уязвимостей были произведены успешные попытки аутентификации и авторизации под учётными записями пользователей различных привилегий (учитель/директор/администратор). Выполнялась подмена сессионных данных уже авторизованных в

системе пользователей. Выполнен ряд произвольных SQL-запросов к доступным базам данных от лица администратора системы и получена различная информация в т. ч. конфиденциальная (адреса проживания, телефоны, ИНН, паспортные данные, данные страховых служб и т. д.).

При эксплуатации указанных уязвимых мест в системе злоумышленник мог бы получить огромное количество информации, связанной с личными делами учащихся, их родителями, а так же руководящего состава учебного заведения и использовать её в незаконных целях.

Сведения об уязвимых местах были доведены до руководства учебного заведения, администрации и службы поддержки АИАС АВЕРС. Никаких ответов и комментариев от компании не поступало. Однако в последующих версиях данного продукта была исправлена одна уязвимость - получение НСД с помощью комментирования пароля при передаче данных на сервер.

Ходаков А.И., Колодин М.Ю., Вус М.А.
Россия, Санкт-Петербург, ООО «Академия информационных технологий»,
Санкт-Петербургский институт информатики и автоматизации РАН

ИНСТРУМЕНТАРИЙ ИНФОРМАЦИОННОГО СОПРОВОЖДЕНИЯ ДЛЯ СИСТЕМЫ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

Качество подготовки специалистов в учебных заведениях профессионального образования определяется совокупностью самых разных условий и факторов. Большое значение при этом имеет характер информационного взаимодействия основных участников образовательного процесса – преподавателей и студентов, систематичность и глубина, содержание и границы их общения.

Прогресс в сфере производства, заметно опережающий развитие практики профессионального образования, ориентирует на существенное расширение круга профессионально-педагогического общения преподавателей и студентов, активизацию повседневного партнерского взаимодействия различных учебных заведений по вопросам преподавания, а также научных исследований. Универсальные требования к уровню подготовленности современного специалиста могут быть успешно реализованы только сознательными усилиями и объединенными интеллектуальными ресурсами коллективного субъекта педагогической деятельности.

Современный студент склонен к интеллектуальной мобильности, он предпочитает получать учебную информацию из самых разнообразных источников, желает самостоятельно сопоставлять, по-своему оценивать, свободно выбирать преподавателей, учебники, методики, формы и режимы обучения. И в этих его запросах – объективное и обоснованное требование времени.

В докладе обсуждается перспектива формирования на базе специально разработанного многофункционального веб-сайта интернет-сегмента в интересах вовлеченных в педагогический процесс профессиональной подготовки кадров субъектов образовательной деятельности, Ресурсы такого сайта дают возможность создания персональных электронных кейсов преподавателей, предоставляя им широкие возможности для изучения опыта своих коллег, в том числе, из других учебных заведений и регионов.

Наличие на общедоступном сайте персональных кейсов способно обеспечить широкое сетевое общение преподавателей, формирование в их профессиональном сообществе атмосферы открытости и взаимодоверия. Личность преподавателя при этом обретает дополнительное пространство для профессионального развития. Предлагаемое информационное сопровождение для системы профессионального образования минимизирует административное вмешательство в процесс взаимодействия преподавателей и студентов, предоставляет им возможность для свободного содержательного общения. У студентов существенно расширяются возможности для свободного выбора учебно-методических материалов, тех продуктов, которые им представляются наиболее интересными, понятными и полезными. Наряду с этим будет происходить своего рода студенческая экспертиза предлагаемых учебно-методических разработок, наиболее удачные из которых будут иметь более высокий рейтинг (в данном случае – показатель скачиваний).

Сайт может стать своеобразной выставочной площадкой, на которой учебное заведение может показать успехи своих сотрудников, их учебно-методические достижения, педагогические находки, результаты научных исследований. Участие в кейс-проекте позволит экономичным способом расширять кооперацию образовательных учреждений в учебной и научной деятельности, стимулировать быстрое распространение передового педагогического опыта. В конечном счете, это будет способствовать повышению качества подготовки специалистов.

Шалагинова О.Б.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ПРОБЛЕМА КАДРОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Информационная безопасность – область науки и техники, охватывающая совокупность программных, аппаратных и организационно-правовых методов и средств обеспечения безопасности информации при ее обработке, хранении и передаче с использованием современных информационных технологий. Это определение приведено из словаря управления персоналом.

Вопросы подготовки персонала или кадров по информационной безопасности получили развитие в России с начала 90-х годов. Тематику обучения составляют как зарубежные курсы, так и авторские курсы отечественных учебных центров, разработанные с учетом специфики российской действительности. В настоящее время в стране сформировались основные направления системы подготовки и переподготовки кадров в области информационной безопасности. Подготовка кадров осуществляется комплексно на нескольких уровнях.

Где и как готовят специалистов в области информационной безопасности? В первую очередь это относится к подготовке и переподготовке специалистов правоохранительных органов, органов суда и прокуратуры в области борьбы с преступлениями в сфере компьютерной информации. В качестве метода отбора кадров для обучения используется тестирование на профессиональную пригодность. Данный метод не является нововведением, но опыт предварительного тестирования абитуриентов, поступающих на специальности, связанные с защитой информации, заслуживает самого пристального внимания в связи с необходимостью высоких морально-этических качеств у специалистов, занимающихся вопросами информационной безопасности. Тестирование на профессиональную пригодность признано обязательным элементом для последующего обучения.

Каковы условия повышения качества подготовки специалистов в области защиты информации? В первую очередь это обеспечение тесной связи учебного процесса с научными исследованиями в области информационной безопасности. В настоящее время сложилась научная школа в области криптографии; по правовым вопросам защиты информации; защите компьютерных систем от вредоносных программ. Также следует отметить привлечение большого числа специалистов и мощного технического обеспечения. Решение проблемы обеспечения учебного процесса педагогическими кадрами высшей квалификации видится в организации краткосрочных курсов повышения квалификации, проведении семинаров и конференций по обмену опытом. Требования к материально-техническому обеспечению учебного процесса очень высоки. Занятия должны проводиться в специально оборудованных помещениях с применением современной вычислительной техники и специальных технических средств. Следует отметить также высокую стоимость обучения.

Вопросы кадрового обеспечения являются важнейшей составной частью деятельности по обеспечению информационной безопасности и борьбы с преступностью в области компьютерной информации. Уделяется все возрастающее внимание проблемам подготовки кадров, потому что существующая система подготовки кадров еще не в полной мере удовлетворяет потребностям страны, а возникающие перед ней новые задачи диктуют необходимость как обновления содержания образования, так и совершенствования организации образования. Борьба с компьютерной преступностью является одной из важнейших задач современности. Успешность противодействия в этом направлении во многом определяется качеством подготовки специалистов по информационной безопасности. Необходимо дальнейшее наращивание объемов подготовки кадров, широкое введение общеобразовательных курсов информационной безопасности при подготовке кадров различной профессиональной направленности с учетом перспектив информатизации общества.

Особенно остро проблема кадрового обеспечения касается правоохранительных органов, а также работников судов, способных в комплексе решать проблемы борьбы с компьютерной преступностью, включая стадии предупреждения преступлений, их обнаружения и локализации. Существует настоятельная необходимость организации планомерной переподготовки и повышения квалификации специалистов по направлению обеспечения информационной безопасности для органов государственной власти и управления, оборонной промышленности, сферы институтов охраны интеллектуальной собственности.

Совместно с другими мерами улучшения подготовки кадров высшей квалификации по проблемам информационной безопасности, имеют в виду и активизацию работы аспирантуры и докторантуры при высших учебных заведениях и научно-исследовательских организациях, подготовки диссертаций по новой специальности по методам и системам защиты информации и информационной безопасности. Вопросы кадрового обеспечения считают важнейшей составной частью деятельности по обеспечению информационной безопасности и борьбой с преступностью в области компьютерной информации.

КРУГЛЫЙ СТОЛ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ – ИНФОРМАЦИОННАЯ КУЛЬТУРА XXI ВЕКА»

Вус М.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ОБ ИНФОРМАЦИОННОЙ КУЛЬТУРЕ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Многоаспектная проблематика формирования новой информационной культуры общества самым непосредственным образом связана с проблемой обеспечения национальной и информационной безопасности. Новая информационная культура не должна замыкаться только на технико-технологических аспектах информатизации. Для будущего страны важно не только, какие знающие специалисты будут работать в народном хозяйстве, но и какими будут их мировоззрение, гражданская, нравственная позиция. Это, в свою очередь, требует целостной государственной концепции информационного образования, формирования информационной культуры.

1. Автор фундаментальной монографии «Основы информационной грамоты» [В.А. Герасименко, 1996], анализируя задачу целенаправленного изучения и эффективного использования информации в практической деятельности современного общества, выделял в качестве системообразующих понятий информационной грамоты информацию, информатику и информатизацию. В качестве центрального предмета изучения он указал на информацию как «атрибут объективного мира, имеющий теоретическое и практическое значение для современного общества». Высшим, наиболее сложным и многообразным типом информации является социальная информация. Социальную информацию создают люди, они же ответственны за качество создаваемой информации.

Для рыночной экономики информация является одним из видов товара. Это значит, что качество и количество (создаваемой) информации оценивается числом долларов. Авторы философии свободы имеют в виду свободу продажи информации по законам рынка. На это необходимо заметить, что рынок есть инструмент торговли, а не цель прогресса. Научно-технический прогресс в информационной сфере, движимый законами рынка, подобен кораблю, плывущему без руля и без ветрил.

Понятие информатика трактуется в Государственном стандарте высшего профессионального образования как «комплексное научное направление, имеющее междисциплинарный характер, активно содействующее развитию других научных направлений и тем самым выполняющее интеграционную функцию в системе наук». При этом подчеркивается, что воспитание у обучающихся информационной культуры должно включать прежде всего «отчетливое представление роли этой науки в становлении и развитии цивилизации в целом и современной социально-экономической деятельности в частности».

2. Начало второго десятилетия XXI века ознаменовалось качественно новым этапом информационной революции – политизацией. Символом информационного прогресса на рубеже XX-XXI веков стало превращение человека из «Homo sapiens» в «Homo televisionius». Внедрение телевидения в процесс человеческого познания мира – важнейшее событие социальной жизни минувшего века. Вместе с тем телевизионное миропознание ведёт и к чрезмерной виртуальности и к ускоренному росту количества ложной информации. [Л.И. Хромов «Теория информации и теория познания», 2006].

Стремительное развитие глобальных социальных сетей, их сервисов, а также смартфонов и иных мобильных устройств кардинально расширило возможности ведения всех форм информационной работы, в т.ч. информационно-психологической, и информационного противоборства. Сегодня страны с наибольшей численностью населения: «Китай, Индия, Facebook, Google…»! Одновременно с этим систематизация математических моделей информационного влияния и информационного управления в социальных сетях показывает, что они все чаще становятся полем информационных противоборств. Киберпространство все чаще становится территорией «боев без правил», т.к. отсутствует соответствующая юридически обязывающая международно-договорная база. [Смирнов А.И. «Глобальная безопасность и «Мягкая сила 2.0», 2012].

С учетом бурного развития информационно-коммуникационных технологий, веб-сервисов, в том числе глобальных социальных сетей, Генеральная Ассамблея ООН 17 марта 2010 г. приняла резолюцию «Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур».

МОЛОДЕЖНАЯ НАУЧНАЯ ШКОЛА «БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ»

Афанасьев Д.Н., Коваленко М.Е.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

АВТОРСКОЕ ПРАВО В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

«Первым полноценным законом об авторских правах был знаменитый «Статут королевы Анны», вступивший в силу в 1710 году — во времена Петра I и Даниеля Дэфо. Согласно этому закону автор имел особые права на своё произведение в течение 14 лет после выпуска и — если он ещё был жив по истечении этих 14 лет — они могли быть продлены еще на 14 лет. Название закона говорило само за себя — «Акт о поощрении учёности». Подразумевалось, что этот закон поможет авторам и издателям печатать больше книг. В то время, пожалуй, наделение авторов особыми правами было мудрым и верным решением. Однако прошло больше 300 лет — и сейчас, в 2013 году, защита авторских прав уже не выглядит таким однозначно уж достойным делом. Мы живём в эпоху торрентов, видеорегистраторов и электронных книг. И поднимая вопрос об авторских правах, в частности в сфере информационных технологий, нужно считаться со временем, в котором мы живем».

Федеральный закон от 2 июля 2013 года № 187-ФЗ «О внесении изменений в законодательные акты Российской Федерации по вопросам защиты интеллектуальных прав в информационно-телекоммуникационных сетях» призван помочь в борьбе с нарушением авторских прав и распространением нелегального мультимедийного контента в Интернете. Закон устанавливает порядок блокировки сайтов, на которых незаконно размещены «фильмы, в том числе кинофильмы, телефильмы, или информация, необходимая для их получения». Изначально предполагалось, что это коснётся всех видов информации, однако, после внесения поправок, закон будет применяться только для видеопродукции. Авторы законопроекта, которые, по мнению представителей области IT, общаются с интернетом буквально «на вы», не приняли во внимание специфику интернет-среды, например, такое понятие, как связность сети. Дело в том, что в законе прописана возможность блокировать IP-адрес целиком. То есть из-за одной «подозрительной» страницы может быть заблокирован весь полезный и вполне добропорядочный ресурс, не говоря уже о десятках доменов, привязанных к нему.

Как отмечают СМИ, общество разделилось на три лагеря: один из них против, второй — за, третьему — все равно. Чтобы выразить позицию первого лагеря, можно процитировать слова одного из основателей ЗАО «Лаборатория Касперского», Евгения Касперского: «Благое намерение защищать изобретателей патентами — сегодня это превратилось в инструмент вымогательства, цель которого прямо противоположна защите инноваций. Современный патентный бизнес — это технологический рэкет». Что касается противоположного лагеря, имеется в виду мнение правообладателей, то их как оказалось данная ситуация не вполне устраивает, поскольку они борются за ужесточение закона. Юрисконсульт Гильдии продюсеров России Сергей Семенов, например, указывает на один из моментов, по которому его коллеги принципиально не смогут договориться с интернет-индустрией. Это вопрос блокировки конкретных страниц, а не всего сайта. С. Семенов указывает на то, что существуют сайты с неимоверным количеством контента. Поэтому десятки, сотни и даже тысячи заблокированных URL-страниц проблему не решат. На практике URL динамичны, а правообладатели видят своей целью вычистку контента со всего сайта (невзирая на побочные эффекты блокировки по IP). Каждая позиция имеет свои сильные и слабые стороны.

Исследование данной проблематики, обзор мнений обеих сторон, позволит увидеть картину в целом и составить о ней собственное мнение. Это даст возможность в дальнейшем взвешенно подходить к вопросам, касающимся авторских прав в информационной среде, в рамках собственной практики находить обоснованные решения возникающих задач.

Бидайбеков Ж.О.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

РОЛЬ ОТДЕЛА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СТРУКТУРЕ ОРГАНИЗАЦИИ

Информатизация российского бизнеса, многих сфер предпринимательской деятельности (финансы, реклама, торговля и т.п.), внедрение компьютерных технологий управления выдвигают на

первый план проблемы информационной безопасности организации. Весьма актуальной для практики задачей является определение в структуре организации места и функций отдела информационной безопасности. При формировании системы безопасности необходимо четко уяснить, какие задачи перед ней стоят. Структура системы защиты информации предприятия должны охватывать не только электронные информационные системы, а весь управленческий комплекс фирмы.

Отрасль информационной безопасности является весьма молодой, этим определяется дефицит высококвалифицированных профессиональных кадрах. Еще одной причиной, по которой тормозится решение задач обеспечения информационной безопасности на предприятии, часто является недостаток внимания со стороны руководства вследствие недооценки им важности таких задач. Так, например, чтобы решить вопрос приобретения соответствующих специализированных технических и программных средств защиты, необходимо обосновать их необходимость лицам, принимающим решения, которые зачастую не являются специалистами и недостаточно осведомлены в этих вопросах.

Автор данной работы пользовался преимущественно методами эмпирического исследования. В материале докладе использованы и будут обобщены находящиеся в свободном доступе в сети Интернет статистические данные о структурах подразделений и служб информационной безопасности различных предприятий. На этом материале автор попытается показать важную роль отдела информационной безопасности на предприятии. Одним из аспектов доклада будет попытка охарактеризовать влияние политики, проводимой руководством в сфере информационной безопасности на формировании корпоративной культуры безопасности.

Представляется, что сегодня руководитель каждого предприятия сам должен быть в достаточной мере знаком с общими вопросами информационной безопасности. Принять решение об учреждении отдела (службы) информационной безопасности руководитель должен понимать, что это подразделение не будет приносить явной прибыли, но оно призвано защитить от возможных непредвиденных убытков.

Бугаенко И.И.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

О ПРАВОВОМ ИНСТИТУТЕ ГОСУДАРСТВЕННОЙ ТАЙНЫ

Основным источником права в области обеспечения информационной безопасности (ИБ) в России является Конституция Российской Федерации. Помимо Конституции, правовые отношения в области ИБ регулируются федеральными законами, указами и распоряжениями Президента РФ, постановлениями Правительства РФ. В комплексе они составляют правовое поле ИБ РФ.

Одним из важнейших документов правового поля ИБ является Закон Российской Федерации «О государственной тайне» от 21.07.1993 № 5485-1 (ред. от 08.11.2011), с принятия которого два десятилетия назад в России начал свое формирование правовой институт защиты государственной тайны (ГТ). Впервые в истории России вопросы ограничения информационного обмена, связанные с необходимостью обеспечения безопасности государства, стали регулироваться открытым нормативно-правовым актом (НПА). Закон «О государственной тайне» решил многие проблемы, которые были выведены из сферы ведомственных закрытых актов в сферу открытого законодательного регулирования. После его принятия была разработана основная нормативно-правовая база для функционирования механизмов реализации закона. Помимо создания базового законодательства, формировалось новое представление об ответственности за преступления, направленные против безопасности государства. Это, как отмечают специалисты, позволило в определенной мере заполнить сложившийся в 1991 – 1993 гг. правовой вакуум, спровоцированный разрушением старой, действовавшей ранее в стране системы защиты ГТ, и приостановить нанесение ощутимого урона интересам государства.

На основе открытых источников в докладе будет предпринята попытка рассмотрения правового института защиты ГТ, его состояния в современной России. Особое внимание будет уделено вопросам ответственности за преступления направленные против безопасности ГТ, в частности, при ее обороте в форме компьютерной информации.

Важной ступенью в становлении правового института защиты ГТ стало принятие в 1996 г. Уголовного кодекса РФ (УК РФ), сменившего действовавший ранее на территории России Уголовный кодекс Российской Советской Федеративной Социалистической Республики (УК РСФСР), утвержденный еще в 1960 г. Ряд статей, имевшихся ранее в УК РСФСР и предусматривавших ответственность за преступления в сфере защиты ГТ, вошли в УК РФ в измененной диспозиции. Это статьи Главы 29 УК РФ «Преступления против основ конституционного строя и безопасности государства»: 275 – «Государственная измена» (ст. 64 УК РСФСР); 276 – «Шпионаж» (ст. 65 УК РСФСР); 283 – «Разглашение государственной тайны» (ст. 75 УК РСФСР); 284 – «Утрата документов, содержащих государственную тайну» (ст. 76 УК РСФСР). Федеральным законом от 12.11.2012 №190-

ФЗ в УК РФ была введена новая статья: 283^1 – «Незаконное получение сведений, составляющих государственную тайну».

Повсеместная информатизация общества, повышение интенсивности информационного обмена, широкое использование инновационных технологий сбора и обработки информации не могут обойти стороной ни одну область жизнедеятельности государства. Очевидно, что не может являться исключением и правовой институт ГТ. Информация давно перестала существовать только на бумажных носителях и перешла в область компьютерной информации. Не могло не коснуться это и информации, содержащей ГТ.

Если вести речь о сведениях содержащих ГТ и представленных в форме компьютерной информации, то следует учитывать ответственность за их незаконное использование и с позиций норм статьи 272 УК РФ – «Неправомерный доступ к компьютерной информации». Под определение компьютерной информации, содержащееся в данной статье, могут подпадать сведения о ГТ, объекты авторского права, информация о служебной, профессиональной, коммерческой тайне и т.д. Представляется, что в такой ситуации не разграничена ответственность, и не определена степень ущерба (какой ущерб считать крупным) конкретно по каждому из возможных противоправных деяний. В этой связи, по мнению автора, целесообразно было бы расширить диспозицию статьи 272 УК РФ - может быть - посредством введения отдельной нормы о неправомерном доступе к компьютерной информации, содержащей сведения о ГТ.)

Вероятно, разграничение ответственности за неправомерный доступ к компьютерной информации может послужить совершенствованию законодательства о ГТ, а также развитию практики регулирования информационных правоотношений. Представляется, что введение предлагаемой нормы в УК РФ даст возможность более дифференцированно устанавливать наказания за преступления направленные против безопасности ГТ, в зависимости от тяжести таких преступлений.

Васильева Н.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

БЕЗОПАСНОСТЬ УСЛУГ СВЯЗИ

Услуга связи – это современный программный продукт, который обеспечивает доступ к информации для абонента мобильного устройства. Это может быть, например, доступ к SMS-сообщениям, MMS-сообщениям, видеоконференциям, данным личного банковского счета, местоположениям абонентов, календарям мероприятий, контактам, знакомствам, посещаемым сайтам в интернете, балансу, голосованиям и к другой информации. При этом актуальны вопросы безопасности.

В законе «О связи» существует понятие «тайна связи» и «личная информация абонента». Так же согласно закону «О связи» защите подлежит «информация об обращении абонента к услугам связи». Абонентская база оператора подпадает под закон «О персональных данных». В отдельных случаях, и в особенности, если абонентское устройство является частью корпоративной среды, то обрабатываемая информация может подпадать под закон «О коммерческой тайне». Если рассматривать услугу «Мобильный банкинг», то обрабатываемая информация подлежит защите согласно закону «О банковской тайне».

Основными проблемами безопасности услуг связи являются:

– Использование мошенниками методов социальной инженерии в отношении абонентов сотовой связи.

– Недобросовестные действия со стороны обслуживающего персонала.

– Уязвимости и не декларированные возможности в программном обеспечении услуг связи, стандартах передачи данных и мобильных телефонах абонентов.

– Существующие механизмы защиты в сотовых телефонах частично неудобны в использовании, некорректно настроены по умолчанию, иногда отсутствуют.

– Использование незащищенных Интернет-соединений в организации части услуг связи.

– Подключение услуги связи без ведома абонента.

Понимание общей структуры системы связи и моделирование ее отдельных процессов позволит:

– Оценить функциональные возможности, встроенные механизмы защиты и уязвимости каналообразующего и коммутационного оборудования, мобильных устройств и приложений, а так же отдельных решений для реализации услуг связи.

– Оценить необходимость и возможность модернизации встроенных механизмов защиты в системе услуг связи с целью повышения их надежности и эффективности.

– Разработать ряд безопасных приложений для мобильных устройств и, возможно, серверных решений для реализации услуг связи, отвечающих как потребностям рынка, так и требованиям безопасности регулирующих органов.

– Провести проверки на отсутствие не декларированных возможностей в системе услуг связи и оценить работоспособность и перспективы существующих решений.

– Оценить возможности пресечения работы мошенников в сети сотовых операторов, использующих методы социальной инженерии. Оценить существующие решения.

Современная структура услуг связи включает в себя следующие компоненты:

– Каналообразующее оборудование оператора связи – радио часть (2G, 3G, 4G или LTE) и коммутационное оборудование (Nokia, HP, Huawei, NEC и др.)

– Мобильные абонентские устройства с базовой платформой (Android, iOS, Windows Mobile и др.) и каналами доступа (Bluetooth, Модем, Wi-Fi, 2G, 3G, 4G или LTE.)

– Система сервисов оператора связи частично реализована на базе решений от крупных поставщиков коммутационного оборудования, частично использует программные решения от менее крупных российских компаний, например Протей, Беркут, Complete и др.

– Оборудование заказчика услуги. (Заказчиком может выступать банк, телевидение, поисковые системы Яндекс, Google и др.)

– Оборудование аутсорсинговой компании, часть сервисов может быть реализована на оборудовании сторонних IT-компаний, а часть каналов может быть арендована у наземных операторов связи (Ростелеком, Метроком и др.)

– Интернет. Часть услуг использует оператора связи только как оператора абонентской базы.

