
# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНОВ РОССИИ (ИБРР-2011)

**VII САНКТ-ПЕТЕРБУРГСКАЯ МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ**

**Санкт-Петербург, 26-28 октября 2011 г.**

# ТРУДЫ КОНФЕРЕНЦИИ

***С Е К Ц И Я***

## ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ

Санкт-Петербург
2011

http://spoisu.ru


# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНОВ РОССИИ (ИБРР-2011)

**VII САНКТ-ПЕТЕРБУРГСКАЯ МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ**

**Санкт-Петербург, 26-28 октября 2011 г.**

# ТРУДЫ КОНФЕРЕНЦИИ

***С Е К Ц И Я***

## ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ

Санкт-Петербург
2011

http://spoisu.ru

УДК (002:681):338.98

И 74

**Информационная** безопасность регионов России (ИБРР-2011). VII
**И 74** Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 26-28 октября 2011 г.: Труды конференции: секция «Информационная безопасность в критических инфраструктурах» / СПОИСУ. – СПб., 2011. – 70 с.
ISBN 978-5-905687-16-7

В сборник включены статьи и доклады, подготовленные участниками VII Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР–2011)» в рамках организованной под руководством ФГУП «НПО «Импульс» секции «Информационная безопасность в критических инфраструктурах».

Предназначен для широкого круга специалистов, руководителей предприятий, представителей органов государственной власти, научных работников и аспирантов, специализирующихся в вопросах защиты информации и информационной безопасности в критических инфраструктурах и автоматизированных системах управления критически важными объектами, нарушение режима работы которых может привести к чрезвычайным последствиям.

**УДК (002:681):338.98**

Редакционная коллегия: *Б.Я. Советов, Р.М. Юсупов, В.П. Заболотский, В.В. Касаткин*
Составители: *И.А. Устинов, В.В. Игумнов, В.Е. Петухов, А.М. Александров, А.Н. Путилин*
Компьютерная верстка: *А.С. Михайлова*

Публикуется в авторской редакции

Подписано в печать 12.10.2011. Формат 60x84⅛. Бумага офсетная.
Печать – ризография. Усл. печ. л. 8,2. Тираж 150 экз. Заказ № 3017
Отпечатано в ООО «Политехника-сервис»
191011, Санкт-Петербург, ул. Инженерная, 6

ISBN 978-5-905687-16-7

## УЧРЕДИТЕЛИ КОНФЕРЕНЦИИ «ИБРР-2011»

- 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 Российской академии наук
- Санкт-Петербургский научный Центр Российской академии наук
- Санкт-Петербургский институт информатики и автоматизации Российской академии наук
- Санкт-Петербургская территориальная группа Российского национального комитета по автоматическому управлению
- Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления

## СОУСТРОИТЕЛИ КОНФЕРЕНЦИИ «ИБРР-2011»

- Российский фонд фундаментальных исследований
- Государственный научный центр РФ - Центральный научно-исследовательский и опытно-конструкторский институт робототехники и технической кибернетики
- ФГУП «Научно-исследовательский институт «Масштаб»
- ФГУП «Научно-исследовательский институт «Рубин»
- ФГУП «Научно-производственное объединение «Импульс»
- ФГУП «ЦентрИнформ»
- СПб ГУП «Санкт-Петербургский информационно-аналитический центр»
- ОАО «Центр компьютерных разработок»
- ЗАО «Ассоциация специалистов информационных систем»
- ЗАО «Институт телекоммуникаций»
- ЗАО «Научно-технический центр биоинформатики и телемедицины «Фрактал»
- ЗАО «РАМЭК-ВС»
- ЗАО «Санкт-Петербургский Региональный Центр защиты информации»
- ЗАО «Эврика»
- ЗАО «Метроком»
- ОАО «Северо-Западный Телеком»
- ООО «ИнТехСервис»
- ООО «Компания «Марвел»
- ООО «Лаборатория инфокоммуникационных сетей»
- ООО «Максима»
- ООО «НеоБИТ»
- Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова
- Петербургский государственный университет путей сообщения
- Санкт-Петербургский государственный политехнический университет
- Санкт-Петербургский государственный университет аэрокосмического приборостроения
- Санкт-Петербургский государственный университет водных коммуникаций
- Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
- Санкт-Петербургский государственный университет технологии и дизайна
- Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
- Санкт-Петербургский институт экономики и бизнеса

- Санкт-Петербургский университет МВД России
- Смольный институт Российской академии образования
- Учебно-методическое объединение вузов России по университетскому политехническому образованию при Московском государственном техническом университете им. Н.Э. Баумана
- Партнерство для развития информационного общества на Северо-Западе России
- Северо-западное отделение Российской академии образования
- Санкт-Петербургская инженерная академия
- Санкт-Петербургское отделение Международной академии информатизации
- Санкт-Петербургское отделение Академии информатизации образования

## КООРДИНАЦИОННЫЙ СОВЕТ КОНФЕРЕНЦИИ «ИБРР-2011»

| | |
|---|---|
| Полтавченко Георгий Сергеевич | Губернатор Санкт-Петербурга |
| Тюльпанов Вадим Альбертович | Председатель Законодательного собрания Санкт-Петербурга |
| Сердюков Валерий Павлович | Губернатор Ленинградской области |
| Макаров Евгений Иванович | Помощник полномочного представителя Президента Российской Федерации в Северо-Западном федеральном округе |
| Алферов Жорес Иванович | Вице-президент Российской академии наук, Председатель Президиума Санкт-Петербургского научного Центра Российской академии наук, Лауреат Нобелевской премии |
| Велихов Евгений Павлович | Академик-секретарь Отделения нанотехнологий и информационных технологий Российской академии наук |
| Щеголев Игорь Олегович | Министр связи и массовых коммуникаций Российской Федерации |
| Фурсенко Андрей Александрович | Министр образования и науки Российской Федерации |
| Макаров Евгений Иванович | Помощник полномочного представителя Президента Российской Федерации в Северо-Западном федеральном округе |
| Никандров Николай Дмитриевич | Президент Российской академии образования |

## ПРЕЗИДИУМ КОНФЕРЕНЦИИ «ИБРР-2011»

| | |
|---|---|
| Тихонов Валерий Владимирович | Вице-губернатор Санкт-Петербурга |
| Демидов Александр Алексеевич | Председатель Комитета по информатизации и связи Санкт-Петербурга |
| Васильев Владимир Николаевич | Председатель совета ректоров Санкт-Петербурга, ректор Санкт-Петербургского государственного университета информационных технологий, механики и оптики |
| Гусев Владимир Сергеевич | Вице-президент Международного Банка «Санкт-Петербург» |
| 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 |
| Максимов Андрей Станиславович | Председатель Комитета по науке и высшей школе Санкт-Петербурга |
| Пешехонов Владимир Григорьевич | Генеральный директор ГНЦ «Центральный научно-исследовательский институт «Электроприбор» |
| Селин Владимир Викторович | Директор ФСТЭК России |
| Советов Борис Яковлевич | Сопредседатель Научного совета по информатизации Санкт-Петербурга |
| Федоров Александр Вячеславович | Первый заместитель Министра юстиции Российской Федерации |

| | |
|---|---|
| Цивирко Евгений Геннадьевич | Председатель Комитета по работе с исполнительными органами государственной власти и взаимодействию с органами местного самоуправления Администрации Санкт-Петербурга |
| Шульц Владимир Леопольдович | Заместитель президента Российской академии наук |
| Юсупов Рафаэль Мидхатович | Директор Санкт-Петербургского института информатики и автоматизации Российской академии наук |

## ОРГАНИЗАЦИОННЫЙ КОМИТЕТ КОНФЕРЕНЦИИ «ИБРР-2011»

### Председатель Организационного Комитета

| | |
|---|---|
| Юсупов Рафаэль Мидхатович | Директор Санкт-Петербургского института информатики и автоматизации Российской академии наук |

### Заместитель председателя Организационного Комитета

| | |
|---|---|
| Майоров Владимир Владимирович | Начальник отдела информационной безопасности, противодействия техническим разведкам и развития системы защиты информации Комитета по информатизации и связи Санкт-Петербурга |

### Члены Организационного Комитета

| | |
|---|---|
| Александров Анатолий Михайлович | Заместитель начальника Центра анализа и экспертизы ФГУП «Научно-производственное объединение «Импульс» |
| Андронова Ольга Олеговна | Главный редактор газеты «Компьютер Информ» |
| Бакурадзе Дмитрий Викторович | Ученый секретарь Санкт-петербургского института информатики и автоматизации Российской академии наук |
| Бачевский Сергей Викторович | Ректор Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича |
| Барышников Сергей Олегович | Ректор Санкт-Петербургского государственного университета водных коммуникаций |
| Басков Дмитрий Вячеславович | Генеральный директор ООО «НеоБИТ» |
| 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 Российской академии наук |
| Гирдин Сергей Алексеевич | Президент ООО «Компания «Марвел» |
| Гоголь Александр Александрович | Советник ректората Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича |
| Григорьев Владимир Александрович | Генеральный директор ООО «Лаборатория инфокоммуникационных сетей» |
| Гуца Анатолий Григорьевич | Главный специалист СПб ГУП «Санкт-Петербургский информационно-аналитический центр» |
| Давыдов Евгений Борисович | Главный конструктор ФГУП «Научно-исследовательский институт «Масштаб» |
| Демидов Алексей Вячеславович | Ректор Санкт-Петербургского государственного университета технологии и дизайна |

| | |
|---|---|
| Долгирев Валерий Алексеевич | Помощник директора Санкт-Петербургского института информатики и автоматизации Российской академии наук по защите информации |
| Дрожжин Владимир Васильевич | Начальник департамента разработки специальных программ ОАО «МегаФон» |
| Жданов Сергей Николаевич | Заместитель генерального директора ЗАО «ВТБ-Девелопмент» |
| Жигадло Валентин Эдуардович | Генеральный директор ООО «Максима» |
| Заборовский Владимир Сергеевич | Заведующий кафедрой телематики Санкт-Петербургского государственного политехнического университета |
| Захаров Юрий Никитич | Директор 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 |
| Игумнов Владимир Вячеславович | Главный конструктор ФГУП «Научно-производственное объединение «Импульс» |
| Ипатов Олег Сергеевич | Заведующий кафедрой Балтийского государственного технического университета «ВОЕНМЕХ» им. Д.Ф. Устинова |
| Исаев Борис Анатольевич | Первый заместитель председателя Комитета по информатизации и связи Санкт-Петербурга |
| Искандеров Юрий Марсович | Заместитель директора Института проблем транспорта им. Н.С. Соломенко Российской академии наук |
| Касаткин Виктор Викторович | Декан ФПК Балтийского государственного технического университета «ВОЕНМЕХ» им. Д.Ф. Устинова |
| Кирсанов Игорь Петрович | Генеральный директор ЗАО «ВО «РЕСТЭК» |
| Ковалев Валерий Иванович | Ректор Петербургского государственного университета путей сообщения |
| 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 |
| Марков Вячеслав Сергеевич | Ученый секретарь Объединенного научного совета Санкт-Петербургского Научного центра Российской академии наук |
| 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 Российской академии наук по информационной безопасности |
| Николаев Алексей Юрьевич | Генеральный директор ЗАО «Эврика» |
| Оводенко Анатолий Аркадьевич | Ректор Санкт-Петербургского государственного университета аэрокосмического приборостроения |
| Остапенко Александр Николаевич | Генеральный директор ЗАО «Лаборатория противодействия промышленному шпионажу» |