– Приложения для мобильных устройств. Размещаются в открытом доступе бесплатно или за символическую плату, например, на Google Play (Play Маркет) или App Store, соответственно.

Моделирования услуги «Мобильный банкинг», например, возможно по следующему графу:

Каналообразующее оборудование (OpenBTS) — Мобильное абонентское устройство (на базе Android) — Оборудование заказчика услуги (СЗФ банка «Сбербанк России») — Приложение для мобильного устройства («Мобильный банк»).

Гилёв Г.А., Негодаев К.С.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

К ВОПРОСУ ОБ АУДИТЕ СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В настоящее время возрастает зависимость успешной деятельности компании от эффективности корпоративной системы защиты информации. Это объясняется увеличением объема жизненно важных данных, обрабатываемых в корпоративной информационной системе. Информационные системы усложняются, растет и число уязвимостей обнаруживаемых в них.

Система менеджмента информационной безопасности должна обеспечивать эффективное управление обеспечением информационной безопасности: отсутствие неприемлемых рисков со стороны информационных систем для организации и поддержание баланса между рисками и затратами на обеспечение информационной безопасности. Аудит системы менеджмента информационной безопасности должен позволить оценить текущее состояние безопасности функционирования корпоративной информационной системы, оценить и спрогнозировать риски, управлять их влиянием на бизнес-процессы компании.

В настоящий момент услуга аудита системы менеджмента информационной системы предлагается многими отечественными и международными компаниями. По имеющимся публикациям и рекламным объявлениям в некоторых компаниях введена практика, когда все специалисты делятся на две группы: группу аудита и группу технических специалистов. В ходе проведения работ у клиента, группа аудита проверяет соответствие системы менеджмента информационной безопасности стандарту ISO 27001, а технические специалисты, используя сетевые сканеры уязвимостей и специально подготовленные скрипты, ищут уязвимости в операционных системах, системах управления базами данных и настройках сетевого оборудования. Итоговый отчет с рекомендациями состоит из двух отдельных частей — требований ISO 27001 и рекомендаций по устранению технических уязвимостей. Страны Евросоюза и США давно занимаются решением проблемы управления рисками связанными с информационной безопасностью. В России процесс создания законодательной базы по построению систем менеджмента информационной безопасности находится в начальной стадии развития. В настоящий момент в России адаптированы только два международных стандарта, а эффективные методики проведения аудита систем менеджмента информационной безопасности отсутствуют.

В работе предполагается:

– Провести анализ требований законов и нормативных правовых актов, регламентирующих проведение аудита системы менеджмента информационной безопасности;

– Рассмотреть основные этапы создания системы менеджмента информационной безопасности на основании требований стандарта ISO 27001;

– Проанализировать сам процесс проведения аудита информационной безопасности.

Итогом работы должен стать обзор методики проведения аудита системы менеджмента информационной безопасности.

Годжиев А.А., Тарасов С.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

АВТОРСКОЕ ПРАВО И ПРОГРАММНЫЕ ПРОДУКТЫ

В век электронных технологий вопросы, связанные с авторским правом, стали актуальными как никогда. Эти вопросы часто становятся предметом споров различных субъектов права. Причины повышенного внимания к такой проблеме вполне очевидны — от определения авторства зависят права на интеллектуальную собственность, а так же прибыль правообладателя. Для нашей страны проблемы интеллектуальной собственности также являются актуальными, вместе с тем правовая культура общества в этих вопросах находится на достаточно низком уровне.

Одним из наиболее ходовых и ценных объектов интеллектуальной собственности являются программные продукты. Однако программные продукты подвержены кражам и нуждаются в защите. На практике не редки случаи, когда программные продукты распространяются и используются противоправными способами.

В настоящее время можно использовать пять основных правовых механизмов защиты программного обеспечения: авторское право, патентное право, институт тайн, договорное право, морально-этические методы противодействия недобросовестной конкуренции. Два наиболее разработанных правовых механизма – это авторское и патентное право. Правовая охрана осуществляется посредством патентов и лицензий.

Так как программные продукты являются уникальными объектами защиты, то традиционные способы защиты авторских прав к ним не подходят. Адаптация таких способов защиты авторских прав под программное обеспечение, к сожалению, оставляет желать лучшего. Патент предоставляет абсолютную монополию, но реализация патентования программных продуктов далеко не проста.

В докладе будут рассмотрены различия между проприетарным программным обеспечением и программным обеспечением с открытым кодом, особенности их лицензирования. Акценты будут сделаны на особенностях законодательства и применения норм авторского права в разных странах.

Гончарова Ю.С., Соляной Т.С.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

ОБ ИНФОРМАЦИОННЫХ ВОЙНАХ

Современный этап развития человеческой цивилизации характеризуется использованием большого количества информационных технологий во всех аспектах жизни общества. В наше время в мире сложно найти области жизнедеятельности, развитие которых не было бы связано с использованием таких технологий. Именно этот факт делает информацию крайне важным «ресурсом» как для государства, так и отдельного человека или организации, что, в свою очередь, делает информацию основным аспектом любого конфликта.

Выделить информацию как способ (орудие) ведения войны пытались давно, но только сравнительно недавно начали появляться теории, которые могут быть положены в основу методологии ведения информационных войн. Благодаря этому появилось новое поле для противоборства на всех уровнях жизни общества, а именно глобальное информационное поле. На этом глобальном поле более сильные в информационном плане государства осуществляют противоборство со слабыми противниками. Информационная война позволяет оказывать существенное воздействие на различные процессы практически на всех уровнях государственного и общественного устройства в любой стране.

В современном мире рядом стран информационная война рассматривается как эффективный способ реализации внешней политики. Поэтому многие страны мира работают над созданием эффективной системы государственного противодействия операциям информационной войны.

Авторами предполагается рассмотрение феномена «информационная война» и прецедентов её реализации в современном мире. В нынешних условиях данная тема весьма актуальна.

Сегодня в мире можно наблюдать процесс глобальной информатизации, приведший к созданию глобального информационного поля. У этого процесса много положительных моментов, но присутствуют и серьезные проблемные аспекты. Прежде всего, это относится к сфере информационной безопасности, к возможностям предотвращения информационных войн. Распространение Интернета расширило возможности ведения информационных войн.

В работе предполагается провести реферативный обзор по тематике «информационных войн», особо уделив внимание используемому в публикациях на эту тему понятийному аппарату.

Понятия информационных и психологических операций будут анализироваться совместно, так как проблема информационных войн не может рассматриваться в рамках одной дисциплины, и носит междисциплинарный характер.

Григорьян К.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

РАЗРАБОТКА МЕТОДА ПОЛУЧЕНИЯ СИГНАТУР ИСПОЛНЯЕМЫХ ФАЙЛОВ

В современном мире, как негативное следствие колоссального технического прогресса, наблюдается тенденция увеличения числа преступлений с использованием компьютерной техники. Соответственно повышаются требования к анализу состояния и уровню обеспечения безопасности информационных процессов и информационных потоков, протекающих в данной среде.

Наиболее сложным направлением при исследовании безопасности применения компьютерной техники является исследование содержимого носителей информации. Сама по себе техника (по своей сути) практически одинакова, во многом стандартизована. Технические стандарты обеспечения надежности компьютерной техники сравнительно хорошо разработаны.

Назначение и способы организации работы компьютерной техники определяются установленным программным обеспечением и содержимым носителей информации. Для практики достаточно актуальна проблема анализа содержания файлов, записанных на различных носителях.

Задачей данной исследовательской работы является выработка наилучшего метода получения сигнатур исполняемых файлов с последующей классификацией их с целью реализации в прикладном программном обеспечении. Это необходимо в целях ускорения процесса проведения криминалистических исследований файлов на носителях информации.

В операционных системах семейства Windows данная задача решается достаточно легко – от каждого скомпилированного исполняемого файла можно взять контрольную сумму (например, MD5) и сравнить её с исходной. В операционных системах, основанных на ядре Linux, такая методика анализа файлов не эффективна, так как под каждую операционную систему файл компилируется заново, что кардинально меняет его контрольную сумму и не позволяет однозначно идентифицировать его при исследовании. Этот факт не позволяет использовать указанную простую методику.

Преследуя цель разработки способа получения сигнатур исполняемых файлов, обратимся к технологии «кусочного хеширования». Суть данной технологии заключается в том, что изначально скомпилированный исполняемый файл декомпилируется (преобразуется в машинный код, который интерпретируется в языке Assembler), затем происходит разбор полученного кода на части, в соответствии со структурой исполняемого файла (программный и секционный заголовки, данные, сегменты). После этого, при помощи хэш-функций (например, SHA, MD4, MD5) могут быть получены контрольные суммы N строк декомпилированного файла, которые заносятся в базу данных (хранилище) для последующего сравнения с другими, аналогично обработанными исполняемыми файлами.

Таким методом исследуются разные версии приложений, утилит и выявляются схожие части, которые помечаются как типичные для этого вида исполняемых файлов (сигнатуры). Может быть также исследовано и найдено оптимальное число N для получения качественного анализа на сигнатуры.

В перспективном плане работы, при успешном тестировании метода, планируется создать прикладное программное обеспечение, которое позволит использовать разработанную методику для получения сигнатур исполняемых файлов, для последующей классификации файлов на носителях информации по категориям критичности.

Дранник А.Л.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

ИСПОЛЬЗОВАНИЕ ПРОГРАММ-СИМУЛЯТОРОВ ПОВЕДЕНИЯ РОЕВЫХ РОБОТОТЕХНИЧЕСКИХ СИСТЕМ ДЛЯ ИССЛЕДОВАНИЯ ВОПРОСОВ БЕЗОПАСНОСТИ

Робототехнические системы «роевого» типа в настоящий момент активно разрабатываются и широко исследуются в отечественной и мировой научной практике. Ожидается, что роевой, распределённый подход к созданию искусственного интеллекта автономных систем позволит решать большой комплекс задач в сферах охраны окружающей среды, медицины, клининга, наблюдения и многих других. В этой связи актуальным становится вопрос проектирования и тестирования робототехнических систем «роевого» типа с точки зрения безопасности.

Новизна и дороговизна испытательных технологий обуславливают отсутствие широкой информационной базы о практических случаях поведения робототехнических устройств. Для всех видов робототехники на сегодняшний день заметен запрос на создание своего рода «испытательных стендов», программ и алгоритмов моделирования, которые позволят как осуществлять разработку безопасных систем и функций, так и осуществлять тестовую контрольную проверку планируемых к выпуску устройств.

Целью данной работы является рассмотрение существующих программ моделирования поведения роевых роботов с точки зрения возможностей применения для исследования вопросов безопасности.

Как и в общем случае программного моделирования, «проигрывание» поведения роботов и потенциальных угроз в программе-симуляторе дает возможность увидеть не только единичные варианты возможного развития событий, но и просчитать максимально широкий спектр возможных путей изменения состояния робототехнической системы и выявить при этом небезопасные состояния.

Все широко известные проекты роевой робототехники, как правило, разрабатывают собственные или адаптируют универсальные программы-симуляторы для компьютерного воспроизведения деятельности своих устройств. Большинство из этих программ открыто для исследовательского сообщества, в том числе имеются и свободно распространяемые, разрешенные для дальнейшего изменения и развития и т.п. Очевидными признаками для классификации данных программ являются вид платформы, визуальные возможности 2 или 3D эмуляции, требования к системным ресурсам и операционной системе, поддерживаемые типы каналов коммуникации моделируемых устройств, пределы расширения количества участников «роя», коммерческие и авторские аспекты применения и т.п.

Практика показывает, что исследования в сфере безопасности могут выдвигать дополнительные требования к программам-симуляторам. Такие требования представляется необходимым определить в настоящей работе. Это могут быть, например, более широкие возможности моделирования окружающей среды (которая для исследовательских нужд прогнозируется как потенциально враждебная), возможности корректировки программных задач роботов-участников и вмешательства в коммуникационные связи внутри «роя» для моделирования возможных атак и т.п. В таком контексте выбор программы определяется конкретными задачами, которые ставятся для исследования.

По результатам сравнения имеющихся программ весьма интересным для решения широкого спектра задач представляется программный продукт V-REP швейцарской корпорации K-Team, производителя оборудования для известных проектов Kilobot, Khepera и др. Среди преимуществ симулятора: свободный исследовательский доступ, открытые возможности расширения функций, как самой программы, так и моделируемых устройств, широкая кросс-платформенность, мощная 3D-среда визуализации. Программа дает возможности создания среды с заданными условиями (в том числе с моделированием особенностей рельефа, добавлением предметов, включением людей), возможности управления такими характеристиками, как освещенность, дальность сигналов коммуникации и т.п., что делает ее применимой для моделирования процессов, актуальных с точки зрения безопасности.

Ендовский А.С.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

МЕТОДЫ РАСЧЕТА РИСКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Система управления рисками информационной безопасности является необходимой на всех этапах работы комплекса защиты информации. При этом управлять рисками невозможно предварительно их не оценив, что в свою очередь должно быть произведено по какой-либо методике. Для выполнения качественной оценки рисков информационной безопасности используется таблица соответствия степени тяжести последствий и вероятности реализации угрозы.

Целью работы является вывод формулы для расчета риска информационной безопасности, позволяющей получить массив значений актуальных рисков и оценить потери в денежном эквиваленте. На этапе оценки рисков наибольший интерес представляют методики, применяемые формулы и входные данные для расчета значения риска.

В классическом виде риск информационной безопасности определяется как функция трёх переменных: вероятность существования угрозы, вероятность существования уязвимости (незащищенности) и потенциальное воздействие. Если любая из этих переменных приближается к нулю, полный риск так же стремится к нулю.

Расчет риска должен производиться с использованием значения угроз и ценность актива. Существенным недостатком многих методик является оценка стоимости активов (размера ущерба) в виде условных значений. Условные значения не имеют единиц измерения применимых в практике, в частности не являются денежным эквивалентом. В итоге это не дает реального представления уровня риска, который возможно перенести на реальные активы объекта защиты.

На первом этапе работы было проанализировано несколько различных методов расчета риска и выработана собственная методика. Предлагается разделить процедуру расчета риска на два этапа: вычисление значения технического риска и вычисление величины потенциального ущерба. Под техническим риском при этом понимается значение риска информационной безопасности состоящего из вероятностей реализации угроз и использования уязвимостей каждого компонента информационной инфраструктуры с учётом уровня их конфиденциальности, целостности и доступности.

Применение такого алгоритма позволит произвести более детальную оценку риска, получив на выходе безразмерное значение вероятности возникновения риска компрометации каждого информационного актива, в отдельности. В последующем будет возможно вычисление значения

ущерба; для чего используется усредненное значение риска каждого информационного актива и размер потенциальных потерь. Предлагаемая методика позволит корректно оценить значение риска информационной безопасности и скалькулировать денежные потери в случае возникновения инцидентов безопасности.

Каторин Ю.Ф., Коржук В.М.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

АНАЛИЗ ВОЗМОЖНОСТЕЙ ТСР ПО ПЕРЕХВАТУ ИНФОРМАЦИИ В СЕТЯХ СОТОВОЙ ЦИФРОВОЙ СВЯЗИ

Традиционные аналоговые системы сотовой связи, хотя и могут создавать определенные трудности для радиоразведки, не считаются особенно сложными для перехвата противником. В таких сетях электронный перехват сотовой связи не только легко осуществить, он, к тому же, не требует больших затрат на аппаратуру, и его почти невозможно обнаружить. Более серьезные трудности вызывает предстоящий массовый переход на цифровые системы. Хотя системы сотовой цифровой радиосвязи работают в том же диапазоне радиочастот, что и традиционные аналоговые системы, в них применяются более сложные сигналы и, самое главное, они имеют встроенные средства защиты информации, например, криптографические.

Три действующих стандарта на системы цифровой сотовой радиосвязи предусматривают применение многократного доступа с временным разделением TDMA, означающего возможность одновременной передачи трех разговоров по одному каналу с последовательным разделением их передачи во времени (что эквивалентно одному вызову). Это в три раза затрудняет ведение радиоразведки. Другой стандарт цифровой сотовой радиосвязи с использованием многократного доступа с кодовым разделением CDMA дает возможность применения техники широкополосных систем с малой вероятностью обнаружения сигналов. Практически никакие другие системы связи не представляют таких трудностей для ведения радиоразведки, как широкополосные.

В докладе проанализированы основные методы перехвата информации в сетях сотовой цифровой связи и сделан вывод, что существующая система перехвата работает с любым типом кодирования, включая алгоритмы A5/1 и A5/2. Хотя цифровые сотовые телефоны, передающие информацию в виде цифрового кода, более совершенны с точки зрения защиты информации, однако и используемый в них алгоритм шифрования Cellular Message Encryption Algorithm (CMEA) может быть вскрыт опытным специалистом в течение нескольких минут с помощью персонального компьютера. Таким образом, современное состояние ТСР позволяет обеспечить быстрый и надежный перехват. Это рождает запрос на создания помех для трафика GSM сигналов, а так же запрос на разработку средств защиты для работы оффлайн. Система перехвата, дешифровки, обработки и мониторинга GSM сигналов полностью пассивная. Алгоритмы защиты сотовой связи, берущие свои истоки в 1980-х годов в настоящее время не могут обеспечить полной конфиденциальности переговоров.

Коваленко М.Е., Слепцова Д.М.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

КЛАВИАТУРНЫЙ ПОЧЕРК КАК СРЕДСТВО ВСПОМОГАТЕЛЬНОЙ АУТЕНТИФИКАЦИИ

Эффективное управление предприятием складывается из многих составляющих. Одно из немаловажных мест занимает защита информации предприятия от несанкционированного доступа.

Со времен появления мультипользовательских систем стала весьма актуальной задача аутентификации пользователя. Особое место в инструментарии решения этой задачи занимают биометрические методы, которые основываются на уникальности биометрической информации, носителем которой является человек. На основе этого разработаны различные методы аутентификации пользователей. В их основу положено распознавание пользователя по структуре лица, сетчатке глаз, форме и особенностям ладони, а также особенностям речи и подписи. Сегодня, в силу высокой стоимости, область применения таких методов ограничена информационными системами, в которых несанкционированный доступ может быть сопряжен со значительными финансовыми потерями.

Существует практическая потребность в разработке простых и недорогих способов идентификации пользователя. Одним из таких способов является применение методики аутентификации, основанной на анализе особенностей ввода текста с клавиатуры.

При работе с компьютером прослеживается индивидуальность пользователя, которая проявляется в скорости набора символов, привычки использовать основную или дополнительную часть клавиатуры, характере «сдвоенных» и «строенных» нажатий клавиш, в излюбленных приемах управления компьютером и т. д. Одна из достаточно сложных задач, повседневно решаемых многими людьми, — быстрый набор текстов с клавиатуры компьютера. Обычно быстрого клавиатурного ввода информации удается достичь за счет использования всех пальцев обеих рук. При этом у каждого

человека проявляется свой уникальный клавиатурный почерк. Физиологические особенности, например такие, как папиллярный узор пальца, геометрия ладони или рисунок радужной оболочки глаза, являются постоянными физическими характеристиками человека. Поведенческие же характеристики, такие, как подпись, голос и клавиатурный почерк, находятся под влиянием как управляемых действий, так и менее управляемых психологических факторов.

Как же можно выявить индивидуальные особенности клавиатурного почерка? Аналогично тому, как и при графологической экспертизе: нужны эталонный и исследуемый образцы текста. Лучше, если их содержание будет одинаковым — так называемая парольная или ключевая фраза. Разумеется, по двум-трем, даже по десяти нажатым клавишам отличить пользователя невозможно. Нужна статистика.

Планируется провести исследование, направленное на выявление зависимости результата от изменения характера эксперимента, например: изменение длины ключевой фразы, время и состояние испытуемого, зависимость скорости ввода слов от их смысла (химик быстрее наберет «водород», «соединение», чем «программа» или «экскаватор»). Сбор биометрической информации о работе пользователя при анализе клавиатурного почерка будет производится посредством замеров интервалов между нажатиями клавиш и времени их удержаний, после чего полученные результаты формируются в матрицу межсимвольных интервалов и вектор времен удержаний клавиш.

В основу эксперимента предполагается положить три метода аутентификации пользователя по клавиатурному почерку:

- метод, основанный на определении общего расстояния;
- метод, основанный на тесте Колмогорова-Смирнова;
- метод, основанный на определении количества ошибок.

Представляется, что и данный метод аутентификации целесообразно будет использовать, лишь при работе с особо ценной информацией. Скорее всего, бухгалтер, от которого потребуется ввести две страницы текста, просто для того, чтобы подтвердить, что перед ним действительно нужное лицо, будет всячески стараться избегать такой системы идентификации. А оператор, работающий с секретами, может работать с такой программой целый день, время от времени отлучаясь от компьютера. А чтобы в этот момент злоумышленники не воспользовались небрежно оставленной в открытом состояние системой, программа будет периодически проводить «скрытый мониторинг» и «негласную проверку». Такая система позволит постоянно контролировать, законный ли пользователь сидит за компьютером. Заметим так же, что при использовании описываемых методов появляется возможность не только подтвердить подлинность лица, но и оценить его психо-физиологическое состояние.

Представляется, что рассматриваемый метод аутентификации пользователя имеет определенные плюсы, такие, например, как простота реализации и внедрения. Реализация (исключительно программная) не потребует от пользователя никаких иных, кроме привычных действий. Возможна скрытая аутентификации. Результат, при определенных условиях, не будет зависеть от психофизического состояния оператора.

Коваль Е.Н.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

РАЗРАБОТКА И ПРИМЕНЕНИЕ МУЛЬТИАГЕНТНЫХ СИСТЕМ

Если мы обратимся к определению из Википедии, то «Многоагентная система» (MAS, англ. Multi-agent system) — это система, образованная несколькими взаимодействующими интеллектуальными агентами. Многоагентные системы могут быть использованы для решения таких проблем, которые сложно или невозможно решить с помощью одного агента или монолитной системы (англ.). Иными словами мультиагентные системы (МАС) это такие информационные системы (ИС), которые объединяют множество других ИС. Они взаимодействуют между собой, влияют друг на друга исполняемыми процессами и взаимосвязанными функциями и увеличивают рост различных, в том числе и новых, атакующих воздействий нарушения целостности, доступности и конфиденциальности информации, распределенных как в пространстве так и во времени.

Разработка МАС включает две основные задачи. Первая – создание агента, вторая – создание «общества» агентов, т.е. включение в систему механизмов взаимодействия агентов. Агентом принято считать информационную (компьютерную) систему, способную выполнять возложенные на нее обязанности, включающие восприятие, принятие решения и осуществление некоторого действия, без вмешательства оператора в течение длительного времени либо полностью автономно в некоторой среде. МАС представляет собой комплекс, включающий множество агентов и инфраструктуру, обеспечивающую их взаимодействие.

Обычно МАС является открытой для внедрения новых агентов и не имеет централизованного управления, поэтому агенты могут преследовать как общие, так и различные цели. Агенты могут быть независимыми, либо представлять собой иерархию, в которой каждому агенту отведена некоторая роль. Наиболее распространен подход, когда управлением группой агентов занимается специальный агент известный как когнитивный агент.

Любой агент может быть описан путем задания отображения, представляющего собой таблицу действий, которые он выполняет в ответ на некоторую последовательность событий и условий. В качестве программного средства реализации этого отображения может быть использована «Система на базе правил», которая хранит множество правил, представленных в формате «если <условие> то <действие>». Такие агенты принято называть «простыми рефлексными».

Основной формой организации взаимодействия между агентами является кооперация, предполагающая сотрудничество, координацию совместных действий и разрешение возникающих конфликтов. МАС должна предоставлять такие механизмы взаимодействия, чтобы они были независимы от вида агентов. Эта проблема может быть решена путем использования стандартного языка запросов и представления знаний. Проводившиеся исследования по созданию модели сложных радио- и робототехнических систем показали, что модели целесообразно строить на основе мультиагентных систем, что позволяет обеспечить работу модели в реальном масштабе времени и ее высокую эффективность.

Если говорить о применении, то теория МАС используется в составных системах обороны. Также МАС применяются на транспорте, в логистике, графике, в геоинформационных системах и во многих других приложениях. МАС хорошо зарекомендовали себя в сфере сетевых и мобильных технологий, для обеспечения автоматического и динамического баланса нагруженности, расширяемости и способности к самовосстановлению. Мультиагентные системы применяются в нашей жизни в графических приложениях, например, в компьютерных играх. Агентные системы также были использованы в фильмах. Применение МАС в различных сферах деятельности обуславливает необходимость формализации выдвигаемых к ним технических требований на этапах разработки, внедрения, эксплуатации.