| | |
|---|---|
| Перепелица Сергей Николаевич | Генеральный директор ООО «ИнТехСервис» |
| Присяжнюк Сергей Прокофьевич | Генеральный директор ЗАО «Институт телекоммуникаций» |
| Рунеев Анатолий Юрьевич | Генеральный директор ФГУП «Научно-исследовательский институт «Рубин» |
| 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 Российской академии наук |
| Устинов Игорь Анатольевич | Генеральный директор ФГУП «Научно-производственное объединение «Импульс» |
| Уткин Виктор Викторович | Директор Центра информационных технологий управления и электронных услуг Санкт-Петербургского государственного университета сервиса и экономики |
| Федорченко Людмила Николаевна | Старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук |
| Цыулев Сергей Валентинович | Начальник сектора информационно-компьютерной безопасности отдела информационной безопасности, противодействия техническим разведкам и развития системы защиты информации Комитета по информатизации и связи Санкт-Петербурга |
| Черешкин Дмитрий Семенович | Заведующий лабораторией Института системного анализа Российской академии наук |
| Эркин Анатолий Григорьевич | Генеральный директор ЗАО «Санкт-Петербургский Региональный Центр защиты информации» |

## ПРОГРАММНЫЙ КОМИТЕТ КОНФЕРЕНЦИИ «ИБРР-2011»

### Председатель Программного Комитета

| | |
|---|---|
| Советов Борис Яковлевич | Сопредседатель Научного совета по информатизации Санкт-Петербурга |

### Заместители председателя Программного Комитета

| | |
|---|---|
| Жигадло Валентин Эдуардович | Генеральный директор ООО «Максима» |
| Молдовян Александр Андреевич | Заместитель директора Санкт-Петербургского института информатики и автоматизации Российской академии наук по информационной безопасности |

### Члены Программного Комитета — руководители секций

### Ученый секретарь Конференции

| | |
|---|---|
| Заболотский Вадим Петрович | Руководитель научно-исследовательской группы Санкт-Петербургского института информатики и автоматизации Российской академии наук |

### 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 |


50 ЛЕТ
ИМПУЛЬС

## *УВАЖАЕМЫЕ КОЛЛЕГИ!*

Исполнилось пятьдесят лет со дня образования Научно-производственного объединения «Импульс». Родившись в стенах Ленинградского политехнического института им. М.И. Калинина, предприятие прошло славный трудовой путь от проблемных лабораторий института через ОКБ ЛПИ им. М.И. Калинина до НПО «Импульс».

У истоков этого пути стоял выдающийся ученый, инженер и организатор - главный конструктор, участник Великой Отечественной войны, лауреат Ленинской и Государственных премий СССР Т.Н. Соколов, в короткие сроки создавший деятельный молодой коллектив, который сумел вывести предприятие на уровень главных стратегических научно-производственных объединений страны.

Потенциал коллектива особенно ярко проявился при решении важнейшей для нашей страны государственной проблемы - создании системы автоматизированного управления новым видом Вооруженных сил страны - Ракетными войсками стратегического назначения.

На предприятии было создано несколько поколений этих систем, обеспечивающих эффективное и надежное автоматизированное управление стратегическими ядерными силами нашей страны в различных, в том числе самых жестких условиях эксплуатации.

В ходе этих работ в НПО «Импульс» разработаны и успешно применяются технологии создания защищенных ключевых систем для критических инфраструктур в таких областях как оборона, транспорт, энергетика и др.

На протяжении нескольких лет в Санкт-Петербурге при поддержке Правительства города, ряда министерств и ведомств проходят представительные научно-технические конференции «Региональная информатика» и «Информационная безопасность регионов России», на которых обсуждаются приоритетные направления и наиболее значимые проекты информатизации, актуальные проблемы обеспечения безопасности и эффективности использования информационных систем и ресурсов, защиты информации в информационных и телекоммуникационных системах и ряд других проблем.

В организации и работе конференций в качестве соустроителя активное участие принимает НПО «Импульс», являясь инициатором и руководителем важнейших секций, на которых при участии ведущих ученых, специалистов, руководителей предприятий и представителей органов государственной власти обсуждаются актуальные проблемы разработки и применения защищенных информационных систем и автоматизированных систем управления в критических инфраструктурах, являющихся жизненно важными для обеспечения национальной и общественной безопасности страны.

В представленный сборник трудов включены доклады, представленные на секции «Информационная безопасность в критических инфраструктурах», организованной по инициативе и при поддержке ФГУП «НПО «Импульс» в рамках VII Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2011)».

Выражаю глубокую признательность и благодарность всем участникам и организаторам конференции «ИБРР-2011» и ее секции «Информационная безопасность в критических инфраструктурах», желаю новых творческих успехов, здоровья и благополучия.