При рассмотрении МАС в совокупности с их возможными применения, довольно часто встречается ситуация, когда на ранних этапах жизненного цикла разработчики уделяют недостаточно внимания вопросам информационной безопасности (ИБ), что может приводить к пересмотру всей архитектуры системы. Вследствие этого требуется оценка различных аспектов ИБ, необходимых в ходе решения технических и технологических задач. Требования к построению профиля защиты определяются исходя из наличия самих и особенностей информационных систем.

Козлова Е.В.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

ИСПОЛЬЗОВАНИЕ МЕТОДА МНОГОМЕРНОГО ШКАЛИРОВАНИЯ В ОЦЕНКЕ СТЕПЕНИ ЗАЩИЩЕННОСТИ РОБОТОТЕХНИЧЕСКИХ СИСТЕМ

В настоящее время существует множество робототехнических систем, организованных по различной логике управления и самоуправления. Одним из направлений робототехники, которому уделяется всё большее внимание, является групповая робототехника.

Объектами исследования для целей настоящей работы будут являться мультиагентные системы управления робототехническими комплексами. Примером таких систем могут служить имитационные модели, эволюционные методы, генетические алгоритмы и т.д. Характер взаимодействия агентов в таких системах зачастую даёт злоумышленнику возможность вмешательства в их работу. Это происходит в связи с организацией командной работы вне контролируемой зоны.

Осознание необходимости исследования вопросов информационной безопасности, а также качественное описание основных угроз и особенностей их реализации применительно к робототехническим комплексам были сформулированы лишь несколько лет назад. Вопрос безопасности функционирования таких систем является, на наш взгляд, ключевым в процессе их практической реализации. В этой связи возникает проблема выбора такого алгоритма, который способен не только функционально осуществить задачу, но и предоставить надежный, достоверный, оптимальный по затратам и использованию ресурсов результат. Для решения данной проблемы нужна, прежде всего, первичная оценка алгоритмов на степень защищенности системы от воздействия злоумышленника и использования имеющихся уязвимостей.

В данной работе предлагается использовать математический аппарат, позволяющий соотнести робототехнические системы с точки зрения их безопасности. В качестве такого аппарата будет использован метод многомерного шкалирования, который широко применяется в таких сферах науки, как социология, экономика и т.д.

Этот метод позволяет располагать точки, соответствующие изучаемым объектам, в некотором многомерном «признаковом» пространстве. На входе будет использована матрица, элементы которой на пересечении i-й строки и j-го столбца, содержит сведения о по парном сходстве анализируемых объектов (в данном случае, алгоритмов и показателей уровня защищенности по выбранному массиву признаков). На выходе предполагается получить числовые значения координат, которые приписываются каждому алгоритму в некоторой новой системе координат, что позволит получить

картину полученных результатов и приступить к оценке изученных алгоритмов с точки зрения уровня их безопасности.

Для реализации используемого метода предполагается решение следующих задач:

1) Выбор алгоритмов, являющихся объектами данного исследования.

2) Выбор классификационных признаков (уязвимость, угрозы информационной безопасности), по которым будет производиться ранжирование объектов.

3) Численная интерпретация классификационных признаков для каждой из систем.

4) Формирование исходной матрицы данных и применение математического аппарата для получения сведений о по парном сходстве анализируемых объектов.

5) Визуализация результатов в новой системе координат.

В результате проведенного исследования должна осуществиться сегментация изученных алгоритмов по уровням их защищенности. В дальнейшем предполагается кластеризация полученных данных с целью выделения групп алгоритмов с различной степенью защищенности. Это позволит выявить алгоритмические уязвимости робототехнических комплексов и обобщить в дальнейшем необходимые меры по защите таких систем.

Комаров К.Ю., Судаков А.М.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

О СИСТЕМЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНАХ ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ САНКТ-ПЕТЕРБУРГА

В современном мире любое государство действует в защиту собственных интересов. Несомненно, что одним из наиболее важных аспектов подобной деятельности является обеспечение информационной безопасности на государственном уровне. Но успешное решение такой задачи невозможно без реализации слаженной системы обеспечения информационной безопасности государства и его субъектов.

Предметом данной работы будет ознакомление (в рамках производственной практики) с элементами системы обеспечения информационной безопасности в органах исполнительной власти. В качестве желаемой цели ставится задача анализа существующей нормативно-правовой базы, формирование общих представлений о деятельности государства и его субъектов, направленной на обеспечение информационной безопасности, а так же прогнозирование и анализ возможных модельных ситуаций. На этой основе могут быть выработаны предложения и рекомендации, нацеленные на улучшение взаимодействия государства и региональных органов власти в представленной области.

В качестве источников могут быть использованы материалы публикаций, архивные документы. При возможности предполагается провести интервьюирование представителей органов исполнительной власти с целью понять основные проблемы в сфере информатизации и информационной безопасности управленческих структур. Помимо вышеперечисленных источников предполагается ознакомление с историческими материалами, чтобы проследить процесс становления системы информационной безопасности, а также с конкретными прецедентами, возникавшими в рассматриваемой области.

Итогом задуманной работы должно стать формирование общих представлений об устройстве системы информационной безопасности органов исполнительной власти города Санкт-Петербурга, а также представлений о существующих проблемах в развитии и совершенствовании системы информационной безопасности.

Кузьмин И.Г.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

МОДЕЛЬ ОБЕСПЕЧЕНИЯ ДОКАЗУЕМОЙ ЦЕЛОСТНОСТИ И ДОСТУПНОСТИ ДАННЫХ, РАЗМЕЩЕННЫХ В УДАЛЁННОЙ РАСПРЕДЕЛЁННОЙ СИСТЕМЕ

С развитием мобильных технологий, модель систем, в которых относительно непроизводительные устройства используют ресурсы «тяжелых» удаленных серверов по средствам открытых каналов связи, получила широкое распространение. Среди всего множества распределенных сервисов, в первую очередь, интерес представляют облачные хранилища данных.

Одной из первых организаций добившейся здесь определенных успехов была Amazon со своим сервисом Simple Storage Service (3S), запущенном ею в марте 2006 г. и пользующимся большим спросом по настоящее время. Коммерческий успех стал катализатором запуска множества схожих сервисов других компаний, таких как: Rackspace (2006), «Calibre Communications» FlexiScale (2007), Dropbox (2008), Windows Azure (2010), Google Drive и Яндек Диск (2012) и другие. (Справедливости ради стоит отметить и сервис Briefcase Yahoo, появившийся еще в августе 1999 г., но прекративший свое существование в марте 2009 г, так и не заняв соответствующую нишу на рынке.)

Несмотря на все свои преимущества, использование внешних ресурсов, порождает ряд проблем, связанных с обеспечением надежности, доступности и безопасности в целом. Тем самым открывая обширное поле для исследований в области информационной безопасности.

За последние семь – восемь лет было опубликовано множество работ, покрывающее основные аспекты построения безопасных систем распределённого характера. Главной целью ранних из них, было обеспечить аутентификацию и целостность данных при их хранении, то есть – как эффективно удостовериться в том, что сервер в ответ на запрос клиента возвращает корректные данные. Более поздние исследования были сосредоточены на аутсорсинге зашифрованных данных и связанных с этим проблемах. Еще более поздние исследования были сосредоточены на проблеме доказуемого хранения данных (Provable Data Possession — PDP) в некоторых литературных источниках так же называемой, проверкой доступности данных (Proof of Data Retrivability — POR). (По своей сути – это немного отличающиеся подходы, но нацеленные на решение одной и той же задачи.)

Основной идеей PDP является обеспечение возможности пользователю эффективно, с высокой периодичностью и безопасно производить проверку того, что сервер, размещающий у себя массивы данных клиента, не жульничает. В данном контексте под жульничеством понимается удаление части данных или размещение не всех данных на быстрых носителях.

Фактически мы постарались обобщить наиболее удачные из предложенных ранее подходов, для построения модели масштабируемой, распределённой системы хранения данных, обеспечивающей необходимые характеристики безопасности с доказуемой надежностью. Ключевые концепции модели были реализованы в конкретных алгоритмах. Это позволило оценить количественные характеристики производительности и потери ресурсов на обеспечение требуемых характеристик безопасности.

Дальнейшая проводимая работа направлена на оптимизацию ключевых криптографических примитивов (применяемые линейные корректирующие коды, возможность их агрегирования, контрольные суммы, являющиеся частью кода, и т.д.).

Кузьмич П.А., Пантюхин И.С., Швед Д.В.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

ПРИНЯТИЕ УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ В СИСТЕМАХ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА

Эффективность функционирования сложных систем и систем защиты информации ограниченного доступа (ИОД) в организации, зависит от сбалансированности и качества принимаемых в ней решений (управляющих воздействий). Под защитой ИОД понимается комплекс работ направленных на выполнение мероприятий по технической защите информации (ТЗИ).

В докладе предлагается методический подход к реализации процесса подготовки и обоснования решений на основе анализа стандартных ситуаций, возникающих в деятельности руководителей организации и специалистов по ТЗИ в повседневной деятельности.

Предлагается следующий алгоритм принятия решений.

На первом шаге фиксируются отклонения отдельных показателей процесса защиты ИОД от требуемых значений. При этом причины отклонения известны, а средства достижения требуемых значений заранее не определены. Такое состояние в управлении защитой ИОД предлагается понимать как стандартная ситуация.

Требуется оценить сложившуюся ситуацию, предложить альтернативные решения, выбрать и обосновать оптимальное (рациональное) решение.

Таким образом, задача комплексной оценки состояния защиты ИОД в организации в общем случае заключается в определении соответствия фактического состояния системы защиты ИОД предъявляемым требованиям и выработке решения на приведение системы в соответствие требованиям нормативных правовых актов и нормативных документов в области защиты ИОД.

Люберт А.С.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

МЕТОД ОПРЕДЕЛЕНИЯ ДВИЖЕНИЯ ОБЪЕКТОВ В ВИДЕОПОТОКЕ НА ОСНОВЕ АНАЛИЗА ВРЕМЕННЫХ РЯДОВ

В докладе обсуждается предложенный метод для решения задачи определения движения объектов в видео-потоке систем видеонаблюдения, а также их классификации. Предложен подход для преобразования статистических данных видеокадра во временной ряд для последующего анализа. Рассматривается реализация способа определения наличия движения, а также классификации объектов в видео-потоке с описанием алгоритмов работы на каждом этапе обработки.

В отличие от стандартных методов, использующих анализ изображений видеокадров, метод, предложенный в работе, использует статистические данные кадра для построения числового ряда, характеризующего изменение сцены во времени. Получаемый временной ряд впоследствии

раскладывается с помощью математического аппарата, представленного методом «Гусеница-SSA», на отдельные компоненты и анализируется на предмет наличия определенных характерных изменений сигнала. Метод «Гусеница-SSA» был выбран как универсальный метод общего назначения, не требующий предварительного задания модели ряда, а также решающий задачи разложения ряда на сумму интерпретируемых компонент, таких как тренд, периодические компоненты и шум.

В качестве исходных статистических данных видеокадра для построения временного ряда были выбраны следующие величины: сумма компонент яркости точек изображения и количество точек изображения, представляющих передний план сцены. Под передним планом (foreground) сцены понимается отличная от фона область изображения видеокадра. В приведенном методе используются методы разделения переднего плана и фона из библиотеки компьютерного зрения OpenCV. Для получения наилучших результатов анализа, перед получением статистических данных к видеокадру могут применяться различные фильтры сглаживания, а также морфологические преобразования. В случае использования метода в условиях недостаточной освещенности, для повышения точности составления временного ряда может применяться эквализация изображения.

Основной принцип работы предлагаемой методики заключается в использовании метода «Гусеница-SSA» для анализа временного ряда, полученного из статистических данных кадров видео-потока. Анализ временного ряда включает в себя следующие шаги: перевод исходного временного ряда координат в траекторную матрицу, сингулярное разложение траекторной матрицы, группировка элементарных матриц, полученных в результате разложения, и диагональное усреднение элементов для получения разложения исходного ряда. В результате анализа из временного ряда извлекается низкочастотная составляющая (тренд), периодические колебания и шум.

В силу периодичности, а также при наличии отчетливых фаз движения человека (и подобных объектов), а именно движения и изменения освещенности отдельных конечностей, в предложенном методике с целью определения движения используется анализ периодических колебаний. Наличие движения определяется появлением периодического колебания с частотой в диапазоне, заданном с учетом конфигурации сцены, расстоянием от устройства видеонаблюдения и другими параметрами. Выход характеристик колебаний (частота, амплитуда) за установленный диапазон может трактоваться как внештатная ситуация – бег, резкое приближение к устройству видеонаблюдения. При наличии обучающей выборки возможна классификация объектов по характеристикам колебаний движения. Определение нескольких движущихся объектов возможно в случае правильного разложения временного ряда на независимые периодические составляющая.

Реализация алгоритма представлена в виде приложения, выполняющего обработку заданного видео-потока, построение временного ряда, а также разложение ряда на составные компоненты с визуальным отображением каждого этапа анализа. В настоящее время проводятся исследования, направленные на повышение качества анализа, подбор наиболее оптимальных параметров алгоритма SSA для получения наилучшего разложения временного ряда, а также апробация дополнительных методов обработки видеоизображений.

Масленников О.С., Егоров В.В.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

ПЕРСОНАЛЬНЫЕ ДАННЫЕ И РАСПРОСТРАНЕНИЕ РЕКЛАМЫ ПО СЕТЯМ ЭЛЕКТРОСВЯЗИ

Звонки рекламного характера, SMS- и факс-рассылки в наше время – не редкость. В большинстве случаев такого рода сообщения предлагают пройти какие-то курсы, или приобрести товар или услугу. Речь идет о не желаемой получателем рекламе. Такая реклама навязывается пользователю без его согласия и идёт по таким средствам связи, как электронная почта, мобильная связь и прочее.

Возникающие вследствие этого проблемы актуальна как для конечных пользователей – простых владельцев средств связи, которые получают подобную рекламу, так и для сотрудников систем информационной безопасности, ибо каждый человек из представленных групп сталкивается с такими проявлениями практически каждый день. В последнее время, все чаще стали встречаться и такие звонки и рассылки, когда человеку предлагает товар или услугу субъект, явно обладающий конфиденциальной информацией, на которую у распространителей рекламы права нет. (Так, например, человеку, у которого заканчивается страховка, звонят в очень короткий период времени несколько страховых фирм; приходят рассылки на конкретное имя и отчество) Обладание персональными данными позволяет нарушителям маскировать свою рекламную деятельность, а также повысить ее эффективность.

Существующая практика показывает, что количество подобных ситуаций возрастает, а при этом нарушители действующего законодательства о персональных данных, оказываются безнаказанными. Такие прецеденты говорят о необходимости совершенствования законодательства в этой области.

Представляется, что изменения в действующем законодательстве помогут изменить положение дел. Так, например, более четкое определение подробных ситуаций в Федеральном законе «О

рекламе»; акцентирование внимания на незаконном использовании персональных данных в рекламной деятельности и четкое определение ответственности, в том числе и более четкое определение обязанностей операторов связи в этой сфере, было бы полезным для практики.

Как сообщалось в СМИ, в Государственную Думу был внесен законопроект (за №342698-6), призванный изменить ситуацию в этой области путем формирования специальной базы данных «не беспокоить». Законопроект предполагает активную деятельность граждан для достижения такой цели. Этот законопроект долгое время находится в стадии рассмотрения. Критики отмечают наличия в нём ряда недостатков, ставящих под сомнение его возможную эффективность. Так, например, в тексте законопроекта нет необходимых требований к операторам связи, которые повысили бы доказуемость нарушений. Четкое определение обязанностей операторов связи, позволило бы повысить доказуемость нарушений, равно как и понизит возможность эксплуатации закона в корыстных целях.

Вероятно, уже само внесение изменений в определение рекламы, могло бы позволить снизить количество ситуаций маскировки рекламы. Акцент на защите персональных данных позволит скорректировать ответственность за нарушение закона.

В свете сказанного, представляется, что совершенствование законодательства о рекламе должно позволить повысить эффективность борьбы с «агрессивной» рекламой в целом, а также уменьшит количество случаев использования и распространения персональных данных.

Нурдинов Р.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

РАЗРАБОТКА МЕТОДИКИ ПОСТРОЕНИЯ ЭФФЕКТИВНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА КОММЕРЧЕСКИХ ПРЕДПРИЯТИЯХ

Выбор мер и средств защиты информации из всего их многообразия является одной из главных задач для специалистов по информационной безопасности (ИБ) на любом предприятии. В настоящее время нет единой общепринятой методики, позволяющей осуществить такой выбор. Хотя сам по себе вопрос необходимости такой методики весьма противоречив.

Преимущество риск-ориентированного подхода заключается в том, что он позволяет определить экономическую эффективность использования системы защиты информации посредством сопоставления величины, на которую уменьшается риск при её использовании, с совокупными затратами на приобретение оборудования и программного обеспечения, его интеграцию, внедрение и эксплуатацию.

Для оценки рисков существует ряд методик, например, CRAMM, RiskWatch, OCTAVE, ГРИФ и другие. Основными недостатками этих методик являются высокая стоимость и отсутствие в них единой базы данных, включающей в себя объекты защиты, активы, угрозы, уязвимости и их взаимосвязи. Сами по себе такие базы не должны быть статичными, в них должна быть предусмотрена возможность обновления с учетом опыта специалистов, использующих данный продукт. Очевидно, что чем точнее должны быть полученные результаты, тем сложнее пользователям проводить оценку рисков по данной методике, поскольку требуется оперировать достаточно большим количеством данных, особенно если оценка рисков проводится в масштабах крупного предприятия. Трудность здесь состоит и в том, что не все необходимые данные можно оперативно получить, и получить в требуемом формате.

Вследствие вышесказанного, по оценкам специалистов в практике большинства коммерческих предприятий оценка рисков ИБ либо не используется совсем, либо её результаты не обладают достаточной точностью для принятия наиболее эффективных решений.

Идея, закладываемая в основу предполагаемой к разработке методики, состоит в том, что она должна быть интегрирована с другими организационно-технологическими системами предприятия. Для реализации этого будет необходимо импортировать данные из электронных бухгалтерских документов предприятия (для определения стоимости информационных активов и оценки ущерба в случае реализации угроз). Предполагается, что проверка состояния защищённости будет проводиться с помощью системы контроля защищённости (предположительно, средствами программного комплекса MaxPatrol). Автоматизация методики будет осуществлена путём формирования программного модуля с использованием платформы RSA Archer eGRC.

Сама методика должна включать в себя ряд подзадач, таких как: классификация объектов защиты, построение модели угроз, оценка рисков ИБ, обработка рисков ИБ, оценка соответствия требованиям ИБ. Для определения наиболее эффективных мер и средств защиты требуется расчет экономических показателей: коэффициента экономической эффективности, рискоёмкости информационных активов и ряда других.

Результатом работы должен стать адаптированный для российского рынка программный продукт, позволяющий построить эффективную и экономически обоснованную систему защиты информации на предприятии.

Панов К.В.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

О ФИЛЬТРАЦИИ КОНТЕНТА В ИНТЕРНЕТ-СООБЩЕСТВАХ

В настоящее время все большее влияние на безопасность государства оказывают события в информационной сфере — события, влияющие на положение страны в информационной или кибервойне. Действия государств, преследующих цели информационной войны фактически не имеют правовых ограничений на мировом уровне. Связано это с тем, что интернет считается свободным пространством для всего мирового сообщества. Конкретное государство может только ограничить внутренний доступ к сети интернет. На безопасность государства в информационной войне влияют такие факторы как наличие собственных аппаратных и программных платформ, собственная система пропаганды, СМИ, развитая законодательная база, собственные системы защиты от компьютерных вирусов, наличие барьеров при поступлении информации к конечному пользователю. В данной работе будет рассмотрен последний фактор, а именно барьеры доступа контенту, который может повлиять на информационное превосходство.

Одним из видов кибератак является выкладывание заведомо ложной, подрывающей общественное мнение информации в интернет-сообществе страны. Страны не афишируют наличие ведомств, занимающихся данной деятельностью. Однако различные источники, которые можно считать достоверными подтверждают их наличие. Согласно Guardian, Пентагон выделяет средства на кибератаки для манипулирования социальными сетями в разных странах мира. Операторы управляют аккаунтами, ничем не отличающимися от реальных пользователей, однако выкладываемые ими сообщения продвигают интересы США. Генг Яшенг, министр обороны Китая, заявил о наличии в Китае подобной армии.

В России данные силы и средства находятся на этапе зарождения. По слова Дмитрия Рогозина, зампреда правительства РФ, к концу 2013 г. планируется создание подразделения, ответственного за информационную безопасность. Проблема программных инструментов уже частично решена — разработан интернет-фильтр, ограничивающий доступ пользователя к некоторым ресурсам.

Имеется и небольшой опыт фильтрации контента. Согласно Конституции Российской Федерации и действующего законодательства сбор, хранение и распространение информации о частной жизни лица без его согласия не допускаются. Определенные материалы, содержащие такую информацию и сообщения в сети, следует рассматривать как правонарушения. Однако проблема возможности блокирования ресурсов на практике вызывает сложности. Кроме того, борьба с прецедентами противоправной деятельности в социальных сетях, например, некоторых владельцев блогов затрудняется легкостью повторной регистрации и возврата контента.

И все же представляется, что проблема блокирования нежелательных сообщений в сети может быть решена посредством использования комплекса правовых и технических мер. Сегодня существующие технические возможности, например, могут быть применены для поиска в сети материалов, сообщений, касающихся определенных личностей. Однако обработку и принятие решений может проводить только человек.

Автору представляется, что правовая база для осуществления необходимой фильтрации контента в сети требует ужесточения, причем как для конечного пользователя, так и владельца ресурса: усиления проверки подлинности, увеличения прав владельца ресурса над пользователем, введения ответственности за противоправное размещение материалов в сети.

Поляков А.М., Никитенков К.С.
Россия, Санкт-Петербург, ООО «Диджитал Секьюрити», Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

РУКОВОДСТВО ПО ОЦЕНКЕ РЕАЛИЗАЦИИ БЕЗОПАСНОСТИ КОРПОРАТИВНЫХ БИЗНЕС-ПРИЛОЖЕНИЙ

Ядро каждой крупной компании – это ERP-система: в ней проходят все критичные для бизнеса процессы, она состоит из множества уровней, таких как сервер СУБД, сервер приложений, клиентское ПО и прочее. На каждом из этих уровней могут находиться уязвимости и ошибки конфигурации, позволяющие злоумышленнику получить неавторизированный доступ к системе. Вся информация хранящаяся в ERP-системах имеет огромное значение, а любой неправомерный доступ к ней может понести за собой громадные потери, вплоть до остановки бизнеса. Поэтому безопасность корпоративных приложений является одной из наиболее обсуждаемых тем в общей сфере безопасности.

Обсуждается проект OWASP-EAS (OWASP - Enterprise Application Security, OWASP – «Безопасность Корпоративных Приложений») или EAS-SEC – «Руководство для людей, участвующих в приобретении, проектировании или внедрении приложений большого масштаба – ERP-системах». Цель проекта EAS-SEC - повышение осведомлённости вышеуказанных лиц о проблемах безопасности корпоративных приложений, создании руководящих принципов и инструментов оценки

безопасности, защищенности, безопасной настройке и разработке корпоративных приложений. Для этого проведён общий анализ основных бизнес-приложений и собраны ключевые области безопасности, на которые необходимо обратить внимание, как при разработке, так и при внедрении корпоративных приложений.

Проект EAS-SEC имеет ряд задач, на основе которых сформировано четыре подпроекта, одним из которых является Enterprise Business Application Security Implementation Assessment Guide («Руководство по оценке реализации безопасности корпоративных бизнес-приложений»). Здесь описываются различные области оценки безопасности корпоративных приложений и ERP-систем. Кроме того, приведены девять наиболее известных проблем безопасности бизнес-приложений на этапе внедрения и эксплуатации (Top 9 Application issues). При составлении списка учитывались три основных параметра: 1) изначальный доступ, который требуется для эксплуатации уязвимости; 2) критичность уязвимости (ущерб, который может быть причинён при ее реализации) и 3) сложность эксплуатации уязвимости.

Основной список проблем был составлен авторами документа в ходе анализа защищённости множества бизнес-приложений и является универсальным для каждого приложения. Эти проблемы являются весомым фактором возникновения тех или иных угроз и реализации атак в этой области, а их предупреждение означает готовность предотвращать большое число атак, направленных на безопасность корпоративных бизнес-приложений.

Перечень разделов документа един для всех бизнес-приложений, однако в данном исследовании представлен детальный анализ самой распространённой платформы для бизнес-приложений - SAP NetWeaver ABAP, в ходе которого, было выявлены 33 ключевых настройки, распределённых по раннее указанным девяти блокам. Такое руководство позволяет показать способы защиты от наиболее распространенных уязвимостей в этой сфере.

Пряхин В.Е.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

ЭФФЕКТИВНОСТЬ МЕТОДОВ АНАЛИЗА ДАННЫХ ПРИ НАГРУЗОЧНЫХ АТАКАХ В ОБСЛУЖИВАНИИ

В настоящее время угроза распределенных атак в обслуживании веб-серверов стоит как никогда остро – простои сервисов, вызванные распределенной нагрузочной атакой, наносят серьезный финансовый и репутационный урон своим владельцам. Также, распределенные атаки в обслуживании все чаще стали использоваться как средство конкурентной борьбы, или способ достижения некоторых политических целей.

В ходе был проведен подробный сбор статистики в условиях реальной нагрузочной атаки на веб-сервис, работающий на кластере серверов. Информация по каждому запросу добавлялась в базу данных и включала такие параметры, как IP адрес, user-agent, тип запроса (GET/POST), время запроса в виде UNIX Timestamp, адрес страницы/файла на сервере (URI), и так далее. Также, такая же база запросов была накоплена за время штатной работы сервиса в течение двух месяцев.

На графиках распределения запросов по объему отдаваемого контента в килобайтах (легкий – скрипты, стили, небольшие картинки; тяжелый – изображения, фотографии) во время штатной работы и нагрузочной атаки можно заметить линейную разделимость паразитных запросов и легитимных. Также была выявлена характерная последовательность запросов для легитимных пользователей – при загрузке страницы в определенном порядке загружается статика, скрипты, и оформление, когда атакующие запросы идут подряд и без закономерностей.

Собрав статистику работы сервиса во время штатной работы и построив распределение запросов, можно отсечь IP – адреса, производящие DDoS – атаку, так как они не запрашивают все нужные адреса, а только избранные — те, что либо больше всего нагружают кластер на генерацию, либо те, что отдают наиболее тяжелый контент реализуя атаку на истощение пропускной способности канала.

Ракыш Ш.Е.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

К ВОПРОСУ ПОВЫШЕНИЯ ПРОФЕССИОНАЛЬНОЙ КВАЛИФИКАЦИИ СОТРУДНИКОВ

Многие компании констатируют дефицит высококлассных специалистов – «безопасников». Это характерно не только для российских, но и для зарубежных компаний. Специалисты в области информационной безопасности испытывают потребность в знаниях о новых технологиях и решениях, в приобретении навыков применения новых средств защиты. Вследствие этого подготовка специалистов служб компьютерной безопасности является важным условием поддержания нормального функционирования как коммерческих, так и государственных структур. А динамика возникновения новых уязвимостей и угроз для безопасности компьютерных сетей требует регулярного повышения квалификации уже действующих сотрудников служб безопасности.

Подготовка, переподготовка и повышение квалификации сотрудников служб информационной безопасности требует высококвалифицированных преподавателей. Имеющиеся в публикациях и свободно доступные данные, статистика подготовки и переподготовки специалистов в области обеспечения информационной безопасности в различных компаниях показывают, что оптимальным вариантом сегодня является специализированные учебные центры для обучения «IT-безопасников». В таких центрах сформированы коллективы опытных специалистов в области защиты информации, разработчиков учебных курсов, а также имеется соответствующая материально-техническая база.

Большинство специалистов придерживается убеждения, что специалисты - «безопасники» должны проходить тренинги не реже двух раз в год, для того, чтобы поддерживать свое профессиональное соответствие в условиях быстро развивающихся информационных технологий. При планировании работы сотрудника ответственного за информационную безопасность рекомендуется предусматривать в бюджете средства для ежегодного повышения квалификации, а также выделять специальное время для его самообразования.

Хорошо подготовленный специалист по информационной безопасности позволит своей организации не только экономить значительные средства, но и окупить инвестиции в свою профессиональную подготовку за счет предотвращения возможного ущерба бизнесу.

Синетова М.М., Цымжитов Г.Б.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

ПАРАМЕТРИЧЕСКИЕ НЕОПРЕДЕЛЕННОСТИ ПРИ АНАЛИЗЕ РИСКОВ В ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ

Физическую основу случайных опасных сигналов, возникающих во время работы в выделенном помещении радиосредств и электрических приборов, составляют побочные электромагнитные излучения и наводки (ПЭМИН). Процессы и явления, образующие ПЭМИН, по способам возникновения разделяют на 4 вида:

1). Не предусмотренные функциями радиосредств и электрических приборов преобразования внешних акустических сигналов в электрические сигналы.

2). Паразитные излучения и наводки.

3). Побочные низкочастотные излучения.

4). Побочные высокочастотные излучения.

За счет ПЭМИН можно считывать информацию с монитора компьютера с помощью специальных технических средств на расстоянии до 200 метров, а то и больше. Также можно считывать информацию с процессора, клавиатуры, винчестера, дисковода. Поэтому все криптосистемы становятся почти бессмысленными, если не принять соответствующих мер защиты. Для защиты от ПЭМИН рекомендуется применять генераторы белого шума (в диапазоне от 1 до 1000 МГц).

Для перехвата побочного электромагнитного излучения средства вычислительной техники «противником» могут использоваться как обычные средства радио-, радиотехнической разведки, так и специальные средства разведки, которые называются техническими средствами разведки побочных электромагнитных излучений и наводок (ТСР ПЭМИН). Обычно ТСР ПЭМИН располагаются за пределами объекта информатизации (контролируемой зоны объекта). Есть пространство вокруг средства вычислительной техники, в пределах которого напряженность электромагнитного поля превышает допустимое (нормированное) значение, следовательно, в пределах данной зоны возможен перехват средством разведки побочных электромагнитных излучений средства вычислительной техники с требуемым качеством. Эта зона для каждого средства вычислительной техники определяется инструментально-расчетным методом при проведении специальных исследований технических средств на ПЭМИН и указывается в предписании на их эксплуатацию или сертификате соответствия.

Однако при анализе и синтезе систем управления параметры объекта часто заданы неточно, что может быть связано с погрешностями измерений, старением и износом оборудования, возмущениями, влияющими на характеристики объекта. В таком случае справедливо говорить о системах управления с неопределенными параметрами, которые могут быть периодически изменяющимися, функциями одной или нескольких переменных, интервальными.

Необходимо проанализировать и синтезировать системы управления с интервальными параметрами. Неопределенность присуща как внешним условиям работы системы, так и самой математической модели объекта. Интервальная модель объекта управления отражает реальную ситуацию когда его точные параметры не определены вследствие неточности данных, а известны только границы диапазонов изменения тех или иных величин. Необходимо также проследить влияние неопределенностей на показатели качества.

Поиск методов синтеза модального управления, инвариантных относительно базиса представления и размерности входов – выходов, привел к модификации первичной постановки задачи модального управления. В модифицированном виде задача получила формулировку обеспечения

векторного и матричного подобия процессов и модальных представлений в синтезируемой системе процессам и модальным представлениям некоторой эталонной системы с желаемой модальной моделью. В такой постановке алгоритмическое обеспечение процедуры синтеза модального управления определяется как решение неоднородного матричного уравнения Сильвестра.

Использование уравнения Сильвестра при синтезе обнаружило и заметное расширение возможностей модального управления, состоящее в достижении как желаемой структуры мод, так и собственных векторов матрицы состояния проектируемой системы. Попытки предъявления требований к структуре собственных векторов матрицы состояния проектируемой системы при условии обеспечения желаемой локализации мод стали появляться по мере интенсификации исследований по использованию геометрических методов в теории управления.

Соломатин А.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

МЕТОД ИДЕНТИФИКАЦИИ ФИЗИЧЕСКИХ ЛИЦ В СИСТЕМАХ ВИДЕОНАБЛЮДЕНИЯ НА ОСНОВЕ НАУЧНО-МЕТОДИЧЕСКОГО АППАРАТА ИММУНОКОМПЬЮТИНГА

Предложен подход для решения задачи идентификации физических лиц в системах видеонаблюдения. Рассмотрена возможность использования научно-методического аппарата иммунокомпьютинга для решения поставленной задачи. Формулируются цели и частные задачи исследования.

Повсеместное использование систем видеонаблюдения для контроля за обеспечением конфиденциальности, целостности и доступности на охраняемых объектах обуславливает важность задач связанных с автоматическим выявлением потенциальных угроз попадающих в поле зрения видеокамер. Поэтому предлагается рассмотреть методику идентификации физических лиц в системах видеонаблюдения.

В рамках задачи по идентификации физических лиц в системах видеонаблюдения был использован метод иммунокомпьютинга, который изучает принципы обработки неструктурированной информации для решения сложных практических задач. Иммунокомпьютинг является новым направлением информатики, обеспечивающий наиболее адекватное компьютерное моделирование иммунной системы и базирующийся на принципах обработки информации молекулами белков и иммунными сетями. Применение математических моделей формальной иммунной системы ведет к разработке компьютера нового типа называемого - иммунокомпьютером. Этот новый тип компьютера назван по аналогии с нейрокомпьютером, который аппаратно реализует модели нейронов.

Математический базис иммунокомпьютинга основан на свойствах сингулярного разложения произвольных матриц и позволяет с большой эффективностью решать такие задачи как обучение с экспертом; самообучение; группировка и классификация; представление результатов вычислений в пространстве образов.

В различных литературных источниках показано, что в реальных задачах распознавания образов иммунокомпьютинг превосходит своего основного конкурента — искусственные нейронные сети, по простоте реализации, быстродействию и безошибочностью распознавания. Возможности формальной иммунной системы позволяют достичь высокого уровня надежности, гибкости и быстродействия вычислений. Дальнейшее развитие данного направления может привести к серьезным прорывам в области компьютерных технологий, в частности в задачах обеспечения безопасности информации за счет обеспечения математически строгого базиса для разработки самообучающихся систем безопасности, способных противостоять заранее неизвестным вторжениям.

Автоматическая идентификации лиц в системах видеонаблюдения для выявления потенциальных угроз является актуальной задачей, решение которой позволяет существенно снижать временные и трудовые затраты в момент осуществления видеосъемки, а также при работе над анализом отснятого видеоматериала. Кроме этого, появляется возможность снизить наличие человеческого фактора в течение всего времени видеонаблюдения за охраняемым периметром.

В рамках исследования рассматривается система видеонаблюдения, установленная на охраняемом периметре. Входная информация поступает в систему с нескольких видеокамер, которые осуществляют съемку при самых разнообразных условиях. К таким условиям можно отнести общую освещенность, расположение и размер объектов, угол обзора, эмоции физических лиц попадающих в кадр.

Основная цель исследования заключается в повышении достоверности идентификации физических лиц в системах видеонаблюдения при низком качестве исходного видеоизображения и разных условиях ведения видеосъемки. Частные задачи исследования сводятся к изучению возможности использования научно-методического аппарата иммунокомпьютинга для решения поставленной цели, а также реализация программного продукта, демонстрирующего работу системы идентификации физических лиц на основе математического аппарата иммунокомпьютинга.

Турченков Д.А., Цветков Л.В.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

РАЗРАБОТКИ КОМПЬЮТЕРНОЙ ЭКСПЕРТНОЙ СИСТЕМЫ

На данный момент информационно-компьютерная экспертиза данных является самым востребованным видом компьютерно-технической экспертизы. В связи с продолжающимся ростом количества обрабатываемой в компьютерных системах информации и ростом преступлений, совершенных с использованием компьютерной техники, проведение экспертизы становится еще более ресурсоемкой задачей.

На практике существует ряд автоматизированных информационно-поисковых систем, используемых для проведения судебных экспертиз в различных областях. Трудность создания автоматизированной информационной системы компьютерной сопряжена с большим разнообразием используемых на практике форматов данных и технологий.

Для решения задачи создания макета такой системы, авторами предлагается использовать метод поиска текстовой и графической информации в неструктурированных массивах данных (файлы, образы жестких дисков, разделы подкачки, оперативная память), с последующей классификацией и определением авторства текстов. Такой метод базируется на сигнатурном и частотном анализе данных для определения их формата и источника.

Предполагается, что планируемая к разработке система позволит проводить поиск информации, созданной пользователем анализируемой системы, для последующей оценки экспертом. Особый интерес может вызвать перспектива доработки метода для решения важной и актуальной прикладной задачи: анализа лицензионности программного обеспечения на основе встроенной системной информации.

Углов Е.Н., Владимирская М.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

РАЗРАБОТКА ПРЕДЛОЖЕНИЯ ПО АДАПТАЦИИ ЗАКОНОДАТЕЛЬСТВА РФ К ВНЕДРЕНИЮ ОБЛАЧНЫХ ТЕХНОЛОГИЙ

Новым этапом развития информационных технологий является перенос вычислений в облачные структуры. На основании опыта, полученного США и Австралией, можно сделать вывод о том, что отказ от устаревших методов обработки информации является ключевым способом сокращения расходов на информационные технологии, что в условиях глобального экономического кризиса является одним из основных показателей эффективности политики, которую ведет государство в области IT.

Как и любая область оборота информационных ресурсов, облачное пространство требует правового регулирования. Регулирование процессов и отношений в области облачных вычислений – сложная задача, так как интересы пользователей, заинтересованных в сохранении контроля над своими данными, и интересы провайдеров облачных вычислений, заинтересованных в максимальной свободе при эксплуатации и развитии своих сервисов, расходятся. Российские законодатели пока что не уделяют облачным вычислениям достаточно внимания. В то же время, судя по материалам обзоров и публикаций, в Евросоюзе, США и Австралии обновление законодательства идет достаточно активно.

Цель работы: подготовить рекомендации, направленные на адаптацию российского законодательства к внедрению новых технологий. На основе изучения и анализа опыта зарубежных стран сформулировать предложения, которые могли бы позволить адаптировать федеральные законы к способам регулирования защиты персональных данных при использовании облачных сервисов. В качестве первого шага потребуется определить такие специфические понятия как «провайдер облачных вычислений» и «облачный хостинг» и др. Представляется, что такие понятия должны были бы получить своё правовое закрепление, возможно, в базовом Федеральном законе «Об информации, информационных технологиях и о защите информации».

Филинюк С.Ю., Еремин О.Е.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

О ПОДГОТОВКЕ КАДРОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В век информационного общества актуальность вопросов защиты информации выходит на одно из первых мест среди прочих задач, решаемых в процессе проектирования, создания и использования современных информационных систем. Причины повышенного внимания к этой проблеме вполне очевидны – от качества мер защиты информации напрямую зависит экономическая безопасность организации. Информация – это ресурс, который, как и другие важные бизнес-ресурсы имеет немалую ценность для организации и, следовательно, нуждается в надежной защите.

Для решения вопросов защиты информации и обеспечения информационной безопасности необходимы специалисты, компетентные в данной области знаний. В основу подготовки таких специалистов положена модель компетенций. Предоставляет интерес попытаться описать, по имеющимся в доступных источниках материалам, логику и технологию разработки и применения модели компетенций для подготовки специалиста по защите информации. Работа основана на исследованиях по созданию моделей специалистов и на методах разработки профессиональных стандартов в отрасли информационных технологий.

Модель компетенций, должна содержать детальное описание стандартов поведения человека, занимающего конкретную должность, ведущих к достижению должностных целей. Степень детализации в модели компетенций зависит от целей, для которых применяется такая модель. Попытка охватить весь спектр информации и разработать модель «на все случаи жизни», как правило, не всегда работает с нужной эффективностью. Такая модель очень сложна в применении и малоэффективна. Кроме того, ее очень сложно разработать, так как, по мнению ряда экспертов, разница между многими компетенциями крайне мала и едва различима.

Судя по доступным публикациям, опыт последних лет применения модели компетенций показывает, что набор компетенций должен быть оптимальным и включать лишь ключевые стандарты поведения. Содержание модели должно соответствовать стратегическим целям развития отрасли. Это означает, что разрабатываемые компетенции должны способствовать дальнейшей деятельности выпускников в различных компаниях в профильной отрасли, направленной на достижение именно заданных целей, а не включать весь мыслимый и немыслимый набор возможных компетенций.

Модель компетенций должна быть полезной для всех, кто руководствуется данной моделью в своей профессиональной деятельности (это и специалисты фирм и компаний, использующие модель в качестве инструмента, преподаватели, слушатели системы повышения квалификации и студенты). Следует помнить, что субъектом модели могут быть студенты, у которых есть свои цели, свои мотивы трудовой деятельности и свои потребности. Это означает, что модель должна представлять интерес для разных категорий пользователей, расширяющих и углубляющих багаж своих профессиональных знаний.

Разрабатываемая модель должна быть гибкой, в неё необходимо заложить возможность изменения и расширения компетенций. В процессе применения модели важно учитывать возможные изменения среды и соответствующей адаптации модели. Оптимальный набор компонентов модели и их изменяемость должны быть направлены на повышение эффективности и эргономичность её использования. Модель компетенции должна быть достаточно проста и понятна разным категориям пользователей.

Само по себе содержание модели не является гарантом создания инструмента по повышению эффективности учебного и рабочего процесса. Результат её использования напрямую связан с качеством организационной деятельности и стройности всей системы управления. Анализ существующей практики показывает, что часто модель компетенций, включающая, казалось бы, все необходимые элементы не дает ожидаемого эффекта. Часто причина такой ситуации в недостатках построение модели.

Цымжитов Г.Б.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

ОПТИМИЗАЦИЯ ТОПОЛОГИИ КОРПОРАТИВНОЙ КОМПЬЮТЕРНОЙ СЕТИ

Корпоративная компьютерная сеть является целостной структурой вычислительных систем, состоящей из взаимодействующих сетей структурных подразделений. Регулярное функционирование корпоративной компьютерной сети требует реализации организационно-технических мероприятий, жесткой дисциплины пользователей и служб сопровождения. Для этого необходима также ее оптимизации посредствам моделирования конкретного сервиса в целях повышения качества обслуживания (Quality of Service). Качество обслуживания является критически важным параметром для администрирования компьютерной сети.

Целью данной работы является оптимизация топологии в существующей корпоративной компьютерной сети для улучшения доступа к сервису, который находится на прикладном уровне модели OSI. Совершенствование организации компьютерной сети – задача актуальная для всех крупных организаций (в основу ее решения предполагается положить некое видение эталонной модели).

Задачи работы:

1) получение статистических данных о времени доступа к сервису;
2) графическое отображение времени ответа сервиса и проектирование прогностической функции;
3) исследование и моделирование аналитической функции работы сервиса;
4) оптимизация топологий сети.

Результатом работы должен стать перечень рекомендаций по оптимизации компьютерной сети для организации, в которой выполнялась данная работа.

Шабанов Д.П.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

О ГЕОИНФОРМАЦИОННЫХ ДАННЫХ И МНОГОПОЗИЦИОННЫХ СИСТЕМАХ НАБЛЮДЕНИЯ

Гарантированное обеспечение достоверности, полноты информации о положении воздушного судна (ВС) и специальных транспортных средств (СТС), доступность радиолокационных данных в любой момент времени являются одними из задач, от решения которых зависит информационная безопасность аэродромных многопозиционных систем наблюдения (АМПСН).

Современные аэродромные многопозиционные системы наблюдения (АМПСН), применяемые в Единой Системе Организации Воздушного Движения (ЕС ОрВД) должны обеспечивать диспетчеров аэродромной зоны достоверной информацией о местоположении и идентификации воздушного судна и специальных транспортных средств, находящихся в зоне ответственности аэропорта. Высокие риски при осуществлении операций взлета, посадки и руления воздушных судов предъявляют соответствующие требования к параметрам АМПСН в том числе и в области информационной безопасности.

Выявление угроз информационной безопасности АМПСН является актуальной задачей как в процессе проектирования и монтажа системы, так и в процессе ее эксплуатации. Угрозы доступности радиолокационной информации для подобного рода систем могут возникать случайно, в результате сложившихся метеоусловий или ошибочных действий персонала. Угрозы нарушения целостности информации (ее достоверности и полноты) могут возникать как в результате ошибок проектирования системы (неправильного размещения приемных станций), так и в процессе эксплуатации АМПСН (возведение новых зданий или сооружений, которые могут создавать углы закрытия для приема сигналов от ВС и СТС).

Для оценки показателей защищенности вновь разрабатываемых АМПСН, анализа компонентного взаимодействия и эмерджентных свойств применяются прогнозные модели, относящиеся к классу эмпирических. Они основаны на измерении технических характеристик, однако для выявления угроз информационной безопасности на ранних этапах разработки АМПСН необходимо также использование геоинформационных данных и данных о текущей обстановке на территории аэропорта.

Шаго Ф.Н.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

К ВОПРОСУ АУДИТА ПРОГРАМНО-ТЕХНИЧЕКИХ КОМПЛЕКСОВ ЗАЩИТЫ ИНФОРМАЦИИ

Совершенствование технологий обработки информации влечет за собой постоянный рост требований к обеспечению информационной безопасности. Особенностью построения механизмов безопасности для реально действующей автоматизированной системы (АС) является их уникальность. Формализация процессов обеспечения информационной безопасности АС порой представляет определенные трудности. Вследствие этого, в целях обеспечения информационной безопасности АС необходимо рассматривать как информационную систему, зачастую слабо формализованного вида.

Руководящие документы Федеральной службы по техническому и экспортному контролю (ФСТЭК России) определяют требования к уровням и классам защиты информации. Критерии по которым принимаются решения о соответствии уровню и классу защиты информации имеют формальный характер – удовлетворяет система защиты информации требованиям критерия или нет. Применяемый «двоичный» подход при классификации не позволяет гибко учитывать специфику и порядок обработки информации в автоматизированной системе. Такой подход к оценке характеристик системы защиты информации не дает овеществленных значений о степени защищенности, не позволяет получить качественную оценку. Для построения автоматизированных систем аудита степени защищенности АС целесообразен переход к вероятностным показателям характеристик системы защиты информации.

В целях обеспечения информационной безопасности разработан целый комплекс теоретических методов. Применение этих методов в решении задач связанных с формализацией процессов обеспечения информационной безопасности дает возможность создавать модели управления защитой информации, описывать возможные информационные потоки в системе. Это позволяет смоделировать систему защиты информации и получить оценку соответствия комплекса защиты информации предъявленным требованиям. С помощью моделей представляется возможным получить адекватные и корректные оценки параметров системы обеспечения информационной безопасности при проведении аудита защищённости информации. Подобные методы и модели применяются при проведении сертификации и аудите автоматизированных систем по требованиям безопасности информации.

Появление новых теоретических и технических решений по построению автоматизированных систем обработки информации влечет за собой ужесточение требований к количественным и качественным параметрам средств защиты информации. Это, в свою очередь, обуславливает необходимость совершенствования процессов защиты информации. Это, в свою очередь, требует создания более совершенных средств защиты и аудита таких средств и систем. Совершенствование аудита программно-технических комплексов средств защиты и безопасности информации требует разработки своего методического и математического аппарата. Этим обуславливается актуальность выбранного направления исследований.

Для решения задачи необходим комплексный подход, предполагающий наличие нескольких этапов. Первый этап – рациональное распределение ресурса по уровням иерархии испытаний. Это позволит определить оптимальные требования к показателю качества и необходимое количество испытаний (времени) для каждого уровня испытаний. Второй этап – определение процедуры формирования факторного пространства, определение стратегии аудита и методов статистического анализа результатов факторного эксперимента. Третий этап – необходимое уточнение модели функционирования самой системы защиты информации. Четвертый этап – объединение экспериментальных и модельных данных, которое должно позволить получить более достоверное представление о характеристиках системы защиты информации. Итоговым результатом должно стать повышение точности оценки характеристик системы защиты информации.

Шацких Р.Н.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

К ВОПРОСУ ОБ УНИВЕРСАЛЬНОЙ ВЕРИФИЦИРУЮЩЕЙ СИСТЕМЕ

Существующие методы обнаружения аномалий условно можно разделить на следующие группы: анализ сигнатур, статистический анализ, поведенческая биометрия, нейронные сети, иммунные сети.