Генеральный директор ФГУП «НПО «Импульс», Кандидат технических наук  И.А. Устинов

# ОРГАНИЗАЦИОННЫЙ КОМИТЕТ СЕКЦИИ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ»

## Сопредседатели

| | |
|---|---|
| Устинов Игорь Анатольевич | Генеральный директор ФГУП «Научно-производственное объединение «Импульс» |
| Игумнов Владимир Вячеславович | Главный конструктор ФГУП «Научно-производственное объединение «Импульс» |
| Петухов Владимир Ефремович | Референт генерального директора ФГУП «Научно-производственное объединение «Импульс», лауреат Государствкнной премии СССР |
| Александров Анатолий Михайлович | Заместитель начальника Центра анализа и экспертизы ФГУП «Научно-производственное объединение «Импульс» |

## Ученый секретарь

| | |
|---|---|
| Путилин Алексей Николаевич | Заместитель главного конструктора ФГУП «Научно-производственное объединение «Импульс» |

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ

**Устинов И.А., Игумнов В.В.**
**Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»**
**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ**

Информационная безопасность (ИБ) - это комплекс организационно-технических мероприятий, обеспечивающих целостность данных и конфиденциальность информации в сочетании с ее доступностью для всех авторизованных пользователей автоматизированной информационной системы. Иными словами, это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений.

Отдельные сферы деятельности систем государственного, военного, финансового управлений, информационные и телекоммуникационные системы, объекты экономики, транспорта, энергетики и т. д. (так называемые критические инфраструктуры) требуют специальных мер обеспечения ИБ и предъявляют особые требования к надежности функционирования информационных систем в соответствии с характером и важностью решаемых задач. Критические инфраструктуры (КИ) это системы объектов, услуг и информационные системы для которых неисправность или уничтожение отдельных элементов будут иметь серьезные негативные последствия для здоровья и безопасности населения, окружающей среды, национальной экономики, обороны и т. д.

ИБ относится к числу важнейших характеристик КИ. Это относится как к ИБ в целом, так и к безопасности информации в частности. При этом ведущая роль в обеспечении ИБ принадлежит ключевой информационно-управляющей системе данной критической инфраструктуры (КСКИ).

Решение этой фундаментальной проблемы и ее контроль проходит на всех этапах жизненного цикла создания информационно-управляющих систем для КИ - от проектирования, изготовления, испытаний, эксплуатации и до утилизации. Меры, принимаемые для ее решения, должны быть сопоставимы с размером возможного ущерба от деструктивных воздействий на КИ.

Технические требования к КСКИ определяются классом решаемых ими задач и задаются соответствующими тактико-техническими заданиями (ТТЗ) Государственных Заказчиков. Отсюда определяются основные требования к алгоритмам функционирования системы, требования к выбору и применению электронной компонентной базы (ЭКБ), схемно-конструкторским решениям, программному обеспечению (ПО), системе защиты процессов и процедур обработки информации и защиты самих объектов системы, к защите каналов связи, подавлению побочных электромагнитных излучений, алгоритмам диагностики и контроля звеньев, технологии отработки и проведения всего комплекса испытаний с максимальным подтверждением заданных требований в условиях стендовой базы предприятия и т. д.

В ФГУП НПО «Импульс» сформирована особая отечественная научно-техническая школа в области создания больших информационных систем. Научные рекомендации этой школы определили технологию создания защищенных КСКИ . Полученные на этой технологии решения позволяют выполнить основные требования к проектируемым системам. Это – практически абсолютная надежность систем, сохранение работоспособности систем при частичных отказах (отказоустойчивость), гарантированная защита информации от различных воздействий, уникальные вероятностно-временные характеристики передачи данных, способность к развитию (открытость), высокие эксплуатационные характеристики систем. Правильность данной технологии подтверждена на практике разработкой и успешным функционированием более 20 созданных автоматизированных систем управления и информационно-управляющих территориально-

распределенных систем, обеспечивающих надежное управление объектами Генерального Заказчика (МО РФ).

КСКИ в зависимости от уровня решаемых задач условно можно разделить на два основных класса – информационно-управляющие системы (ИУС) и командные системы управления (КСУ).

Функциональные требования и условия применения этих двух классов систем существенно отличаются друг от друга, что неизбежно отражается на технической политике по созданию систем и по обеспечению их ИБ. Не последняя роль здесь принадлежит правильному выбору ЭКБ.

ИУС чаще всего построены в основном на применении импортных аппаратных, программных и технологических решений и, обеспечивают функционирование в мирное время и в начальный период ухудшения военно-политической обстановки. КСУ требуют высокого уровня технологической независимости и ИБ, и должны обеспечивать функции управления объектами, в том числе и необслуживаемыми, с высокой вероятностью выполнения поставленных Руководством страны задач во всех условиях функционирования государства. В связи с этим должны предъявляться особые требования к «кирпичикам» построения КСКИ – элементной базе, она должна быть сугубо отечественная и российского производства.

Применение импортной ЭКБ и импортного ПО не гарантирует необходимый уровень информационной защиты из-за возможного наличия в ней различных «закладок» (в ЭРИ), «троянских коней» (в ПО) и т. д. Наличие этих вредоносных вставок, приводит к блокированию выполнения системой основных функций, в случае перевода ее в режим применения, неприемлемый для эвентуального противника, и соответственно делает данную КСКИ беззащитной в конфликтных ситуациях.

Гарантированное противостояние угрозам и обеспечение требуемого уровня ИБ возможно надежно обеспечить применением доверительных отечественных программно-аппаратных платформ (ПАП) при создании систем, ее составных частей и комплексов средств автоматизации (КСА). Проблемам обеспечения кибер-безопасности в информационных системах и создания доверительных отечественных ПАП были посвящены в этом году два заседания НТС ВПК при правительстве РФ, что подчеркивает их важность и актуальность на современном этапе.