Метод анализа сигнатур базируется на простом понятии совпадения последовательности с образцом, указывающим на характеристику вредного трафика. Основные достоинства: очень быстрый; правила легко написать, понять и настроить; огромная поддержка компьютерного сообщества в быстром производстве сигнатур для новых опасностей. Основные недостатки: замедляется время работы системы, использующей данный метод, за счет увеличения числа проверяемых сигнатур; выявление только уже известных атак, сигнатуры которых имеются.

Методы статистического анализа основаны на построении статистического профиля поведения системы в течение некоторого периода «обучения», при котором поведение системы считается нормальным. Затем, в режиме обнаружения, система оценивает отклонения наблюдаемых значений от значений, полученных во время обучения. Основные достоинства: высокая адаптивность к неизвестным атакам. Основные недостатки: высокий уровень ложных срабатываний при использовании в локальных сетях, где поведение объектов не имеет усреднённого характера; статистические анализаторы плохо обрабатывают изменения в информационной системе; статистический метод устойчив только в пределах конкретной системы. Построенные статистические профили нельзя использовать в других аналогичных информационных системах.

В основе методов поведенческой биометрии лежит гипотеза о различии «почерка» работы с интерфейсами ввода-вывода для различных пользователей. На базе построенного профиля нормального поведения для данного пользователя обнаруживаются отклонения от этого профиля, вызванные попытками других лиц работать с клавиатурой или другими физическими устройствами ввода. Основные достоинства: высокая адаптивность к неизвестным атакам. Основные недостатки: низкая верифицируемость метода; метод устойчив только в пределах конкретной системы; данный метод позволяет отслеживать атаки только на уровне отдельного узла сети.

Нейронные сети для обнаружения аномалий обучаются в течение определенного периода времени, в течение которого наблюдаемое поведение считается нормальным. Обучение нейронной сети осуществляется последовательностью команд. Входные данные сети состоят из текущих команд и прошлых команд, которые обрабатываются нейронной сетью с целью предсказания последующих команд. После того как нейронная сеть обучена множеством последовательных команд защищаемой системы или одной из ее подсистем, сеть представляет собой «образ» нормального поведения. После обучения нейронная сеть запускается в режиме распознавания. Основные достоинства: адаптивность; высокая верифицируемость. Основные недостатки: нейронные сети имеют высокую вычислительную сложность обучения, что затрудняет их применение на больших потоках данных; нейронные сети устойчивы только в пределах той сети, в которой они обучались, что существенно ограничивает применимость метода (только локальная устойчивость).

В основу принципов работы иммунных сетей заложены основные механизмы функционирования естественной иммунной системы, предохраняющей человека от опасных инородных тел. Происходит распознавание аномалий и имитация процессов, в результате которых

генерируются ранее неизвестные сигнатуры, которые в свою очередь сравниваются с нормальным профилем. Основные достоинства: высокая адаптивность к неизвестным атакам. Основные недостатки: большая вычислительная сложность; иммунные сети устойчивы только в пределах той сети, в которой они обучались, что существенно ограничивает применимость метода (только локальная устойчивость).

Приведенный обзор показывает, что существующие методы обнаружения аномалий не обладают оптимальным балансом достоинств и недостатков. Вследствие этого возникает потребность создания универсальной верифицируемой системы, обладающей высокой адаптивностью к неизвестным атакам с низким уровнем ложных срабатываний и обладающей приемлемой вычислительной сложностью.

Шоломов И.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

О НЕОБХОДИМОСТИ КОМПЛЕКСНОГО ПОДХОДА К ПРЕДОТВРАЩЕНИЮ НАРУШЕНИЯ АВТОРСКИХ ПРАВ

Проблема контрафакции в информационных технологиях стоит достаточно остро и над её решением неустанно борются специалисты различных сфер, в том числе и специалисты по информационной безопасности.

Противоправное присвоение интеллектуальной собственности призван предотвратить Федеральный закон «О внесении изменений в законодательные акты Российской Федерации по вопросам защиты интеллектуальных прав в информационно-телекоммуникационных сетях» (от 2 июля 2013 года №187-ФЗ). Действующее Российское законодательство предусматривает и уголовную ответственность за противоправные деяния в отношении объектов интеллектуальной собственности. Однако мировая практика показывает, что только репрессивные меры недостаточно эффективны в борьбе с явлением, охватывающим большую часть планеты. Согласно исследованию BSA и IDC в России 60% ПО установленного на ПК в 2008 году было контрафактным (Согласно исследованию BSA и IDC от 14 мая 2009 года), а в 2011 году – 63% (Исследование BSA «Конкурентное преимущество Экономический эффект от использования лицензионного ПО»). И это только ПО, которое даже не затрагивается новым законом. Что уж говорить о кино, музыке и книгах?

В рамках работы была поставлена задача изучить примеры «пиратства» в сфере IT и существующие недостатки в практике противодействия нарушениям авторских прав.

Многочисленные открытые общедоступные источники, в частности, видео и обзоры свободно распространяемые в сети Интернет, с которыми ознакомился автор, привели к убеждению, что нельзя все некритично принимать на веру. К сожалению, абсолютное большинство таких обзоров весьма поверхностны, а их авторы, так называемые «обзорщики», больше заинтересованы в собственном пиаре (например, в раскрутке своих сайтов), вследствие этого в их материалах мало конструктива. Встречаются, однако, и заслуживающие внимания материалы, авторы которых, видимо, вполне квалифицированные люди, четко и аргументировано высказывающие обоснованные и бесспорно интересные идеи.

Автором были также использованы материалы исследований BSA и IDC. По изученным материалам удалось сформировать определенные представления о первопричинах возникновения существующих проблем, и о том какими путями их можно решать.

Результатом ознакомления с указанными выше материалами стало расширение знаний и кругозора автора о проблеме интеллектуальной собственности и формирующееся мнение о том, что только комплексный подход к проблеме противодействия нарушения авторских прав, может быть эффективным.

Ященко М.А., Елисеев Ю.М.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

К ВОПРОСУ ОБ ИЗВЛЕЧЕНИИ ИНФОРМАЦИИ ИЗ БРАУЗЕРОВ

Наиболее распространенными преступлениями в сфере компьютерной информации сегодня являются неправомерный доступ к информации и компьютерное «пиратство». По данным ГИЦ МВД России, если в 1997 году было зарегистрировано всего 7 преступлений в сфере компьютерной информации, то в 2002 году их число возросло до 4050 таких преступлений, а в 2005 г. составило 10214 случаев. Эта тенденция имеет место и сегодня. Также многие “некомпьютерные” преступники пользуются сетью Интернет для совершения преступлений (так, например, различного рода мошенники, педофилы и др.).

Вследствие сказанного сегодня становится актуальной так называемая «форензика» – подраздел криминалистики, прикладная наука о раскрытии преступлений, связанных с компьютерной информацией, об исследовании цифровых доказательств, о методах поиска, получения и

закрепления таких доказательств. А если преступники пользуются браузерами, то следовательно и вся информация об истории посещения веб-страниц и введенных паролях хранится самим браузером. Эта информация чрезвычайно ценна для криминалистов.

В связи с изложенным, авторы задались целью написать единую методику для не деструктивного извлечения информации из браузеров, не запуская при этом сами браузеры. Такая методика может оказаться полезной для криминалистических исследований. Предметом нашего рассмотрения стали актуальные версии Интернет браузеров: Internet Explorer, Mozilla Firefox, Opera и Google Chrome, работающих под ОС Microsoft Windows. Перечисленные браузеры являются сегодня самыми популярными в России. По имеющимся оценкам, Google Chrome имеет долю рынка в 24,1%, Mozilla Firefox – 11,1%, Opera – 8,5%, а Internet Explorer – 3,8%.

Предполагается, что запланированная к созданию методика позволит унифицировать процесс поиска и извлечения необходимой информации в ходе следственных и криминалистических мероприятий, а также будет востребована при разработке и осуществлении мер информационной безопасности на объектах. В рамках заданного исследования будет проведен анализ браузеров и методов хранения и обработки ими интересующей нас информации. В перспективе планируется выйти на программную реализацию задуманной методики.

ОГЛАВЛЕНИЕ

ГОСУДАРСТВЕННАЯ ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕГИОНОВ РОССИИ 13

Балыбердин А.Л., Вус М.А.
Россия, Москва, Административный департамент аппарата Правительства РФ,
Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
К ДВАДЦАТИЛЕТИЮ РОССИЙСКОГО ЗАКОНА «О ГОСУДАРСТВЕННОЙ ТАЙНЕ» 13

Вус М.А., Макаров О.С.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
Беларуссия, Минск, ГУО «Институт национальной безопасности Республики Беларусь»
О РАЗРАБОТКЕ СТРАТЕГИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ГОСУДАРСТВ – УЧАСТНИКОВ СНГ 14

Иванов В.П.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
НЕКОТОРЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ 15

Игнатьев М.Б., Липинский Я.А., Ненашев В.А., Никитин А.В., Шепета А.П.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения
КАК ОБУСТРОИТЬ ОКОЛОЗЕМНОЕ ПРОСТРАНСТВО ДЛЯ БОРЬБЫ С КОСМИЧЕСКИМИ
УГРОЗАМИ 16

Карамышев В.Е., Сичкарук А.В., Черешкин Д.С.
Россия, Москва, Институт системного анализа РАН
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОБЪЕКТОВ ПУТЕМ УПРАВЛЕНИЯ РИСКАМИ НАРУШЕНИЯ
ТРЕБОВАНИЙ 17

Лепёхин А.Н.
Беларуссия, Минск, Академия МВД Республики Беларусь
ОБ ОТДЕЛЬНЫХ НАПРАВЛЕНИЯХ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА В ОБЕСПЕЧЕНИИ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 18

Пономаренко А.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННОГО ОБЩЕСТВА РОССИИ 20

Самойленко Е.А.
Россия, Санкт-Петербург, ЗАО «АСИС»
ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИИ 21

Синещук Ю.И., Филиппов А.Г.
Россия, Санкт-Петербург, Военно-морская академия им. Адмирала Флота Советского
Союза Н.Г. Кузнецова, Санкт-Петербургский университет ГПС МЧС России
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, КАК ОСНОВА ОБЕСПЕЧЕНИЯ ЭФФЕКТИВНОСТИ
СИСТЕМЫ УПРАВЛЕНИЯ МЧС 22

Советов Б.Я., Колбанёв М.О., Татарникова Т.М.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет
«ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербургский государственный
экономический университет
О РАЗВИТИИ ТЕХНОЛОГИИ ИНФОРМАЦИОННОГО ОБЩЕСТВА 23

Соколов С.С., Новоселов Р.Ю.
Россия, Санкт-Петербург, Государственный университет морского и речного флота
имени адмирала С.О. Макарова
ГРИД-СИСТЕМЫ – БУДУЩЕЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ТРАНСПОРТНОЙ СФЕРЫ 23

Федоров Д.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
ПОДХОД К ФОРМАЛИЗАЦИИ ОПИСАНИЯ ДЕСТРУКТИВНОГО ИНФОРМАЦИОННОГО
ВОЗДЕЙСТВИЯ НА ЛИЧНОСТЬ И ОБЩЕСТВО 24

Шишкин В.М., Абросимов И.К.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ДИНАМИЧЕСКАЯ МОДЕЛЬ СИСТЕМЫ ВЗАИМОДЕЙСТВИЯ РАЗВИТИЯ ИКТ И ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ 25

Яковлева Н.В.
Россия, Санкт-Петербург, Санкт-петербургский филиал «Финансовый университет при Правительстве Российской Федерации»
СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ СИСТЕМЫ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОГО СОТРУДНИЧЕСТВА РЕГИОНОВ В ФОРМЕ ПАРАДИПЛОМАТИИ 26

ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 27

Баушев С.В., Буторин Н.В., Гаценко О.Ю., Самонов А.В.
Россия, Санкт-Петербург, ЗАО «Центр научно-прикладных исследований «ИнформПро»
ПРОГРАММНЫЙ КОМПЛЕКС СОЗДАНИЯ И ПРОВЕРКИ ЮРИДИЧЕСКИ ЗНАЧИМЫХ ЦИФРОВЫХ ФОТОСНИМКОВ 27

Бачило И.Л.
Россия, Москва, Институт государства и права РАН
О ПОДХОДАХ К СОВЕРШЕНСТВОВАНИЮ ИНФОРМАЦИОННОГО ЗАКОНОДАТЕЛЬСТВА 27

Бондуровский В.В.
Россия, Санкт-Петербург, Межпарламентская Ассамблея государств-участников СНГ
ОБ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПРАВ ЧЕЛОВЕКА В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ 28

Клишков В.Б., Пасынков В.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
НЕКОТОРЫЕ ПРОБЛЕМЫ ПРЕСТУПНОСТИ В СФЕРЕ КОМПЬЮТЕРНЫХ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ 31

Кононов О.А., Кононова О.В., Попенко Н.В.
Россия, Санкт-Петербург, Смольный институт РАО, Санкт-Петербургский государственный университет аэрокосмического приборостроения, Москва, Президиум РАН
ПРАВОВЫЕ ВОПРОСЫ ЭЛЕКТРОННОЙ БИБЛИОТЕКИ 32

Кононов О.А., Кононова О.В., Попенко Н.В.
Россия, Санкт-Петербург, Смольный институт РАО, Санкт-Петербургский государственный университет аэрокосмического приборостроения, Москва, Президиум РАН
ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ЭЛЕКТРОННОЙ ПОЧТЫ 33

Кучерявый М.М.
Россия, Санкт-Петербург, Управление ФСТЭК России
К ВОПРОСУ ПРАВОВОГО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ПРОИЗВОДСТВЕННЫМИ И ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФРАСТУКТУРЫ 33

Мазнев В.Б.
Россия, Санкт-Петербург, Межрегиональный институт экономики и права при МПА ЕврАзЭС
ПРОБЛЕМЫ КИБЕРПРЕСТУПНОСТИ И КИБЕРБЕЗОПАСНОСТИ: АКТУАЛЬНЫЕ РИСКИ И ВОЗМОЖНОСТИ ПРОТИВОДЕЙСТВИЯ (ПРАВОВОЙ АСПЕКТ) 34

Макаров О.С.
Беларуссия, Минск, ГУО Институт национальной безопасности
О НЕКОТОРЫХ АСПЕКТАХ ХАРАКТЕРИСТИКИ ПРАВОВЫХ МЕР ЗАЩИТЫ ГОСУДАРСТВЕННЫХ СЕКРЕТОВ ГОСУДАРСТВ-УЧАСТНИКОВ СНГ 35

Макаров О.С.
Беларуссия, Минск, ГУО «Институт национальной безопасности Республики Беларусь»
К ВОПРОСУ О СУЩНОСТНОЙ ХАРАКТЕРИСТИКЕ ГОСУДАРСТВЕННЫХ СЕКРЕТОВ КАК ИСТОЧНИКА ПОВЫШЕННОЙ ОПАСНОСТИ 36

Максимова Е.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
РАЗВИТИЕ СИСТЕМЫ НОРМАТИВНОГО ПРАВОВОГО РЕГУЛИРОВАНИЯ ОТНОШЕНИЙ В ОБЛАСТИ СОЗДАНИЯ И ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ 37

Нигметов Н.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
СОДЕРЖАНИЕ ОПЕРАТИВНО-РОЗЫСКНЫХ МЕРОПРИЯТИЙ В СЕТИ ИНТЕРНЕТ..... 38

Перевалов Д.В., Вус М.А.
Беларуссия, Минск, ГУО «Институт национальной безопасности Республики Беларусь»,
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
О ПРОЕКТЕ МОДЕЛЬНОГО ЗАКОНА МПА СНГ «О КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТАХ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ»..... 39

Сагайдак А.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
ПРОФИЛАКТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ 40

Смирнова О.Г.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
СРАВНИТЕЛЬНЫЙ АНАЛИЗ КЛАССИФИКАЦИЙ КИБЕРПРЕСТУПЛЕНИЙ И ИХ СВЯЗЬ С УГОЛОВНЫМ ЗАКОНОДАТЕЛЬСТВОМ РФ 41

Сорокина Е.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
СОВРЕМЕННОЕ СОСТОЯНИЕ НОРМАТИВНО-ПРАВОВОЙ БАЗЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРЕДИТНО-ФИНАНСОВОГО УЧРЕЖДЕНИЯ 42

Ярмоленко Н.В.
Россия, Санкт-Петербург, Санкт-Петербургский военный институт внутренних войск МВД России
ПРОБЛЕМЫ ПРАВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ..... 43

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ..... 45

Аполлонский А.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД
ИДЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ ИНТЕРНЕТА И КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ 45

Атисков А.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ИСПОЛЬЗОВАНИЕ ОНТОЛОГИЧЕСКОГО ПРОЕКТИРОВАНИЯ ДЛЯ АВТОМАТИЗИРОВАННОГО АНАЛИЗА ДОКУМЕНТОВ ПОЛИТИКИ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ..... 46

Афанасьев С.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ОНТОЛОГИЧЕСКИЙ ПОДХОД К ОПРЕДЕЛЕНИЮ ОБЛАЧНЫХ СЕРВИСОВ 47

Белоусов А.С.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова
СОВРЕМЕННЫЕ ТЕХНОЛОГИИ ПЕРЕДАЧИ ДАННЫХ В БЕЗОПАСНЫХ БЕСПРОВОДНЫХ ТРАНСПОРТНЫХ СЕТЯХ 47

Биричевский А.Р.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ПОДХОД К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ВЗАИМОДЕЙСТВИЯ ПРОЦЕССОВ ПРИ РАЗРАБОТКЕ ОПЕРАЦИОННЫХ СИСТЕМ 49

Большаков В.И., Большакова Л.В., Яковлева Н.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
МЕТОДЫ МНОГОМЕРНОГО СТАТИСТИЧЕСКОГО АНАЛИЗА В РЕШЕНИИ ПРОБЛЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 50

Виноградов А.Б., Щиголева М.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОПАСНЫХ РЕЖИМОВ РАБОТЫ В НАУЧНЫХ ИССЛЕДОВАНИЯХ 50

Демьянчук А.А., Новикова Е.С., Молдовян Д.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербургский институт информатики и автоматизации РАН
СПОСОБ ПОВЫШЕНИЯ УРОВНЯ БЕЗОПАСНОСТИ ПРОТОКОЛОВ АУТЕНТИФИКАЦИИ С НУЛЕВЫМ РАЗГЛАШЕНИЕМ СЕКРЕТА 51

Дормидонтов А.А., Зубакин В.В.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного
АНАЛИЗ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОГО ОБМЕНА ПРИ ПРИМЕНЕНИИ ДИНАМИЧЕСКИХ АЛГОРИТМОВ МАРШРУТИЗАЦИИ 52

Дулатов И.Н.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова
ОРГАНИЗАЦИОННЫЕ И ПРАВОВЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ 53

Ежгуров В.Н., Соколов С.С.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова
УЯЗВИМОСТИ В СИСТЕМАХ УПРАВЛЕНИЯ МУЛЬТИМОДАЛЬНЫМИ ПЕРЕВОЗКАМИ НА ПРИМЕРЕ СУБД ERP-КЛАССА 54

Кислов Р.И., Юрин И.В.
Россия, Санкт-Петербург, ООО Центр защиты информации «Актив»,
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
К ВОПРОСУ ОБ ИЗМЕРЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 55

Зорин К.М.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет» ЛЭТИ» им. В.И. Ульянова (Ленина)
ПРОГНОЗИРОВАНИЕ СЕТЕВЫХ АТАК С ПОМОЩЬЮ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ И DATA MINING 56

Ковальногова Н.М.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова
УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЭКОНОМИЧЕСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ 56

Колесникова С.И.
Россия, Томск, Национальный исследовательский Томский государственный университет
ОСОБЕННОСТИ ПРИМЕНЕНИЯ ХАОТИЧЕСКИХ МОДЕЛЕЙ В ШИФРОВАНИИ ИНФОРМАЦИИ 57

Колодин М.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБРАЗОВАТЕЛЬНЫХ СИСТЕМ 58

Култышев Е.И., Полонский А.М., Козлов А.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В БЮРО ПРОПУСКОВ БИЗНЕС-ЦЕНТРА 59

Макшаков В.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
МЕТОД ИДЕНТИФИКАЦИИ ИСТОЧНИКОВ ИМПУЛЬСНОГО РАДИОИЗЛУЧЕНИЯ 60

Михайлов Н.С.
Россия, Санкт-Петербург, ОАО «Равенство»
РАЗГРАНИЧЕНИЕ ПРАВ ДОСТУПА В ИНТЕГРИРОВАННОЙ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ..... 60

Лавренов В.В.
Беларуссия, Минск, Академия МВД Республики Беларусь
ОЦЕНКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ РЕСПУБЛИКИ БЕЛАРУСЬ 61

Полубелова О.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
СТРАТЕГИИ РАЗРЕШЕНИЯ АНОМАЛИЙ ФИЛЬТРАЦИИ МЕЖСЕТЕВЫХ ЭКРАНОВ 62

Потехин В.С., Синещук Ю.И., Скряга Ю.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,
Военно-морская академия им. Адмирала Флота Советского Союза Н.Г. Кузнецова
ИНФОРМАЦИОННЫЕ УГРОЗЫ И УЯЗВИМОСТИ ТЕХНОЛОГИИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ..... 63

Советов Б.Я., Колбанёв М.О., Татарникова Т.М.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербургский государственный экономический университет
МОДЕЛЬ ФИЗИЧЕСКИХ ХАРАКТЕРИСТИК СИГНАЛОВ..... 64

Саенко И.Б., Куваев В.О.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН,
Военная академия связи им. С.М. Буденного
ОБ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЕ РАЗГРАНИЧЕНИЯ ДОСТУПА К РЕСУРСАМ ЕДИНОГО ИНФОРМАЦИОННОГО ПРОСТРАНСТВА ДЛЯ РАЗНОРОДНЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ 65

Сенцова А.Ю., Машкина И.В.
Россия, Уфа, Уфимский государственный авиационный технический университет
ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОЙ НЕЙРОННОЙ СЕТИ ДЛЯ ОЦЕНКИ РИСКА НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ 66

Соколов С.С., Бориев З.В.
Россия, Санкт-Петербург, Государственный университет морского и речного флота
имени адмирала С.О. Макарова
МЕТОД ОБЕЗЛИЧИВАНИЯ КАК ФАКТОР УМЕНЬШЕНИЯ РИСКОВ РЕАЛИЗАЦИИ УГРОЗЫ РАЗГЛАШЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ХРАНЕНИИ В ИНФОРМАЦИОННЫХ БАЗАХ ДАННЫХ 67

Соколов С.С., Ежгуров В.Н.
Россия, Санкт-Петербург, Государственный университет морского и речного флота
имени адмирала С.О. Макарова
СИТУАЦИОННАЯ МОДЕЛЬ НАРУШИТЕЛЯ В ИНФОРМАЦИОННЫХ СИСТЕМАХ НА ТРАНСПОРТЕ..... 68

Солодянников А.В.
Россия, Санкт-Петербург, ЗАО «Ассоциация специалистов информационных систем»
ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ В ОБЩЕЙ СИСТЕМЕ ДЕЛОПРОИЗВОДСТВА ПРЕДПРИЯТИЯ 69

Уварова Ю.А.
Россия, Санкт-Петербург, Российский государственный педагогический университет
им. А.И. Герцена
ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В УСЛОВИЯХ БЫСТРОЙ СМЕНЫ ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКОЙ СРЕДЫ ГОРОДА СОЧИ 70

Фаткиева Р.Р.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
МНОГОМАШТАБНЫЙ АНАЛИЗ СЕТЕВОГО ТРАФИКА 71

Федорченко Л.Н.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ОБ АСПЕКТАХ ОНТОЛОГИЧЕСКОГО АНАЛИЗА ДОКУМЕНТОВ В СТАНДАРТАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 71

Филиппов А.Н., Стародубцев А.А.
Российская Федерация, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
МЕТОДЫ СОЗДАНИЯ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ В ПРИБОРОСТРОЕНИЕ 72

Чудиловская Т.Г.
Беларуссия, Минск, Академия МВД Республики Беларусь
ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЛАЧНЫХ ТЕХНОЛОГИЙ 73

Щиголева М.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им.В.И.Ульянова (Ленина)
ОПРЕДЕЛЕНИЕ УРОВНЯ РАЗРЕШЕННЫХ ПОТЕРЬ СЕМАНТИЧЕСКОЙ БИОФИЗИЧЕСКОЙ МОДЕЛИ С СОХРАНЕНИЕМ КАЧЕСТВА ДОСТАТОЧНОСТИ ЦЕЛЕВОЙ УСТАНОВКЕ ПОСТРОЕНИЯ МОДЕЛИ..... 74

Ярошевич Л.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет кино и телевидения
ПАУЗЫ В ИЗОБРАЗИТЕЛЬНЫХ СИСТЕМАХ 74

СОВРЕМЕННЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ 76

Абрамов М.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ЗАЩИТА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ НА ИНТЕРНЕТ-ПОРТАЛЕ РЕДАКЦИИ ЭЛЕКТРОННОГО НАУЧНОГО ЖУРНАЛА 76

Аранов В.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет
ЗАЩИТА ИСПОЛНЯЕМОГО МАШИННОГО КОДА ОТ ОБРАТНОГО ПРОЕКТИРОВАНИЯ ПРИ ПОМОЩИ МНОГОУРОВНЕВОЙ ВИРТУАЛИЗАЦИИ 76

Алексеев А.В., Марченко А.В., Удодова Е.Н., Горбачев Р.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
ПРАКТИКА ФОРМИРОВАНИЯ КОГНИТИВНЫХ БАЗ ДАННЫХ И ЗНАНИЙ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЭКСПЛУАТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ И ОЦЕНКИ КОНКУРЕНТНОЙ СПОСОБНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ 77

Алексеев А.В., Потехин В.С.
Россия, Санкт-Петербург, Институт автоматизации процессов борьбы за живучесть корабля, судна, НИИ (оперативно-стратегических исследований строительства ВМФ) ВУНЦ ВМФ «Военно-морская академия»
ТЕХНОЛОГИЯ И ПРАКТИКА ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ И ИНТЕЛЛЕКТУАЛЬНОЙ ПОДДЕРЖКИ ЛИЦ, ОБОСНОВЫВАЮЩИХ И ПРИНИМАЮЩИХ РЕШЕНИЯ, КАК СРЕДСТВО ЗАЩИТЫ ОТ ВНУТРЕННИХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ..... 78

Андрущенко Д.М.
Украина, Запорожье, Запорожский национальный технический университет
МЕТОД ЗАЩИТЫ АВТОРСКОГО ПРАВА НА ЦИФРОВЫЕ ИЗОБРАЖЕНИЯ 79

Березин А.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ПОДХОДЫ К ПОСТРОЕНИЮ КРИПТОСХЕМ НА ОСНОВЕ ЗАДАЧ ФАКТОРИЗАЦИИ И ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ 80

Березин А.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ВАРИАНТЫ ЗАДАЧИ ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ ПО СОСТАВНОМУ МОДУЛЮ 81

Березин А.Н., Демьянчук А.А., Рыжков А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ПРОТОКОЛЫ С НУЛЕВЫМ РАЗГЛАШЕНИЕМ, ИСПОЛЬЗУЮЩИЕ АЛГОРИТМЫ ОТКРЫТОГО ШИФРОВАНИЯ..... 82

Блюм В.С. Заболотский В.П.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ПОЛНОТА ИНТЕГРИРОВАННОЙ ЭЛЕКТРОННОЙ МЕДИЦИНСКОЙ КАРТЫ, КАК УСЛОВИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПАЦИЕНТА 83

Богданов А.В., Примакин А.И., Синещук М.Ю., Синещук Ю.И., Яковлева Н.А.
Россия, Санкт-Петербург, Государственный Эрмитаж, Санкт-Петербургский университет МВД России
ПОСТРОЕНИЕ КОНЦЕПТУАЛЬНОЙ МОДЕЛИ НАРУШИТЕЛЯ С ЦЕЛЬЮ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ..... 84

Борзенко Р.А., Вайчикаускас М.А., Молдовян Д.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербургский институт информатики и автоматизации РАН
ПРОТОКОЛЫ ЦИФРОВОЙ ПОДПИСИ НА ОСНОВЕ ГОСТ Р 34.10–2012 85

Бориев З.В.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова
ЗАЩИТА ИНФОРМАЦИИ В БАЗАХ ДАННЫХ 85

Бухарметов М.Р.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПЕРЕДАЧИ ДАННЫХ ПО ОТКРЫТЫМ КАНАЛАМ НА ВОДНОМ ТРАНСПОРТЕ..... 86

Бухарметов М.Р.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова
МЕТОДЫ ОБЕСПЕЧЕНИЯ ЗАЩИЩЕННОГО ДОКУМЕНТООБОРОТА В ТРАНСПОРТНОЙ СФЕРЕ.... 87

Вайчикаускас М.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ПРЕОБРАЗОВАНИЕ ОТКРЫТЫХ ТЕКСТОВ, ШИФРОТЕКСТОВ И РЕЗУЛЬТАТОВ ШИФРОВАНИЯ ДЛЯ ОПРЕДЕЛЕНИЯ КРИПТОГРАФИЧЕСКОЙ СТОЙКОСТИ АЛГОРИТМОВ ГЕНЕРАЦИИ КЛЮЧЕВОЙ ИНФОРМАЦИИ..... 88

Вайчикаускас М.А., Мондикова Я.А., Фахрутдинов Р.Ш.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербургский институт информатики и автоматизации РАН
АЛГОРИТМ ОТКРЫТОГО ШИФРОВАНИЯ НАД ДВОИЧНЫМ ПОЛЕМ..... 89

Воробьев В.И., Евневич Е.Л., Шкиртиль В.И.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
МОДЕЛИРОВАНИЕ ЗАЩИЩЕННОСТИ СЕРВИСОВ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ..... 90

Деменева А.А.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова
ЗАЩИТА МНФОРМАЦИИ В MICROSOFTOFFICE 90

Десницкий В.А., Котенко И.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
КОНФИГУРИРОВАНИЕ ВСТРОЕННЫХ СИСТЕМ ЗАЩИТЫ В РАМКАХ СЕРВИСОВ МНОГОУРОВНЕВОЙ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА 91

Десницкий В.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ВЕРИФИКАЦИЯ ИНФОРМАЦИОННЫХ ПОТОКОВ В СИСТЕМАХ СО ВСТРОЕННЫМИ УСТРОЙСТВАМИ 92

Десницкий В.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
МЕТОДИКА КОНФИГУРИРОВАНИЯ БЕЗОПАСНОГО ВСТРОЕННОГО УСТРОЙСТВА 93

Дойникова Е.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ПОДХОД К АНАЛИЗУ ЗАЩИЩЕННОСТИ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ СИСТЕМЫ ПОКАЗАТЕЛЕЙ ЗАЩИЩЕННОСТИ 94

Дубенецкий В.А., Цехановский В.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ЗАЩИТА ИНФОРМАЦИИ В КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ УПРАВЛЕНИЯ «РЕСУРС». 95

Зыков В.М.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
АНАЛИЗ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ 95

Игнатьев М.Б., Шейнин Ю.Е., Литовкин А.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения
НА ПУТИ К ЭКАФЛОПОВСКИМ МАШИНАМ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ – ОТ ЦИФРОВЫХ АНАЛОГОВ ЧЕРЕЗ РЕКУРСИВНЫЕ СТРУКТУРЫ К КВАНТОВЫМ КОМПЬЮТЕРАМ 96

Игнатьев М.Б., Герасимов Г.М., Липинский Я.А., Макин П.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения
АВТОНОМНЫЙ АДАПТИВНЫЙ ШАГАЮЩИЙ РОБОТ ДЛЯ ДИАГНОСТИКИ ГАЗОПРОВОДОВ 98

Игнатьев М.Б., Катермина Т.С., Ненашев В.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения*, Нижневартовский государственный университет
ПРОБЛЕМА ПРОГНОЗИРОВАНИЯ ЗЕМЛЕТРЯСЕНИЙ ПУТЕМ МОДЕЛИРОВАНИЯ ДВИЖЕНИЯ КОНТИНЕНТАЛЬНЫХ ПЛИТ 99

Карпина А.С.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова
ОРГАНИЗАЦИОННОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ НА ПРИМЕРЕ ТРАНСПОРТНО-ЛОГИСТИЧЕСКИХ КЛАСТЕРОВ 99

Кетов Д.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет
ПРОГРАММНЫЕ СРЕДСТВА КОНТРОЛЯ ДИНАМИЧЕСКОЙ ЦЕЛОСТНОСТИ ПРИКЛАДНЫХ ПРОЦЕССОВ В ОПЕРАЦИОННЫХ СИСТЕМАХ ВЫСОКОПРОИЗВОДИТЕЛЬНЫХ МЕЖСЕТЕВЫХ ЭКРАНОВ 100

Козина Г.Л., Никулищев Г.И.
Украина, Запорожье, Запорожский национальный технический университет
ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ЭЛЛИПТИЧЕСКИХ КРИВЫХ НАД КОНЕЧНЫМ ВЕКТОРНЫМ ПОЛЕМ В СХЕМАХ СЛЕПОЙ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ 101

Козьмовский Д.В., Куватов В.И., Примакин А.И.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
МЕТОДЫ АНАЛИЗА ТРАФИКА В ИНТЕРЕСАХ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И КОНТРОЛЯ СЕТЕВОЙ ДЕЯТЕЛЬНОСТИ ПОЛЬЗОВАТЕЛЕЙ РАСПРЕДЕЛЕННЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ..... 102

Коноплев А.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет
ЗАЩИТА ВЫСОКОПРОИЗВОДИТЕЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ НА ОСНОВЕ АВТОМАТИЧЕСКОГО УПРАВЛЕНИЯ ДОСТУПОМ ЗАДАНИЙ К ВЫЧИСЛИТЕЛЬНЫМ УЗЛАМ..... 103

Копыльцов А.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
СОХРАНЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ ДАННЫХ ПРИ ПОДДЕРЖКЕ ПРИНЯТИЯ РЕШЕНИЙ НА ОСНОВЕ ИЗВЛЕКАЕМОЙ СПЕЦИАЛЬНЫМ ОБРАЗОМ ИНФОРМАЦИИ 104

Копыльцов А.В., Сорокин И.В.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена
МОДЕЛИ РАСПОЗНАВАНИЯ ВРЕДОНОСНЫХ ПРОГРАММ НА ОСНОВЕ ЭНТРОПИЙНЫХ ХАРАКТЕРИСТИК ... 104

Корниенко А.А., Глухов А.П.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения,
Москва, ОАО «РЖД»
СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ЖЕЛЕЗНОДОРОЖНОМ ТРАНСПОРТЕ: СОВРЕМЕННОЕ СОСТОЯНИЕ И ЗАДАЧИ СОВЕРШЕНСТВОВАНИЯ 105

Корт С.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет
АНАЛИЗ ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ GPU ДЛЯ ПОСТРОЕНИЯ СИГНАТУРНЫХ СИСТЕМ ОБНАРУЖЕНИЯ АТАК 106

Котенко И.В., Новикова Е.С.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ПОДХОД К ПОСТРОЕНИЮ СИСТЕМЫ ВИЗУАЛЬНОГО АНАЛИЗА ДЛЯ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ ИНТЕЛЛЕКТУАЛЬНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ЖЕЛЕЗНОДОРОЖНОГО КОМПЛЕКСА РОССИИ..... 106

Котенко И.В., Саенко И.Б.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
О ПОСТРОЕНИИ МНОГОУРОВНЕВОЙ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ НА ЖЕЛЕЗНОДОРОЖНОМ ТРАНСПОРТЕ..... 107

Котенко И.В., Саенко И.Б., Полубелова О.В., Дойникова Е.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ОНТОЛОГИЯ ПОКАЗАТЕЛЕЙ ЗАЩИЩЕННОСТИ КОМПЬЮТЕРНОЙ СЕТИ КАК ОСНОВА ВЫРАБОТКИ КОНТРМЕР 108

Култышев Е.И., Полонский А.М., Степанов А.Г.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения
КЛАССИФИКАЦИЯ СИСТЕМЫ УПРАВЛЕНИЯ ОБУЧЕНИЕМ MOODLE С ПОЗИЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 109

Купреенко С.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет
МОДЕЛИ И МЕТОДЫ ОРГАНИЗАЦИИ ПАРАЛЛЕЛЬНЫХ ВЫЧИСЛЕНИЙ ПРИ РЕШЕНИИ ЗАДАЧИ УПРАВЛЕНИЯ ДОСТУПОМ К ИНФОРМАЦИОННЫМ РЕСУРСАМ..... 110

Мальцев В.А
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова
АППАРАТНЫЕ СРЕДСТВА, ИСПОЛЬЗУЮЩИЕСЯ ПРИ ПОСТРОЕНИИ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННО-ЗАЩИЩЕННЫЕ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ..... 111

Мальцев В.А.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова
ПРОГРАММНЫЕ СРЕДСТВА, ИСПОЛЬЗУЮЩИЕСЯ ПРИ ПОСТРОЕНИИ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННО-ЗАЩИЩЕННЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ 112

Масюк А.А., Сараджишвили С.Э.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет
МЕТОДЫ КАТЕГОРИЗАЦИИ ПОЛНОТЕКСТОВЫХ РЕСУРСОВ В СИСТЕМАХ КОНТЕНТНОЙ ФИЛЬТРАЦИИ 113

Михайлов Н.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ВИЗУАЛИЗАЦИЯ КОНТРОЛИРУЕМЫХ ЗОН И ГРУПП ПОЛЬЗОВАТЕЛЕЙ ПРИ АНАЛИЗЕ СТЕПЕНИ ЗАЩИЩЕННОСТИ КРИТИЧНЫХ ДОКУМЕНТОВ ОТ СОЦИО-ИНЖЕНЕРНЫХ АТАК С УЧЁТОМ СТРУКТУРЫ СВЯЗЕЙ МЕЖДУ ПОЛЬЗОВАТЕЛЯМИ ИНФОРМАЦИОННОЙ СИСТЕМЫ 114

Молдовян Д.Н., Мондикова Я.А., Горячев А.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
АЛГОРИТМ КОММУТАТИВНОГО ОТРИЦАЕМОГО ШИФРОВАНИЯ 114

Муравьев А.В., Мондикова Я.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и информатизации РАН,
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ СЛАБОЙ КРИПТОГРАФИИ 116

Муравьев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и информатизации РАН
ТЕХНОЛОГИЯ АВТОМАТИЗИРОВАННОЙ ПРОВЕРКИ НАЛИЧИЯ НЕЛЕГИТИМНЫХ ПОЛЬЗОВАТЕЛЕЙ В СИСТЕМЕ 117

Нестерук Ф.Г.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ТЕНДЕНЦИИ РАЗВИТИЯ АДАПТИВНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ 117

Нечитайленко Р.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕЖИМЕ ФИЛЬТРАЦИИ ИНФОРМАЦИИ В ТЕРРИТОРИАЛЬНО-РАЗНЕСЕННОЙ СИСТЕМЕ 118

Никифоров О.Г., Стародубцев Ю.И.
Россия, Санкт-Петербург, ОАО «НИИ «Рубин»
О ПРИМЕНЕНИИ МЕТОДОВ МНОГОУРОВНЕВОЙ МНОГОПОЗИЦИОННОЙ ЗАЩИТЫ В ЗАДАЧАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 119

Новикова Е.С.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ВЫЯВЛЕНИЕ АНОМАЛЬНОЙ АКТИВНОСТИ В СИСТЕМЕ МОБИЛЬНЫХ ДЕНЕЖНЫХ ПЕРЕВОДОВ С ПОМОЩЬЮ МЕТОДОВ ВИЗУАЛЬНОГО АНАЛИЗА 120

Парфенов Н.П.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
ПОЛОЖЕНИЕ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКА – СОСТАВНОЕ ЗВЕНО СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ПРЕДПРИЯТИЯ 120

Перервенко А.В.
Россия, Санкт-Петербург, ЗАО «АСИС»
АДАПТАЦИЯ КОРПОРАТИВНОЙ МЕТОДИКИ ОЦЕНКИ РИСКОВ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РС БР ИББС-2.2-2009 ДЛЯ КРУПНЫХ КРЕДИТНЫХ ОРГАНИЗАЦИЙ 121

Пичугин Ю.А., Фаткиева Р.Р.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена, Санкт-Петербургский институт информатики и автоматизации РАН
КОСВЕННЫЕ ПРИЗНАКИ КОМПЬЮТЕРНОЙ АТАКИ НА ОСНОВЕ СПЕКТРАЛЬНОГО АНАЛИЗА СЕТЕВОГО ТРАФИКА В РАЗРАБОТКЕ СРЕДСТВ ИНФОРМАЦИОННОЙ ЗАЩИТЫ 122

Примакин А.И.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
ПОЛИТИКА БЕЗОПАСНОСТИ, КАК КЛЮЧЕВОЕ ЗВЕНО СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ХОЗЯЙСТВУЮЩЕГО СУБЪЕКТА 123

Рудакова С.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ВЫБОР МЕТРИК ДЛЯ ПРОВЕДЕНИЯ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 124

Рыжков А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ПОДХОД К ВЕРОЯТНОСТНОМУ КОДИРОВАНИЮ СООБЩЕНИЙ ТОЧКАМИ ЭЛЛИПТИЧЕСКОЙ КРИВОЙ 124

Рыжков А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ВЫБОР ПАРАМЕТРОВ ДЛЯ ПОСТРОЕНИЯ «ИДЕЛЬНЫХ» АЛГОРИТМОВ КОММУТАТИВНОГО ШИФРОВАНИЯ 125

Соколов С.С., Карпина А.С.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова
УМЕНЬШЕНИЕ ВЕРОЯТНОСТИ РЕАЛИЗАЦИИ УГРОЗЫ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ТРАНСПОРТНО-ЛОГИСТИЧЕСКИХ КЛАСТЕРОВ МЕТОДОМ СТРУКТУРНОГО СИНТЕЗА ИНФОРМАЦИОННЫХ ПОТОКОВ 126

Супрун А.Ф.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет
МЕТОДИКА ОЦЕНКИ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ОТ УТЕЧКИ ИНФОРМАЦИИ ЗА СЧЕТ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ 127

Чечулин А.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ПРИМЕНЕНИЕ АНАЛИТИЧЕСКОГО МОДЕЛИРОВАНИЯ ДЛЯ ПОВЫШЕНИЯ УРОВНЯ ЗАЩИЩЕННОСТИ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ 127

Шерстюк М.Ю., Воронков К.Л.
Россия, Санкт-Петербург, ЗАО «Институт инфотелекоммуникаций»
ОСОБЕННОСТИ ВЕДЕНИЯ ЭЛЕКТРОННЫХ МЕДИЦИНСКИХ ПЕРСОНАЛЬНЫХ ЗАПИСЕЙ 128

Шоров А.В., Чечулин А.А., Котенко И.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
КАТЕГОРИРОВАНИЕ ВЕБ-САЙТОВ ДЛЯ СИСТЕМ БЛОКИРОВАНИЯ ВЕБ-САЙТОВ С НЕПРИЕМЛЕМЫМ СОДЕРЖИМЫМ НА ОСНОВЕ АНАЛИЗА ТЕКСТОВОЙ И ГРАФИЧЕСКОЙ ИНФОРМАЦИИ 129

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ 131

Аверьянов Е.Г.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПРОЦЕССОВ МАРШРУТИЗАЦИИ В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ ... 131

Авраменко В.С.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного
СТРАТЕГИИ УПРЕЖДАЮЩЕЙ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ 131

Авраменко В.С., Маликов А.В.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного
ПРОБЛЕМА ДИАГНОСТИРОВАНИЯ НАРУШЕНИЙ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ 132

Агеев С.А.
Россия, Санкт-Петербург, ЗАО «ПКБ «РИО»
ИНТЕЛЛЕКТУАЛЬНОЕ ИЕРАРХИЧЕСКОЕ УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЗАЩИЩЕННЫХ МУЛЬТИСЕРВИСНЫХ СЕТЯХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ 133

Буренин А.Н.
Россия, Санкт-Петербург, ОАО «НИИ «Рубин»
МОДЕЛИ МОНИТОРИНГА СОВРЕМЕННЫХ ЗАЩИЩЕННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ 133

Верзун Н.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
МОДЕЛЬ ПРОЦЕССА ПЕРЕДАЧИ ИНФОРМАЦИИ В СЕТИ С РАЗГРАНИЧЕНИЕМ ПРАВ ДОСТУПА С ИСПОЛЬЗОВАНИЕМ УСТРОЙСТВА КОНТРОЛЯ ДОСТУПА 134

Воронков К.Л., Логинов А.А., Шерстюк Ю.М.
Россия, Санкт-Петербург, ЗАО «Институт инфотелекоммуникаций»
ПРИМЕНЕНИЕ ОДНОНАПРАВЛЕННЫХ ШЛЮЗОВ В СИСТЕМАХ МОНИТОРИНГА ТЕЛЕКОММУНИКАЦИЙ 135

Воронков К.Л., Рожнов М.Д.
Россия, Санкт-Петербург, ЗАО «Институт инфотелекоммуникаций»
РОЛЕВАЯ МОДЕЛЬ РАЗГРАНИЧЕНИЯ ДОСТУПА К СЕРВИСАМ УПРАВЛЕНИЯ ТЕЛЕКОММУНИКАЦИЯМИ 135

Воронков К.Л., Таран В.В., Шерстюк К.Ю., Шерстюк Ю.М.
Россия, Санкт-Петербург, ЗАО «Институт инфотелекоммуникаций»
ИНФОРМАЦИОННАЯ ИНТЕГРАЦИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМЕ УПРАВЛЕНИЯ ТЕЛЕКОММУНИКАЦИЯМИ 136

Выговский Л.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им.В.И. Ульянова (Ленина)
ПРОБЛЕМЫ ЛИЧНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ОБЛАЧНЫХ ПРИЛОЖЕНИЙ 137

Григорьев В.А., Хворов И.А.
Россия, Санкт-Петербург, ООО «Лаборатория инфокоммуникационных сетей»,
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
ТЕХНОЛОГИЯ DSRC КАК ОСНОВА РЕАЛИЗАЦИИ СЕТИ ПЕРЕДАЧИ ДАННЫХ В ИНТЕЛЛЕКТУАЛЬНЫХ ТРАНСПОРТНЫХ СИСТЕМАХ 138

Гурьев С.Н., Дмитриенко О.А.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного
ПОСТРОЕНИЕ ВИРТУАЛЬНЫХ ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ В ЛВС СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ 138

Гурьев С.Н., Емцова А.А.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного
ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ БЕСПРОВОДНЫХ СЕТЕЙ В ТАКТИЧЕСКОМ ЗВЕНЕ УПРАВЛЕНИЯ 139

Гурьянова Я.М., Деньжонков К.А., Кий В.Я.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного
ПОВЫШЕНИЕ ЗАЩИЩЕННОСТИ РАСПРЕДЕЛЕННОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ВВУЗ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ VPN 140

Давыдов А.В., Синюк А.Д.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного
МЕТОД ОТКРЫТОГО КЛЮЧЕВОГО СОГЛАСОВАНИЯ СЕТИ СВЯЗИ 140

Демидов А.А.
Россия, Санкт-Петербург, Комитет по телекоммуникациям и информатизации
Ленинградской области
ОБЩИЕ КОНЦЕПТУАЛЬНЫЕ ПОЛОЖЕНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
НА ОБЪЕКТАХ ОРГАНОВ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ..... 141

Деньжонков К.А.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного
НАПРАВЛЕНИЯ РАЗВИТИЯ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ УЗЛОВ СВЯЗИ 143

Деньжонков К.А., Кий А.В.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного
УПРАВЛЕНИЕ ДОСТУПОМ К ИНФОРМАЦИОННЫМ РЕСУРСАМ АВТОМАТИЗИРОВАННЫХ
СИСТЕМ С ПРИМЕНЕНИЕМ МЕТОДОВ ПОСЛЕДОВАТЕЛЬНОГО АНАЛИЗА ДАННЫХ..... 144

Дормидонтов А.А., Зубакин В.В., Кривошеева М.В.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного
АНАЛИЗ СПОСОБОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ ЛОКАЛЬНЫХ
ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ 145

Калинин М.О., Павленко Е.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ УПРАВЛЕНИЯ УЗЛАМИ ПРОГРАММНО-КОНФИГУРИРУЕМЫХ
СЕТЕЙ..... 145