Свойство доверительности означает однозначное соответствие работы КСКИ алгоритмам и функциям, заложенным в неё для выполнения основной задачи. Доверительность означает также предсказуемость поведения этой системы в соответствии с тактико-техническими требованиями на всём наборе внешних воздействующих факторов. Свойство доверительности должно обеспечиваться как в самих защищенных ключевых системах, так и в технологиях их создания, исключающих утечку проектной информации, минимизацию инженерных ошибок и исключающих внедрение недекларированных возможностей в конечный продукт.

Понятие доверительности сложилось в ФГУП НПО «Импульс» в процессе создания КСКИ на протяжении 50-летней напряженной инженерной деятельности объединения, юбилей которой мы будем отмечать в этом году 26 декабря. Доверительность не является новым свойством для систем разработки нашего объединения, так как они проектируются на отечественной радиационно-стойкой ЭКБ и на ПО собственной разработки, на базе доверительных операционных систем.

Необходимо отметить, что постоянно растущая сложность и объемы задач управления требует интенсивного развития отечественной ЭКБ, ее максимального быстродействия, максимальных объемов памяти, сверхмалых габаритов и энергопотребления. Однако не достаточно ограничиваться только вопросами создания отечественной ЭКБ, необходимо проводить работы и по совершенствованию технологий проектирования.

Необходимо подчеркнуть, что проведение определенных мероприятий по технической защите информации и реализация организационных мер также позволяют решать задачу повышения уровня ИБ. Так большое влияние на качество создаваемых систем имеет уровень развития стендовой базы настройки и отработки создаваемых КСА, который позволяет полностью решить все вопросы противодействия иностранным техническим разведкам (ИТР) и провести максимальную проверку всех заданных функций на систему в соответствие с ТТЗ Генерального Заказчика.

Наличие в составе научно-производственного объединения крупного опытного завода и стендового комплекса позволяет без задержек проводить изготовление и отработку новейших образцов создаваемой техники и запускать в серийное производство изделия по тщательно отработанной конструкторской документации, а в дальнейшем на этапе эксплуатации осуществлять авторское сопровождение созданных систем.

Важное значение для обеспечения необходимого уровня работы системы имеет качество контроля состояния звеньев систем и процессов функционирования. На всех этапах создания и эксплуатации изделий функционирует эффективная система контроля качества создаваемой продукции.

Сложнейшие изделия, выпускаемые ФГУП НПО «Импульс», невозможно создать в одиночку. Решающую роль здесь играют кооперация предприятий промышленности (соисполнители работ) и умение организовать с ними работу. ФГУП НПО «Импульс» накопило богатый опыт работы с обширной кооперацией по созданию КСКИ.

На всех жизненных этапах разработки, изготовления, эксплуатации создаваемых систем определяющая роль принадлежит квалифицированным кадрам и их технологической поддержке. Источником достижений объединения является его коллектив высококвалифицированных специалистов в области системотехники, схемотехники, телекоммуникаций, конструирования, микроэлектроники, программного обеспечения, защиты информации и других разделов информатики.

Понимая значимость создания защищенных КСКИ, опыт нашего объединения в вопросах создания таких систем «под ключ», в 2010 году на базе ФГУП НПО «Импульс» была создана секция №6 «Информационные технологии в критических инфраструктурах». Секция успешно работает уже второй год.

**Александров А.М.**
**Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»**

## РАЗЛОЖЕНИЕ ИНТЕГРАЛЬНЫХ ТРЕБОВАНИЙ ПО ВЕРОЯТНОСТЯМ ЛОЖНЫХ СИГНАЛОВ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ

Рассматривается некоторая критическая инфраструктура (КИ), содержащая *n* объектов. Состояние объектов контролируется по совокупности параметров. Результаты этого контроля образуют случайный поток, который поступает для обработки в центр КИ. Поступившие в момент времени *t* сигналы, от *i*-го объекта могут нести как истинную информацию о некотором событии, которое произошло на объекте в момент времени *t* (вероятность этого $p_i(t)$), так и ложную информацию (вероятность этого $q_i(t)$) может не поступить никакой новой информации (вероятность этого $r_i(t)$.

Очевидно, $p_i(t) + q_i(t) + r_i(t) = 1$

Центр КИ обрабатывает поступающую информацию по соответствующему правилу.

Например, если для решения некоторой задачи требуется истинная информация от всех объектов, вероятность этого, есть:

$$\prod_{i=1}^{n} p_i(t)$$

Если хотя бы от одного объекта поступит ложная информация, то центр КИ выдаст ложное решение задачи. Интегральная вероятность ложного решения есть:

$$Q(n,t) = \prod_{i=1}^{n} \left[ p_i(t) + q_i(t) \right] - \prod_{i=1}^{n} p_i(t). \qquad (1)$$

Вероятность Q, определяется формулой (1) и является условной вероятностью, так как не учитывает вероятность распределения моментов времени $t_i$.

В дальнейшем будем рассматривать условную вероятность однородных объектов $p_i(t_i)=\dots\ p_n(t_n)=p,\ q_i(t_i)=\dots\ q_n(t_n)=q$. Поэтому из (1) получается:

$$Q(n)=(p+q)^n-p^n \qquad (2)$$

Исследуем некоторые свойства функции $Q(n)$. В частности, при каких условиях:

$$Q(n+k)<Q(n),\ k\geq 1 \qquad (3)$$

Введем обозначение $\delta=q/p$.

Опуская промежуточные выкладки, получим, что неравенство (3) выполняется если:

$$q^k \angle \delta^k \frac{(1+\delta)^n - 1}{(1+\delta)^{n+k} - 1} \quad (4)$$

Для иллюстраций этих результатов построим таблицу значений вероятности *Q(n)* для *q*=0,1 и различных значений *n* и *p*.

Таблица 1

Вероятность интегрального ложного сигнала

| ***n*** / ***p*** | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| 0,3 | 0,1 | 0,050 | 0,037 | – | – | – | – |
| 0,4 | 0,1 | 0,090 | 0,061 | – | – | – | – |
| 0,5 | 0,1 | 0,110 | 0,089 | 0,057 | – | – | – |
| 0,6 | 0,1 | 0,130 | 0,127 | 0,111 | 0,090 | – | – |
| 0,7 | 0,1 | 0,150 | 0,169 | 0,170 | 0,160 | 0,141 | 0,117 |

Из таблицы непосредственно видно, что интегральная вероятность *Q(n)* может принимать наибольшее значение по *n*. Это значение можно ориентировочно найти, если в формуле (2) считать *n* непрерывной величиной, а вероятность *Q* непрерывной функции:

$$Q(x)=(p+q)^x-p^x \quad (5)$$

Применив известные правила поиска максимума, и решив уравнение *Q′(x)*=0, найдем соотношение для получения искомого *x*:

$$\left(\frac{p+q}{q}\right)^x = \frac{\lambda n p}{\lambda n (p+q)} \quad (6)$$

Таблица 2

Значения *x, n*, при которых $Q=max_1\ [q=0,1]$

| ***p*** | 0,4 | 0,5 | 0,6 | 0,7 | 0,8 |
|---|---|---|---|---|---|
| ***x*** | 1,25 | 1,65 | 2,19 | 3,58 | 6,57 |
| ***n*** | 1 | 2 | 2÷3 | 3÷4 | 6 |

*Некоторые выводы:*

1. Значение интегральной вероятности ложного сигнала $Q(n)$ в общем случае не является монотонной функцией и может иметь максимум, зависящий от соотношения индивидуальных вероятностей истинных и ложных сигналов.

2. Грубой оценкой экстремальных значений ёмкости $n$ критической инфраструктуры может служить решение дифференциального уравнения $Q'(x)$.

3. Изложенный способ разложения интегральной вероятности при обработке сигналов по логической схеме «И», может быть использован для других логических схем, например для схемы «ИЛИ» и др.

**Антонов А.А., Ридигер В.К., Федотов А.А., Филиппов А.С.**
**Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»**

## ИСПОЛЬЗОВАНИЕ ВЫСОКОУРОВНЕВЫХ СРЕДСТВ ПРОЕКТИРОВАНИЯ ДЛЯ РАЗРАБОТКИ СНК НА БАЗЕ БМК 5516БЦ1Т1-002 В КРИТИЧЕСКИХ СИСТЕМАХ

*Введение.* В настоящее время в России активно развивается навигационная система ГЛОНАСС. Согласно программе модернизации системы ГЛОНАСС, действующей до 2020 года, на 2013-2014 годы намечен запуск усовершенствованного спутника КА «Глонасс-К2»

для проведения летно-конструкторских испытаний. Одним из усовершенствований будет применение более точного хронометра. Задача разработки хронометра возложена на ОАО «РИРВ». Для повышения скорости и качества разработки ОАО «РИРВ» привлекло к разработке ЗАО «МК ИМКО» и каф. КСПТ ФТК СПбГПУ. Авторы статьи приняли участие в разработке системы на кристалле (СнК) «ТАЙМ-ИМКО» — специализированной ИС на базе радиационно-стойкого БМК 5516БЦ1Т1-002 фирмы ОАО «Ангстрем».

## 1. Описание разрабатываемой СнК

### *1.1. Назначение и состав разрабатываемой системы*

Разрабатываемая СнК является системой для бортового синхронизирующего устройства спутников ГЛОНАСС. Функции разрабатываемой СнК:

– Синтез частоты для квантового стандарта частоты на рубидиевой газовой ячейке – формирование частоты подмешивания;
– Формирование сетки частот и шкалы времени;
– Передача данных внешней телеметрии.

Под частотой подмешивания понимается частота f, избирательно поглощаемая рубидиевой газовой ячейкой 87Rb. Эта частота используется для подстройки кварцевого генератора (5 МГц). Точность выходной частоты при этом не ниже 10-11 [2].

Получаемая с кварцевого генератора частота поступает на вход сетки частот, формирующей набор служебных частот, а также частоту 1 Гц для шкалы времени, которая является источником точного времени.

Разрабатываемая ИС состоит из двух независимых блоков:

– Синтезатор синусоидального сигнала управляемой частоты;
– Блок БСУ.

Разработка синтезатор синусоидального сигнала управляемой частоты (далее генератор синуса) велась непосредственно авторами статьи. Разработку блока БСУ осуществлял специалист ОАО «РИРВ», а авторы статьи проводили его корректировку и тестирование. В связи с этим в данной статье вопросы разработки блока БСУ практически не затрагиваются.

### *1.2. Синтезатор синусоидального сигнала управляемой частоты*

Синтез сигналов управляемой частоты имеет широкое применение в вычислительной технике. Под термином «синтезатор частоты» понимают электронное устройство, способное из опорной частоты получать на выходе требуемую частоту или набор частот, согласно управляющим сигналам [6]. Наиболее простым и популярным методом синтеза сигналов на данный момент является прямой цифровой синтез. Структурная схема синтезатора приведена на рис. 1.