Кий А.В. Морозов И.В.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного
СХЕМА КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ В ГЕОИНФОРМАЦИОННЫХ СИСТЕМАХ 146

Кононов О.А., Кононова О.В.
Россия, Санкт-Петербург, Смольный институт РАО, Санкт-Петербургский государственный
университет аэрокосмического приборостроения
О ГУМАНИТАРНЫХ АСПЕКТАХ ИНФОКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ 147

Крживокольский Д.В.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного
ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ ДЕКАМЕТРОВЫХ ПАКЕТНЫХ СЕТЕЙ
ЗА СЧЕТ ПРИМЕНЕНИЯ АЛГОРИТМОВ ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ ЧАСТОТНЫМ
РЕСУРСОМ 147

Курилов Д.А., Костиков В.В.
Россия, Санкт-Петербург, ЗАО «Институт инфотелекоммуникаций»
КОНТРОЛЬ ДОСТУПНОСТИ ХОСТОВ IP-СЕТИ..... 148

Логинов А.А., Олимпиев А.А., Рожнов М.Д.
Россия, Санкт-Петербург, ЗАО «Институт инфотелекоммуникаций»
АРХИВАЦИЯ И ВОССТАНОВЛЕНИЕ ДАННЫХ СЛУЖБ УПРАВЛЕНИЯ ТЕЛЕКОММУНИКАЦИЯМИ . 148

Лопатин Д.В., Анурьева М.С., Ерёмина Е.А., Лопатина М.В., Калинина Ю.В.
Россия, Тамбов, Тамбовский государственный университет имени Г.Р. Державина
АКТУАЛЬНЫЙ УРОВЕНЬ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ УГРОЗ ДЛЯ ПОЛЬЗОВАТЕЛЯ
..... 149

Моляков А.С.
Россия, Москва, ФГУП «НИИ «Квант»
ИССЛЕДОВАНИЕ НОВЫХ МОДЕЛЕЙ И МЕТОДОВ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТЬЮ С ЦЕЛЬЮ ПРОТИВОДЕЙСТВИЯ СРЕДСТВАМ СКРЫТОГО ВОЗДЕЙСТВИЯ ... 150

Никифоров О.Г.
Россия, Санкт-Петербург, ОАО «НИИ «Рубин»
О ПОДХОДЕ К СИНТЕЗУ СИСТЕМЫ МНОГОУРОВНЕВОЙ МНОГОПОЗИЦИОННОЙ ЗАЩИТЫ 150

Овчинников А.В., Чуднов А.М.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного
ОПТИМИЗАЦИЯ ПРИЕМНИКА С «МЯГКИМ» РЕШАЮЩИМ ПРАВИЛОМ В УСЛОВИЯХ ПРЕДНАМЕРЕННЫХ ПОМЕХ 151

Олимпиев А.А., Шерстюк Ю.М.
Россия, Санкт-Петербург, ЗАО «Институт инфотелекоммуникаций»
ВОЗМОЖНОСТИ И ВАРИАНТЫ РАЗГРАНИЧЕНИЯ ДОСТУПА К ОБЪЕКТНОЙ МОДЕЛИ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ 151

Паращук И.Б.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного
СЕТЕВОЙ МОНИТОРИНГ КАК КЛЮЧЕВОЙ ЭТАП ПОДГОТОВКИ И ПРИНЯТИЯ РЕШЕНИЯ ПО УПРАВЛЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ РЕГИОНАЛЬНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ 152

Платонов В.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет
АНАЛИЗ ПОДХОДОВ К ОБНАРУЖЕНИЮ СЕТЕВЫХ АТАК В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ 153

Платонов В.В., Семенов П.О.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет
МЕТОДЫ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА В ЗАДАЧЕ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК 154

Сазонов В.В., Манаенко С.С., Беззубов О.В.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного
О НЕОБХОДИМОСТИ СИНТЕЗА АНСАМБЛЕЙ ДИСКРЕТНЫХ ОРТОГОНАЛЬНЫХ СИГНАЛОВ ДЛЯ ЗАЩИЩЕННЫХ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ 155

Синюк А.Д.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного
МЕТОДИКА ОЦЕНКИ ЭФФЕКТИВНОСТИ ОТКРЫТОГО СЕТЕВОГО КЛЮЧЕВОГО СОГЛАСОВАНИЯ 155

Старков А.М.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного
ПРОБЛЕМА ОПЕРАТИВНОГО УПРАВЛЕНИЯ ВИРТУАЛЬНЫМИ ВЫЧИСЛИТЕЛЬНЫМИ СЕТЯМИ В КОРПОРАТИВНЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ 156

Суворова А.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
УГРОЗООБРАЗУЮЩЕЕ ПОВЕДЕНИЕ В СЕТИ ИНТЕРНЕТ: МЕТОДЫ ОЦЕНКИ ПАРАМЕТРОВ 157

Тарасов О.М., Кузнецова О.В., Мусаева Г.К.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного
ПОИСК ОПТИМАЛЬНОГО ПРОСТРАНСТВЕННОГО ПОЛОЖЕНИЯ ВВОДИМЫХ В СИСТЕМУ СВЯЗИОБЪЕКТОВ ПО МИНИМАЛЬНОСТИ СУММАРНОГО РАССТОЯНИЯ ДО КОРРЕСПОНДИРУЮЩИХ УЗЛОВ 157

Удалов В.С.
Россия, Лодейное Поле, Свирский район гидросооружений и судоходства – филиал ФБУ «Администрация «Волго-Балт»
ИСПОЛЬЗОВАНИЕ СХЕМ ПАРАЛЛЕЛЬНОГО КОМПЛЕКСИРОВАНИЯ С ЦЕЛЬЮ ПОВЫШЕНИЯ ЭЛЕКТРОМАГНИТНОЙ ЗАЩИЩЕННОСТИ (ЭМЗИК) КАНАЛОВ CDMA 158

Черняков А.В.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ В ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ 159

Шерстюк Ю.М., Воронков К.Л., Олимпиев А.А.
Россия, Санкт-Петербург, ЗАО «Институт инфотелекоммуникаций»
ВИДЫ ПРАВ И ПОЛНОМОЧИЙ В КОМПЛЕКСЕ СЛУЖБ УПРАВЛЕНИЯ ТЕЛЕКОММУНИКАЦИЯМИ 160

Шерстюк Ю.М., Костиков В.В., Курилов Д.А.
Россия, Санкт-Петербург, ЗАО «Институт инфотелекоммуникаций»
СЕРВИСНЫЕ СРЕДСТВА ТЕХНОЛОГИЧЕСКОГО КОНТРОЛЯ ТЕЛЕКОММУНИКАЦИОННОГО ОБОРУДОВАНИЯ 161

Шерстюк Ю.М., Логинов А.А., Олимпиев А.А., Шерстюк К.Ю.
Россия, Санкт-Петербург, ЗАО «Институт инфотелекоммуникаций»
МИГРАЦИЯ ПОЛНОМОЧИЙ УПРАВЛЕНИЯ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ 162

Шерстюк Ю.М., Логинов А.А., Рожнов М.Д., Таран В.В.
Россия, Санкт-Петербург, ЗАО «Институт инфотелекоммуникаций»
УРОВНИ ЗАЩИТЫ СРЕДСТВ ОПЕРАТИВНОГО УПРАВЛЕНИЯ ТЕЛЕКОММУНИКАЦИЯМИ 162

Шубников М.М.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова
РАДИОЛОКАЦИЯ И РАДИОНАВИГАЦИЯ 163

Ющенко Н.А., Тулупьева Т.В.
Россия, Санкт-Петербург, Северо-Западный институт управления РАНХиГС, Санкт-Петербургский институт информатики и автоматизации РАН
КЛАССИФИКАЦИЯ ПУБЛИКУЕМЫХ ПОСТОВ В АККАУНТАХ ПОЛЬЗОВАТЕЛЕЙ СОЦИАЛЬНЫХ СЕТЕЙ . 164

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ 165

Алексеев А.В.
Россия, Санкт-Петербург, Институт автоматизации процессов борьбы за живучесть корабля, судна
КОНЦЕПЦИЯ РАНГОВОЙ ПАРТНЕРСКОЙ СЕРТИФИКАЦИИ СИСТЕМ ОБРАБОТКИ И ЗАЩИТЫ ИНФОРМАЦИИ КАК СРЕДСТВО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЭКСПЛУАТАЦИИ И КОНКУРЕНТНОСПОСОБНОСТИ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ 165

Алексеев А.В., Марченко А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
ИНФОРМАЦИОННАЯ СИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЭКСПЛУАТАЦИИ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ 166

Верховых Н.И., Перепелкина С.Ю., Франк А.В.
Россия, Екатеринбург, ФГУП «Научно-производственное объединение автоматики имени академика Н.А. Семихатова»
ВОССТАНОВЛЕНИЯ ТЕЛЕМЕТРИЧЕСКОЙ ИНФОРМАЦИИ В УСЛОВИЯХ ИЗБЫТОЧНОСТИ 167

Дмитриев А.Г., Михайленко Е.И., Стефановская Н.В.
Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс»
ПРОТОКОЛ РЕГУЛИРУЕМОГО ВИРТУАЛЬНОГО КАНАЛА ВИРТУАЛЬНОЙ ПРИВАТНОЙ СЕТИ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ 168

Емелин В.И. Михайлов Д.С.
Россия, Санкт-Петербург, ОАО «Научно-исследовательский институт «Вектор»
ОЦЕНКА И ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ УСТОЙЧИВОСТИ В КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТАХ ... 168

Завадский С.В. Филиппова Т.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет, ОАО «Научно-производственное объединение «Импульс»
ВЫСОКОТЕХНОЛОГИЧНЫЕ ИНТЕГРИРОВАННЫЕ РЕШЕНИЯ В ЗАДАЧАХ РАЗРАБОТКИ И ТЕСТИРОВАНИЯ АППАРАТУРЫ ПЕРЕДАЧИ ДАННЫХ 169

Кораблев И.Н., Вологдин М.А., Калугин П.С., Кабанцов К.К.
Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс»
МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ УСТОЙЧИВОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ К АТАКАМ ТИПА «ОТКАЗ В ОБСЛУЖИВАНИИ» 171

Михайленко Е.И.
Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс»
ОСОБЕННОСТИ СЕТЕВОГО ВЗАИМОДЕЙСТВИЯ КРИТИЧЕСКИХ ИНФРАСТРУКТУР С МУЛЬТИСЕРВИСНОЙ СЕТЬЮ ОБЩЕГО ПОЛЬЗОВАНИЯ 172

Михайленко Е.И., Стефановская Н.В., Фомин В.Н.
Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс»
ПРОГРАММНЫЙ КОМПЛЕКС СОВМЕЩЕННОГО КОММУТАТОРА И IP-ШЛЮЗА ОБЪЕКТА КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ 173

Новиков А.Е.
Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс»
БАЗОВЫЕ ТЕХНОЛОГИИ СОЗДАНИЯ И СОПРОВОЖДЕНИЯ АСУ КРИТИЧЕСКИХ ИНФРАСТРУКТУР..... 173

Ростовцев А.Г.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет
СНИЖЕНИЕ СЛОЖНОСТИ ДИФФЕРЕНЦИАЛЬНОЙ АТАКИ НА AES С ИСПОЛЬЗОВАНИЕМ ВИРТУАЛЬНЫХ ИЗОМОРФИЗМОВ 174

ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ 176

Левкин И.М., Микадзе С.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
ОСНОВНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ НА СОВРЕМЕННОМ ЭТАПЕ 176

Безрук Г.Г., Левкина С.В.
Россия, Санкт-Петербург, Региональный центр Главного научно-исследовательского испытательного центра робототехники МО РФ, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
ИНФОРМАЦИОННО-ЛИНГВИСТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ СИТУАЦИОННЫХ ЦЕНТРОВ ЭКОНОМИЧЕСКОГО МОНИТОРИНГА 177

Богатырев В.А., Богатырев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
ВЕКТОРНАЯ ОПТИМИЗАЦИЯ РЕЗЕРВИРОВАННОЙ ДРЕВОВИДНОЙ СЕТИ 178

Богатырев В.А., Алексанков С.М., Демидов Д.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
РЕЗЕРВИРОВАННАЯ ВЫЧИСЛИТЕЛЬНАЯ СИСТЕМА ОГРАНИЧЕННОГО ВОССТАНОВЛЕНИЯ 179

Вербицкий В.С., Утин Л.Л.
Беларуссия, Гомель, Иностранное частное производственное унитарное предприятие «АЛКОПАК»
ОПЫТ ОБЕСПЕЧЕНИЯ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ БЕЗОПАСНОСТИ ОФИСНЫХ ПОМЕЩЕНИЙ В УСЛОВИЯХ ЖЕСТКИХ ФИНАНСОВЫХ ОГРАНИЧЕНИЙ..... 180

Воробьев А.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
СТРУКТУРИЗАЦИЯ КОРПОРАТИВНОГО ЦЕНТРА ОБРАБОТКИ ДАННЫХ..... 181

Гейда А.С.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
МЕТОДИКА ОЦЕНИВАНИЯ КОНКУРЕНТОСПОСОБНОСТИ ИЗДЕЛИЙ И ВЫПУСКАЮЩИХ ИХ ПРЕДПРИЯТИЙ НА ОСНОВЕ ИССЛЕДОВАНИЯ ПОТЕНЦИАЛА СИСТЕМ 181

Гейда А.С., Лысенко И.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
МЕТОД ПЛАНИРОВАНИЯ МОДЕРНИЗАЦИИ ТЕХНОЛОГИЧЕСКОЙ БАЗЫ ПРЕДПРИЯТИЙ В УСЛОВИЯХ РИСКА..... 182

Григорова А.В., Емелин В.И.
Россия, Санкт-Петербург, ОАО «Научно-исследовательский институт «Вектор»
ЗАЩИТА ИНВЕСТИЦИОННЫХ ПРОЕКТОВ В СФЕРЕ НЕДВИЖИМОСТИ ОТ ДЕЙСТВИЙ КОНКУРЕНТНОЙ РАЗВЕДКИ 182

Евдокимов Ю.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
ПРОЕКТИРОВАНИЕ ОСНАСТКИ ДЛЯ УСТРОЙСТВ ЛИНИИ СБОРКИ МИКРООБЪЕКТИВОВ..... 183

Колбанёв М.О., Татарникова Т.М., Воробьев А.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
ДВУХУРОВНЕВАЯ МОДЕЛЬ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ 184

Коршунов И.Л.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
РОЛЬ И МЕСТО ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В НАПРАВЛЕНИИ ПОДГОТОВКИ 080101.65 «ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ»..... 185

Кравченко К.Ю., Утин Л.Л.
Беларуссия, Гомель, Иностранное частное производственное унитарное предприятие «АЛКОПАК»
ОСОБЕННОСТИ ПРОВЕДЕНИЯ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ИНОСТРАННЫХ ПРЕДПРИЯТИЯХ 186

Левкин И.М., Сорокина Е.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
РЕЙДЕРСКИЙ ЗАХВАТ КАК ОСОБАЯ ФОРМА ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКОЙ УГРОЗЫ.. 187

Левкина С.В.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
ОСОБЕННОСТИ КОМПЛЕКСНОЙ ОЦЕНКИ ТЕКУЩЕГО СОСТОЯНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ..... 187

Москвин Д.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет
ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ СОВРЕМЕННЫХ ПОТРЕБИТЕЛЬСКИХ УСТРОЙСТВ 188

Мошак Н.Н.
Россия, Санкт-Петербург, Главное управление Банка России по Ленинградской области
СИСТЕМЫ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ТЕРРИТОРИАЛЬНЫХ УЧРЕЖДЕНИЯХ БАНКА РОССИИ 189

Пичугин Ю.А., Кондрашков А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербургский государственный экономический университет
СТАТИСТИЧЕСКИЕ ОЦЕНКИ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ И РИСКА НА ОСНОВЕ АЛЬТМАНОВСКОГО ПОДХОДА..... 190

Пойманова Е.Д.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
СОВРЕМЕННЫЕ ТЕХНОЛОГИИ СОХРАНЕНИЯ ИНФОРМАЦИИ..... 190

Попова Е.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
МНОГОКРИТЕРИАЛЬНЫЙ ОПТИМИЗАЦИОННЫЙ ВЫБОР СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ (СЗИ) ДЛЯ МАЛЫХ ПРЕДПРИЯТИЙ..... 191

Проснеков С.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
СРАВНИТЕЛЬНЫЙ АНАЛИЗ СВОБОДНОРАСПРОСТРАНЯЕМЫХ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ ДЛЯ ИСПОЛЬЗОВАНИЯ В МАЛОЙ СЕТИ 192

Пуха Г.П.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
СИСТЕМЫ ИНТЕЛЛЕКТУАЛЬНОЙ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ – ИННОВАЦИОННОЕ НАПРАВЛЕНИЕ ИССЛЕДОВАНИЙ И ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИТ..... 193

Тихомиров С.А., Богатырев В.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики,
Санкт-Петербургский государственный экономический университет
АГЕНТНО-ОРИЕНТИРОВАННАЯ СИСТЕМА ЗАЩИТЫ ОТ DDOS-АТАК 194

Филиппов А.Н., Морозов Ю.С., Кондидатов А.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
ПРИМЕНЕНИЕ ОНТОЛОГИИ В МНОГОАГЕНТНОЙ САПР ТП МЕХАНИЧЕСКОЙ ОБРАБОТКИ ДЕТАЛЕЙ 194

Харинов М.В., Заболотский В.П.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ЦЕЛОЧИСЛЕННАЯ ОЦЕНКА КОЛИЧЕСТВА ИНФОРМАЦИИ В ЗАДАЧАХ СТЕГАНОГРАФИИ И РАСПОЗНАВАНИЯ ИЗОБРАЖЕНИЙ 195

Шаршов А.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОГО ВЗАИМОДЕЙСТВИЯ АВТОМАТИЗИРОВАННЫХ ТРАНСПОРТНЫХ ЛИНИЙ С ПРОМЫШЛЕННЫМ ОБОРУДОВАНИЕМ 196

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ГИДРОМЕТЕОРОЛОГИИ 197

Александрова Л.В., Попов Н.Н.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет
УЧЕТ И РАСПРЕДЕЛЕНИЕ СЕТЕВОЙ НАГРУЗКИ С ПОМОЩЬЮ СПЕЦИАЛИЗИРОВАННЫХ СРЕДСТВ МОНИТОРИНГА ОБОРУДОВАНИЯ 197

Григорьев Р.С., Калинин В.О., Моргунов М.А.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРИ ПРОВЕДЕНИИ ГИДРОЛОГИЧЕСКИХ И ГИДРОГРАФИЧЕСКИХ ИССЛЕДОВАНИЙ МИРОВОГО ОКЕАНА 197

Завируха В. К., Замятин А. Ю.
Россия, Санкт-Петербург, Арктический и антарктический научно-исследовательский институт,
Москва, Федеральная служба по гидрометеорологии и мониторингу окружающей среды
СОЗДАНИЕ И ИСПОЛЬЗОВАНИЕ ОБЪЕКТОВЫХ ПУНКТОВ И СЕТЕЙ МНОГОФУНКЦИОНАЛЬНЫХ РАДИОЛОКАЦИОННЫХ КОМПЛЕКСОВ 198

Канаев А.К., Опарин Е.В.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения
МОДУЛЬ СПЕЦИАЛЬНОГО МАТЕМАТИЧЕСКОГО И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ПО АВТОМАТИЗАЦИИ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ УПРАВЛЕНИЯ СЕТЬЮ ТАКТОВОЙ СЕТЕВОЙ СИНХРОНИЗАЦИИ ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЫ ОАО «РЖД» 199

Митько А.В.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет
ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОДВОДНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ В УСЛОВИЯХ АРКТИЧЕСКОГО РЕГИОНА 200

Митько А.В., Авдеенко А.В., Кротенко В.Ю.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет
ПРИНЦИПЫ ЗАЩИТЫ ИНФОРМАЦИИ В ТРЕНАЖЁРНЫХ ОБУЧАЮЩИХ СИСТЕМАХ В ГИДРОМЕТЕОРОЛОГИИ 201

Митько А.В., Авдошина А.И., Халзакова А.А.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет
ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕЖИМЕ «СЕТЕЦЕНТРИЧЕСКИХ ВОЙН» В ГИДРОМЕЕОРОЛОГИИ 201

Привалов А.А., Вандич А.П.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения
МОДУЛЬ СПЕЦИАЛЬНОГО МАТЕМАТИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ ЕДИНОЙ СИСТЕМЫ МОНИТОРИНГА И АДМИНИСТРИРОВАНИЯ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ОАО «РЖД» 202

Привалов А.А., Рыхлов П.В., Чалов И.В., Евглевская Н.В.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения
ОБ УСТРОЙСТВЕ ПРЕДОТВРАЩЕНИЯ ВЫДЕЛЕНИЯ АКУСТИЧЕСКОЙ ИНФОРМАЦИИ В ПОМЕЩЕНИЯХ, ОСВЕЩАЕМЫХ КОМПАКТНЫМИ ЛЮМИНИСЦЕНТНЫМИ ЛАМПАМИ 203

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЭКОЛОГИИ..... 204

Афанасьев В.П., Камышев И.В., Ломовцев С.В., Орехов Д.Л., Теруков Е.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), ООО «НТЦ тонкопленочных технологий в энергетике при ФТИ им. А.Ф. Иоффе»
ПРОБЛЕМЫ ЭКОЛОГИИ И СОВРЕМЕННОЕ СОСТОЯНИЕ ТОНКОПЛЕНОЧНОЙ СОЛНЕЧНОЙ ЭНЕРГЕТИКИ 204

Афанасьев В.П., Бобыль А.В., Иванов Г.А., Ершенко Е.М., Плешков Д.В., Скворцов Д.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Физико-технический институт им. А.Ф. Иоффе РАН
МОНИТОРИНГ ЭФФЕКТИВНОСТИ РАБОТЫ СОЛНЕЧНЫХ МОДУЛЕЙ НА ШИРОТЕ САНКТ-ПЕТЕРБУРГА 204

Агафонова Д.С., Сидоров А.И., Колобкова Е.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
ЛЮМИНЕСЦЕНТНЫЕ ОПТИЧЕСКИЕ СТЕКЛА И ВОЛОКНА КАК ЧУВСТВИТЕЛЬНЫЕ ЭЛЕМЕНТЫ ВОЛОКОННО-ОПТИЧЕСКИХ ДАТЧИКОВ ЭЛЕКТРИЧЕСКОЙ ДУГИ, ИСКРЫ И ТЕМПЕРАТУРЫ ДЛЯ ПРЕДУПРЕЖДЕНИЯ АВАРИЙНЫХ СИТУАЦИЙ..... 205

Алексеева-Попова Н.В., Дроздова И.В., Беляева А.И.
Россия, Санкт-Петербург, Ботанический Институт им. В.Л. Комарова РАН
ОЦЕНКА РЕГИОНАЛЬНОГО ФОНОВОГО УРОВНЯ ТЯЖЕЛЫХ МЕТАЛЛОВ В РАСТЕНИЯХ ПОЧВАХ ПРИ МОНИТОРИНГЕ ЗАГРЯЗНЕНИЯ СРЕДЫ В ЛЕНИНГРАДСКОЙ ОБЛАСТИ..... 206

Бархатов А.В., Веремьев В.И., Ковалев Д.А., Коновалов А.А., Михайлов В.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ИСПОЛЬЗОВАНИЕ СИСТЕМ ПОЛУАКТИВНОЙ РАДИОЛОКАЦИИ В ЭКОЛОГИЧЕСКОМ МОНИТОРИНГЕ ГИДРОСФЕРЫ И АТМОСФЕРЫ..... 207

Бузников А.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ДИСТАНЦИОННАЯ СПЕКТРОМЕТРИЯ РАСТИТИЕЛЬНОГО ПОКРОВА ОДИН ИЗ МЕТОДОВ ОЦЕНКИ ЭКОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ РЕГИОНА..... 207

Бунина Ю.Е., Готюр И.А., Костромитинов А.В.
Россия, Санкт-Петербург, Военно-космическая академия имени А.Ф.Можайского
МЕТОДИКА ВЫЯВЛЕНИЯ И УСТРАНЕНИЯ ИСКАЖЕНИЙ ЭКОЛОГИЧЕСКОЙ ИНФОРМАЦИИ 208