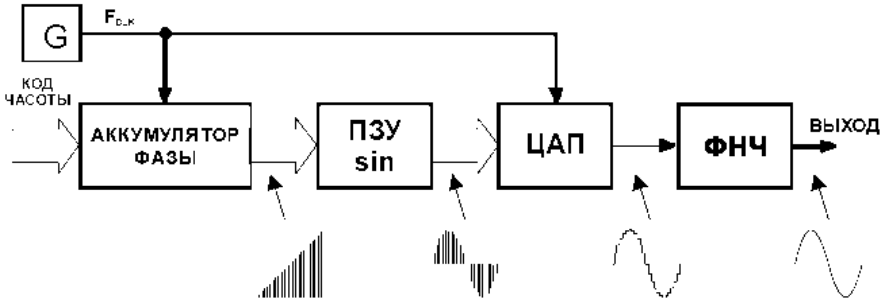



Рис. 1. Структурная схема синтезатора сигнала методом DDS

На рис. 1 приведена типовая структура DDS-синтезатора. Частота формируемого сигнала определяется входом аккумулятора фазы. Аккумулятор фазы — это накапливающий сумматор, формирующий код аргумента *x* функции sin(*x*). Аргумент подается на адресный вход ПЗУ, содержащей значения функции, соответствующие подаваемому адресу. Цифро-аналоговый преобразователь (ЦАП) преобразует цифровое значение синуса в аналоговый сигнал, а фильтр нижних частот (ФНЧ) делает выходной сигнал гладким. Наиболее популярна реализация функции sin(x) на ПЗУ, однако также возможна реализация в виде логической функции (ЛФ). Выходная частота синтезатора вычисляется по формуле 1, где $f_{in}$ – опорная частота, *D* – код частоты, *N* – разрядность аккумулятора фазы.

$$f_{out} = \frac{f_{in} \cdot D}{2^N} \quad (1)$$

К разрабатываемому генератору синуса предъявлены следующие основные требования:

1) Максимальная опорная тактовая частота не ниже 40 МГц;
2) Точность выходной частоты не ниже $10^{-9}$;
3) Для обеспечения заданной точности, разрядность аккумулятора фазы должна составлять 40 разрядов.
4) Генератор синуса должен осуществлять переключение между двумя выходными частотами с одной из заданных частот модуляции, а также формировать частоты модуляции и другие служебные частоты на выходе;
5) Загрузка кода частоты должна осуществляться как последовательным, так и параллельным кодом.

Анализ и выполнение этих и других требований рассмотрены в п.п. 2.2.

### *1.3. Этапы разработки. Элементная база*

В связи с высокой ценой ошибки при проектировании БМК 5516БЦ1Т1 принято решение разделить проектирование на два этапа:

1) проектирование на нестойком аналоге 1592ХМ1Т-021 [3],
2) переход к БМК 5516БЦ1Т1-002 [4].

Оба БМК разработаны компанией ОАО «Ангстрем». В первый этап также входит прототипирование разрабатываемой СнК на ПЛИС, что позволяет исключить функциональные ошибки при проектировании. Прототипирование на ПЛИС, однако, не позволяет осуществить проверку временных характеристик схемы. Это объясняет необходимость применения БМК 1592ХМ1Т, временные характеристики которого совпадают с временными характеристиками БМК 5516БЦ1Т1. Обе БИС БМК 100000 четырех-транзисторных логических ячеек; максимальная частота тактирования – 50 МГц; напряжение питания: 4,5..5,5 В. БМК 5516БЦ1Т1 выполнена по технологии кремний на сапфире (КНС), что обеспечивает ее высокую стойкость к внешним воздействующим факторам (ВВФ) по ГОСТ РВ20.39.414.2-98.

Показатели 1592ХМ1Т по стойкости к ядерным воздействиям существенно ниже, чем у 5516БЦ1Т1, особенно по фактору 7.И8, который является наиболее критичным рамках данной разработки: сбои в схеме формирования точного времени недопустимы. Это стало причиной выбора 5516БЦ1Т1 в качестве целевой элементной базы. 5516БЦ1Т1 является полным функционально-библиотечным аналогом 1592ХМ1Т, это обеспечит возможность быстрого и безошибочного портирования СнК «ТАЙМ-ИМКО» на целевой кристалл, после отработки на относительно дешевом БМК 1592ХМ1Т.

## 2. Разработка СнК «ТАЙМ-ИМКО». Основные этапы

### *2.1. Разработка маршрута проектирования. Согласование с ОАО «Ангстрем»*

Основной идеей при выполнении данной работы было внедрение нового маршрута проектирования, позволяющего ускорить процесс проектирования и снизить риск ошибок, привносимых в процессе проектирования. При этом основным требованием является возможность поддержки разработанного маршрута фирмой-изготовителем БМК, т.е. ОАО «Ангстрем».

Разработка БМК 1592ХМ1Т (также и 5516БЦ1Т1) поддержана средой разработки фирмы Cadence в отличие от других, более старых разработок ОАО «Ангстрем». Это существенно упрощает задачу разработчика, поскольку в этом случае нет необходимости в схемном вводе проекта. Проект можно вводить на языках VHDL/Verilog HDL. Кроме того ангстремовская среда разработки поддерживает наиболее распространенные форматы временных диаграмм, что упрощает процесс моделирования и формирования тестов. В данном маршруте проектирования не применяется устаревший САПР «Невод». В результате разработан маршрут проектирования для генератора синуса (рис. 2).