Василевский А.М., Коноплев Г.А., Степанова О.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ОЦЕНКА СТЕПЕНИ ЗАГРЯЗНЕНИЯ ВОДЫ ПО УФ СПЕКТРАМ ПОГЛОЩЕНИЯ 208

Веремьев В.И., Коновалов А.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ ЭКОЛОГИЧЕСКОГО КОНТРОЛЯ ОКРУЖАЮЩЕГО ПРОСТРАНСТВА НА БАЗЕ МНОГОПОЗИЦИОННЫХ РАДИОЛОКАЦИОННЫХ КОМПЛЕКСОВ..... 209

Викторов С.В.
Россия, Санкт-Петербург, Санкт-Петербургский научно-исследовательский центр экологической безопасности РАН, Санкт-Петербургский государственный университет
ЭФФЕКТИВНОСТЬ ДИСТАНЦИОННЫХ МЕТОДОВ ОБНАРУЖЕНИЯ НЕФТЯНЫХ ЗАГРЯЗНЕНИЙ (НА ПРИМЕРЕ БАЛТИЙСКОГО МОРЯ) 210

Горохов В.Л., Витковский В.В., Бузников А.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный архитектурно-строительный университет, Специальная астрофизическая обсерватория РАН, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
КОГНИТИВНЫЕ ОБРАЗЫ МНОГОМЕРНЫХ РАСПРЕДЕЛЕННЫХ БАЗ ДАННЫХ ЭКОЛОГИЧЕСКОГО И КОСМИЧЕСКОГО МОНИТОРИНГА, КАК ИНДИКАТОРЫ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГО ВТОРЖЕНИЯ В ИХ КОНТЕНТ 210

Горохов В.Л., Витковский В.В., Бузников А.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный архитектурно-строительный университет, Специальная астрофизическая обсерватория РАН, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
КОГНИТИВНАЯ ВИЗУАЛИЗАЦИЯ ИНДИКАЦИИ ОПАСНОСТЕЙ ВЫЯВЛЯЕМЫХ НА ОСНОВЕ ДИСТАНЦИОННОГО ЗОНДИРОВАНИЯ..... 210

Горяинов В.С., Бузников А.А., Черноок В.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ВОЗМОЖНОСТЬ ПРИМЕНЕНИЯ ЛИДАРНЫХ СИСТЕМ ДЛЯ КОНТРОЛЯ СОСТОЯНИЯ ВОДНЫХ РЕСУРСОВ 211

Готюр И.А., Кулешов Ю.В., Маков А.Б, Суворов С.С., Щукин Г.Г.
Россия, Санкт-Петербург, Военно-космическая академия имени А.Ф.Можайского
КОНЦЕПЦИЯ СОЗДАНИЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ МЕТЕОРОЛОГИЧЕСКОГО И ЭКОЛОГИЧЕСКОГО ОБЕСПЕЧЕНИЯ КОСМОДРОМА «ВОСТОЧНЫЙ» 211

Гришканич А.С., Бузников А.А., Редька Д.Н., Жевлаков А.П., Кащеев С.В.
Россия, Санкт-Петербург, ОАО «НПК «Государственный оптический институт им С.И. Вавилова», Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
МОНИТОРИНГ МЕТАНОВЫХ ВЫБРОСОВ В АРКТИКЕ ДЛЯ ОЦЕНКИ ИЗМЕНЕНИЯ КЛИМАТА МЕТОДОМ ЛАЗЕРНОГО ЗОНДИРОВАНИЯ..... 212

Гришканич А.С., Бузников А.А., Елизаров В.В., Жевлаков А.П., Кащеев С.В.
Россия, Санкт-Петербург, ОАО «НПК «Государственный оптический институт им С.И. Вавилова», Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ЛИДАРНЫЕ КОМПЛЕКСЫ АВИАЦИОННОГО БАЗИРОВАНИЯ С УЛЬТРАСПЕКТРАЛЬНЫМ РАЗРЕШЕНИЕМ..... 213

Гришканич А.С., Бузников А.А., Елизаров В.В., Жевлаков А.П., Кащеев С.В.
Россия, Санкт-Петербург, ОАО «НПК «Государственный оптический институт им С.И. Вавилова», Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
АЭРОПОИСК МЕСТОРОЖДЕНИЙ УГЛЕВОДОРОДОВ МЕТОДОМ ЛАЗЕРНОГО ЗОНДИРОВАНИЯ. 214

Гришканич А.С., Лобанова Е.Г., Редька Д.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ЭКОЛОГИЧЕСКИЕ ОСОБЕННОСТИ СОЗДАНИЯ ЛАЗЕРНЫХ СИСТЕМ ДИСТАНЦИОННОГО ПИТАНИЯ ФОТОЭЛЕКТРИЧЕСКИХ ПРЕОБРАЗОВАТЕЛЕЙ 215

Захаров И.С., Величко А.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ ТЕМПЕРАТУРНЫХ ПОПУЛЯЦИОННЫХ РЕАКЦИЙ ИНФУЗОРИЙ КАК ИНФОРМАТИВНЫХ ПОКАЗАТЕЛЕЙ ВРЕДНЫХ ФАКТОРОВ В СРЕДЕ 215

Новиков А.В., Летучий Ю.А., Тимощук А.С.
Россия, Санкт-Петербург, Военно-космическая академия имени А.Ф.Можайского
СХЕМА ФУНКЦИОНИРОВАНИЯ КОСМИЧЕСКОГО КОМПЛЕКСА ПРИ РЕШЕНИИ ИНФОРМАЦИОННЫХ ЗАДАЧ МОНИТОРИНГА ЭКОЛОГИЧЕСКОЙ ОБСТАНОВКИ В КОСМОСЕ И ИЗ КОСМОСА 216

Парфенов В.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ПРОБЛЕМЫ ТОЧНОСТИ ИЗМЕРЕНИЙ И СОЗДАНИЯ ЭЛЕКТРОННЫХ 3D-МОДЕЛЕЙ ПРИ МОНИТОРИНГЕ ЭКСТЕРЬЕРНЫХ СКУЛЬПТУРНЫХ ПАМЯТНИКОВ МЕТОДОМ ТРЕХМЕРНОГО ЛАЗЕРНОГО СКАНИРОВАНИЯ 217

Цыганкова И. А.,Заболотский В.П.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ПРОГРАММНЫЙ КОМПЛЕКС ПОДДЕРЖКИ ПРИНЯТИЯ ВРАЧЕБНЫХ РЕШЕНИЙ 218

Шилин Б.В.
Россия, Санкт-Петербург, Санкт-Петербургский центр экологической безопасности РАН
ВИДЕОСПЕКТРАЛЬНЫЙ МЕТОД РЕГИСТРАЦИИ АНТРОПОГЕННОГО СТРЕССА РАСТИТЕЛЬНОСТИ 219

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОЦИОКОМПЬЮТИНГЕ 220

Азаров А.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ФОРМАЛИЗАЦИЯ КОСПЛЕКСА «ИНФОРМАЦИОННАЯ СИСТЕМА — ПЕРСОНАЛ — КРИТИЧНЫЕ ДОКУМЕНТЫ» В ПРОБЛЕМЕ АНАЛИЗА ЗАЩИЩЕННОСТИ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ ОТ СОЦИО-ИНЖЕНЕРНЫХ АТАК 220

Бродовская Е.В.
Россия, Москва, Московский государственный гуманитарный университет им. М.А. Шолохова
ОСОБЕННОСТИ ИССЛЕДОВАНИЯ ПОЛИТИЧЕСКОГО ПРОТЕСТА В РУНЕТЕ: КОГНИТИВНЫЕ КАРТЫ, МАТАФОРЫ, МЕМЫ..... 220

Верт Н.С., Маховенко Е.Б.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет
ДОКАЗУЕМОЕ ХРАНЕНИЕ КОПИЙ ДАННЫХ НА ОБЛАЧНОМ СЕРВЕРЕ..... 221

Долгоруков А.М.
Россия, Москва, Московский государственный университет им. М.В. Ломоносова, Московский государственный гуманитарный университет им. М.А. Шолохова
МЕТОДЫ ИССЛЕДОВАНИЯ ON-LINE СЕТЕЙ В Е-ЭТНОМЕТОДОЛОГИЧЕСКОЙ ПЕРСПЕКТИВЕ 222

Завируха В. К., Байгутлина И.А., Замятин А.Ю., Цыпанов С.А.
Россия, Санкт-Петербург, Арктический и антарктический научно-исследовательский институт, Болгария, Несебр, ООД «Синергия Инвест»
ИСКАЖЕНИЕ ИСТОРИИ РОССИИ В РЕЗУЛЬТАТЕ ИНФОРМАЦИОННОЙ ВОЙНЫ 223

Корт С.С., Евдокимов Д.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет
ДИНАМИЧЕСКАЯ БИНАРНАЯ ИНСТРУМЕНТАЦИЯ. ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ..... 224

Лаврова Д.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет
ПАРАЛЛЕЛЬНАЯ ОБРАБОТКА СЕТЕВОГО ТРАФИКА ДЛЯ АНАЛИЗА БЕЗОПАСНОСТИ ПЕРЕДАВАЕМЫХ ОБЪЕКТОВ 224

Нечаев В.Д.
Россия, Москва, Московский государственный гуманитарный университет им. М.А. Шолохова
ГРАНИЦЫ СВОБОДЫ И БЕЗОПАСНОСТИ В ПРОСТРАНСТВЕ ИНТЕРНЕТ В ОЦЕНКАХ РОССИЙСКИХ ПОЛЬЗОВАТЕЛЕЙ (ПО РЕЗУЛЬТАТАМ ИССЛЕДОВАНИЯ WORLD INTERNET PROJECT IN RUSSIA - 2012) 226

Торопова А.В., Фроленков К.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ЗАДАЧА МОДЕЛИРОВАНИЯ РАСПРОСТРАНЕНИЯ МНЕНИЙ НА ОСНОВЕ КОМПЛЕКСНОГО АНАЛИЗА ЭЛЕКТРОННЫХ СОЦИАЛЬНЫХ СЕТЕЙ 227

Тулупьев А.Л., Абрамов М.В., Азаров А.А., Тулупьева Т.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ЗАЩИТА КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ НА ИНТЕРНЕТ-ПОРТАЛЕ РЕДАКЦИИ ЭЛЕКТРОННОГО НАУЧНОГО ЖУРНАЛА 227

Тулупьев А.Л., Тулупьева Т.В., Азаров А.А., Фильченков А.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
АЛГОРИТМЫ АНАЛИЗА ЗАЩИЩЕННОСТИ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ ОТ СОЦИО-ИНЖЕНЕРНЫХ АТАК 228

Тулупьев А.Л., Тулупьева Т.В., Михайлов Н.Ю., Азаров А.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
РАЗГРАНИЧЕНИЕ ДОСТУПА К ИНФОРМАЦИОННЫМ РЕСУРСАМ С ЦЕЛЬЮ ЗАЩИТЫ КРИТИЧНЫХ ДОКУМЕНТОВ ПОЛЬЗОВАТЕЛЕЙ ОТ СОЦИО-ИНЖЕНЕРНЫХ АТАК 228

Фильченков А.А., Суворова А.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
РАЗЛИЧИЕ В ГРАФАХ РАСПРОСТРАНЕНИЯ ВИРУСОВ И ВИРУСНЫХ МАТЕРИАЛОВ В СОЦИАЛЬНЫХ СЕТЯХ 228

Чиркин Е.С.
Россия, Тамбов, Тамбовский государственный университет им. Г.Р. Державина
ОПАСНОСТЬ ИСПОЛЬЗОВАНИЯ ОРИГИНАЛЬНЫХ ФАЙЛОВ В СИСТЕМАХ АВТОМАТИЗИРОВАННОЙ ПРОВЕРКИ НА ПЛАГИАТ 229

Шаповалов В.Л., Бубнов А.Ю.
Россия, Москва, Московский государственный гуманитарный университет им. М.А. Шолохова
ОСНОВНЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ АУДИТОРИИ РУНЕТА (ПО РЕЗУЛЬТАТАМ ИССЛЕДОВАНИЯ WORLD INTERNRT PROJECT IN RUSSIA - 2012) 230

Щедрин П.О.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ СТАНЦИИ ОКОНЧАТЕЛЬНОЙ СБОРКИ МИКРООБЪЕКТИВОВ 231

ПОДГОТОВКА И ПЕРЕПОДГОТОВКА КАДРОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 232

Абрамян Г.В.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена
ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ НЕЛИНЕЙНОГО РАЗВИТИЯ СОВРЕМЕННОГО РЕГИОНАЛЬНОГО ОБРАЗОВАНИЯ И ПОДГОТОВКИ КАДРОВ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 232

Барабаш П.А.
Россия, Санкт-Петербург, Смольный институт Российской академии образования
ОСОБЕННОСТИ ПРЕПОДАВАНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ «ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ» 232

Барабаш П.А.
Россия, Санкт-Петербург, Смольный институт Российской академии образования
О НЕОБХОДИМОСТИ РАЗДЕЛА ПО ИНФОРОМАЦИОННОЙ БЕЗОПАСНОСТИ В УЧЕБНОЙ ДИСЦИПЛИНЕ «ИНФОКОММУНИКАЦИОННЫЕ СИСТЕМЫ И СЕТИ » 233

Белая Т.И.
Россия, Санкт-Петербург, Северо-Западный институт печати Санкт-Петербургского государственного университета технологии и дизайна
ЧЕЛОВЕК КАК ОСНОВНОЙ ЭЛЕМЕНТ СИСТЕМЫ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ 234

Залещанский Б.Д., Свиридов А.П., Павлова О.А., Шалобина Е.А.
Россия, Москва, Московский государственный технический университет радиотехники, электроники и автоматики
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СОЦИО-ТЕХНИЧЕСКИХ СИСТЕМ ЭКОНОМИЧНЫМИ СТРАТЕГИЯМИ УПРАВЛЕНИЯ ПОДГОТОВКОЙ ПЕРСОНАЛА 235

Касаткин В.В., Советов Б.Я., Цехановский В.В.
Россия, Санкт-Петербург, Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ПРОФИЛЬ ПОДГОТОВКИ БАКАЛАВРОВ «БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ» В СОСТАВЕ НАПРАВЛЕНИЯ «ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ» 235

Куватов В.И., Пантиховский О.В., Примакин А.И., Синещук Ю.И.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России, ВУНЦ ВМФ «Военно-морская академия имени Адмирала Флота Советского Союза Н.Г. Кузнецова»
ПРИМЕНЕНИЕ БЛОЧНО-МОДУЛЬНЫХ ТЕХНОЛОГИЙ ДЛЯ ОПТИМИЗАЦИИ УЧЕБНЫХ ПЛАНОВ И ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ПОДГОТОВКИ КУРСАНТОВ ПО СПЕЦИАЛЬНОСТИ 090915.65 – «БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРАВООХРАНИТЕЛЬНОЙ СФЕРЕ» 236

Морозов В.Е., Дрозд А.В.
Россия, Москва, ООО «Новые поисковые технологии»
ОБУЧЕНИЕ СПЕЦИАЛИСТОВ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВОПРОСАМ ПРАКТИЧЕСКОГО ИСПОЛЬЗОВАНИЯ DLP-СИСТЕМ 237

Пантюхин О.И.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного
ПРЕПОДАВАНИЕ СОВРЕМЕННЫХ ДИСЦИПЛИН В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 238

Раскин А.В., Фральцова Т.А.
Россия, Москва, Войска воздушно-космической обороны, Институт повышения квалификации ТЭК
ОСОБЕННОСТИ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В СФЕРЕ ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ 239

Рябова А.А.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова
ИСПОЛЬЗОВАНИЕ СИСТЕМЫ ДИСТАНЦИОННОГО ОБУЧЕНИЯ «ФАРВАТЕР» В ПОДГОТОВКЕ КВАЛИФИЦИРОВАННЫХ КАДРОВ 239

Салтыков Е.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
ПОИСК И АНАЛИЗ УЯЗВИМОСТЕЙ В ПРОГРАММЕ «АВЕРС: ЭЛЕКТРОННЫЙ КЛАССНЫЙ ЖУРНАЛ» 240

Ходаков А.И., Колодин М.Ю., Вус М.А.
Россия, Санкт-Петербург, ООО «Академия информационных технологий», Санкт-Петербургский институт информатики и автоматизации РАН
ИНСТРУМЕНТАРИЙ ИНФОРМАЦИОННОГО СОПРОВОЖДЕНИЯ ДЛЯ СИСТЕМЫ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ 241

Шалагинова О.Б.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
ПРОБЛЕМА КАДРОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 241

КРУГЛЫЙ СТОЛ
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ – ИНФОРМАЦИОННАЯ КУЛЬТУРА XXI ВЕКА» 243

Вус М.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ОБ ИНФОРМАЦИОННОЙ КУЛЬТУРЕ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 243

МОЛОДЕЖНАЯ НАУЧНАЯ ШКОЛА «БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ»..... 244

Афанасьев Д.Н., Коваленко М.Е.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
АВТОРСКОЕ ПРАВО В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ..... 244

Бидайбеков Ж.О.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
РОЛЬ ОТДЕЛА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СТРУКТУРЕ ОРГАНИЗАЦИИ..... 244

Бугаенко И.И.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
О ПРАВОВОМ ИНСТИТУТЕ ГОСУДАРСТВЕННОЙ ТАЙНЫ 245

Васильева Н.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
БЕЗОПАСНОСТЬ УСЛУГ СВЯЗИ..... 246

Гилёв Г.А., Негодаев К.С.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
К ВОПРОСУ ОБ АУДИТЕ СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ..... 247

Годжиев А.А., Тарасов С.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
АВТОРСКОЕ ПРАВО И ПРОГРАММНЫЕ ПРОДУКТЫ 248

Гончарова Ю.С., Соляной Т.С.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
ОБ ИНФОРМАЦИОННЫХ ВОЙНАХ..... 248

Григорьян К.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
РАЗРАБОТКА МЕТОДА ПОЛУЧЕНИЯ СИГНАТУР ИСПОЛНЯЕМЫХ ФАЙЛОВ 249

Дранник А.Л.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
ИСПОЛЬЗОВАНИЕ ПРОГРАММ-СИМУЛЯТОРОВ ПОВЕДЕНИЯ РОЕВЫХ РОБОТОТЕХНИЧЕСКИХ СИСТЕМ ДЛЯ ИССЛЕДОВАНИЯ ВОПРОСОВ БЕЗОПАСНОСТИ 249

Ендовский А.С.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
МЕТОДЫ РАСЧЕТА РИСКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 250

Каторин Ю.Ф., Коржук В.М.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
АНАЛИЗ ВОЗМОЖНОСТЕЙ TCP ПО ПЕРЕХВАТУ ИНФОРМАЦИИ В СЕТЯХ СОТОВОЙ ЦИФРОВОЙ СВЯЗИ 251

Коваленко М.Е., Слепцова Д.М.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
КЛАВИАТУРНЫЙ ПОЧЕРК КАК СРЕДСТВО ВСПОМОГАТЕЛЬНОЙ АУТЕНТИФИКАЦИИ 251

Коваль Е.Н.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
РАЗРАБОТКА И ПРИМЕНЕНИЕ МУЛЬТИАГЕНТНЫХ СИСТЕМ 252

Козлова Е.В.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
ИСПОЛЬЗОВАНИЕ МЕТОДА МНОГОМЕРНОГО ШКАЛИРОВАНИЯ В ОЦЕНКЕ СТЕПЕНИ ЗАЩИЩЕННОСТИ РОБОТОТЕХНИЧЕСКИХ СИСТЕМ 253

Комаров К.Ю., Судаков А.М.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
О СИСТЕМЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНАХ ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ САНКТ-ПЕТЕРБУРГА 254

Кузьмин И.Г.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
МОДЕЛЬ ОБЕСПЕЧЕНИЯ ДОКАЗУЕМОЙ ЦЕЛОСТНОСТИ И ДОСТУПНОСТИ ДАННЫХ, РАЗМЕЩЕННЫХ В УДАЛЁННОЙ РАСПРЕДЕЛЁННОЙ СИСТЕМЕ 254

Кузьмич П.А., Пантюхин И.С., Швед Д.В.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
ПРИНЯТИЕ УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ В СИСТЕМАХ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА 255

Люберт А.С.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
МЕТОД ОПРЕДЕЛЕНИЯ ДВИЖЕНИЯ ОБЪЕКТОВ В ВИДЕОПОТОКЕ НА ОСНОВЕ АНАЛИЗА ВРЕМЕННЫХ РЯДОВ 255

Масленников О.С., Егоров В.В.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
ПЕРСОНАЛЬНЫЕ ДАННЫЕ И РАСПРОСТРАНЕНИЕ РЕКЛАМЫ ПО СЕТЯМ ЭЛЕКТРОСВЯЗИ 256

Нурдинов Р.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
РАЗРАБОТКА МЕТОДИКИ ПОСТРОЕНИЯ ЭФФЕКТИВНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА КОММЕРЧЕСКИХ ПРЕДПРИЯТИЯХ 257

Панов К.В.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
О ФИЛЬТРАЦИИ КОНТЕНТА В ИНТЕРНЕТ-СООБЩЕСТВАХ 258

Поляков А.М., Никитенков К.С.
Россия, Санкт-Петербург, ООО «Диджитал Секьюрити», Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
РУКОВОДСТВО ПО ОЦЕНКЕ РЕАЛИЗАЦИИ БЕЗОПАСНОСТИ КОРПОРАТИВНЫХ БИЗНЕС-ПРИЛОЖЕНИЙ 258

Пряхин В.Е.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
ЭФФЕКТИВНОСТЬ МЕТОДОВ АНАЛИЗА ДАННЫХ ПРИ НАГРУЗОЧНЫХ АТАКАХ В ОБСЛУЖИВАНИИ 259

Ракыш Ш.Е.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
К ВОПРОСУ ПОВЫШЕНИЯ ПРОФЕССИОНАЛЬНОЙ КВАЛИФИКАЦИИ СОТРУДНИКОВ 259

Синетова М.М., Цымжитов Г.Б.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
ПАРАМЕТРИЧЕСКИЕ НЕОПРЕДЕЛЕННОСТИ ПРИ АНАЛИЗЕ РИСКОВ В ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ 260

Соломатин А.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
МЕТОД ИДЕНТИФИКАЦИИ ФИЗИЧЕСКИХ ЛИЦ В СИСТЕМАХ ВИДЕОНАБЛЮДЕНИЯ НА ОСНОВЕ НАУЧНО-МЕТОДИЧЕСКОГО АППАРАТА ИММУНОКОМПЬЮТИНГА 261

Турченков Д.А., Цветков Л.В.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
РАЗРАБОТКИ КОМПЬЮТЕРНОЙ ЭКСПЕРТНОЙ СИСТЕМЫ 262

Углов Е.Н., Владимирская М.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
РАЗРАБОТКА ПРЕДЛОЖЕНИЯ ПО АДАПТАЦИИ ЗАКОНОДАТЕЛЬСТВА РФ К ВНЕДРЕНИЮ ОБЛАЧНЫХ ТЕХНОЛОГИЙ 262

Филинюк С.Ю., Еремин О.Е.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
О ПОДГОТОВКЕ КАДРОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 262

Цымжитов Г.Б.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
ОПТИМИЗАЦИЯ ТОПОЛОГИИ КОРПОРАТИВНОЙ КОМПЬЮТЕРНОЙ СЕТИ 263

Шабанов Д.П.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
О ГЕОИНФОРМАЦИОННЫХ ДАННЫХ И МНОГОПОЗИЦИОННЫХ СИСТЕМАХ НАБЛЮДЕНИЯ 264

Шаго Ф.Н.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
К ВОПРОСУ АУДИТА ПРОГРАМНО-ТЕХНИЧЕКИХ КОМПЛЕКСОВ ЗАЩИТЫ ИНФОРМАЦИИ 264

Шацких Р.Н.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
К ВОПРОСУ ОБ УНИВЕРСАЛЬНОЙ ВЕРИФИЦИРУЮЩЕЙ СИСТЕМЕ 265

Шоломов И.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
О НЕОБХОДИМОСТИ КОМПЛЕКСНОГО ПОДХОДА К ПРЕДОТВРАЩЕНИЮ НАРУШЕНИЯ АВТОРСКИХ ПРАВ . 266

Ященко М.А., Елисеев Ю.М.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
К ВОПРОСУ ОБ ИЗВЛЕЧЕНИИ ИНФОРМАЦИИ ИЗ БРАУЗЕРОВ 266

ОГЛАВЛЕНИЕ 268