Основной особенностью разработанных маршрутов проектирования является проведение верификации на всех этапах разработки, позволяющей не допустить привнесения ошибок на каком-либо этапе.


Рис. 2. Разработанный маршрут проектирования генератора синуса

Первым этапом после получения технического задания (ТЗ) на генератор синуса от ОАО «РИРВ» является формирование спецификации. Спецификацию на генератор синуса удобно задавать на языке программирования высокого уровня (ЯВУ), например С, с использованием стандартных библиотек. Такую спецификацию можно довольно легко перевести в синтезируемое HDL-описание с использованием высокоуровневых средств проектирования и верификации класса SystemC. В работе применялся язык CatapultC, в результате чего получено синтезируемое описание, соответствующее спецификации по своей функциональности, однако непригодное для реализации в целевой элементной базе. Полученное описание используется как эталонная модель (ЭМ) при тестировании (см. рис 2). Подробнее об ЭМ на CatapultC в п.2.3.

### *2.2. Разработка VHDL-описания генератора синуса. Прототипирование на ПЛИС*

Разработка велась в САПР Altera Quartus II 9.0. ОАО «Ангстрем» имеет положительный опыт изготовления БМК из проектов, заданных в среде Quartus II. Кроме того прототипирование велось на ПЛИС EP2C8F256 и EP3C5E144, фирмы Altera, для которых Quartus II является основной средой разработки. В результате: описание для БМК без проблем «легло» в ПЛИС. Результаты тестирования прототипа совпали с результатами моделирования и результатами тестирования ЭМ на CatapultC. В дальнейшем прототип генератора синуса на ПЛИС будет использоваться в качестве эталонной модели при тестировании БМК.

Структурная схема генератора синуса (блок Sin_Generator) представлена на рис. 3.

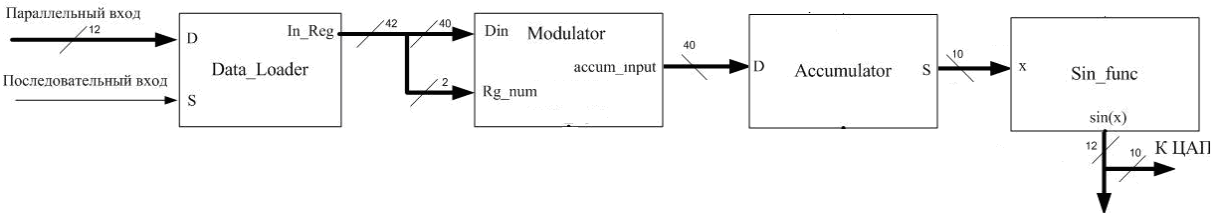



Рис. 3. Структурная схема блока Sin_Generator

Блок Data_Loader осуществляет загрузку кода частоты как в последовательном режиме (42 разряда) так и в параллельном (12 разрядов). Полученный код частоты попадает в блок модуляции (Modulator), где записывается в один из двух регистров, выходы которых коммутируются с частотой модуляции (15, 30 или 78 Гц) на вход 40-разрядного аккумулятора фазы (Accumulator). Аккумулятор фазы – накапливающий сумматор, формирующий аргумент функции Sin(x), который поступает на устройство Sin_func, реализующее функцию Sin(x) с помощью ЛФ. На выходе этого блока формируется 12-разрядный цифровой код синуса, который далее поступает на ЦАП (10 старших разрядов). Большая разрядность аккумулятора фазы, а также возможность модуляции, обеспечивают высокую точность выходной частоты.

Наиболее сложным блоком генератора синуса является аккумулятор фазы — это 40-разрядный накапливающий сумматор, работающий на частоте 40 МГц. Для обеспечения заданной производительности был разработан блок Accumulator со специфической архитектурой. Блок Accumulator представляет собой 10-ступенчатый конвейер, разбивающий суммирование 40-разрядных слов на суммирование 10 групп по 4 разряда. Он

состоит из простейших 4-разрядных сумматоров и цепочек конвейеризирующих регистров. Суммирование 4-разрядных групп осуществляется с последовательным переносом, между группами реализован управляющий перенос. Суммирование каждой 4-разрядной группы дублируется, сумма вычисляется как для единичного переноса в младший разряд группы, так и для нулевого. Сигнал переноса, полученный при суммировании в предыдущей группе разрядов, является управляющим для мультиплексора, коммутирующего обе суммы на выход. Такой подход позволяет значительно ускорить процесс суммирования. Время срабатывания одноразрядного сумматор из библиотеки AGA12C 1592XMx составляет ~2 нс [5]. Это означает, что время срабатывания четырехразрядного сумматора составит не менее 8 нс, но и скорее всего не более 10 нс. При работе на частоте 40 МГц (T = 25 нс) такого времени срабатывания достаточно для корректной работы устройства. В связи с применением 10-ступенчатого конвейера, для обеспечения заданной тактовой частоты 40 МГц, задержка появления первого слова на выходе блока Accumulator составляет 10 тактов.

Функция синуса реализована в виде ЛФ в связи с тем, что встроенное в кристалл ПЗУ ресурсоемко и не отвечает требованиям быстродействия, а применение внешнего ПЗУ недопустимо.

### *2.3. Применение языка CatapultC для верификации генератора синуса*

Спецификация проектируемой системы является первичным и главным источником информации для разработчика конечных модулей системы. Современный подход предполагает задание подобных спецификаций, в том числе и на ЯВУ класса C и C++, что позволяет реализовывать систему программно, а с привлечением современных компиляторов и аппаратно [1]. Одним из путей оптимизации процесса перехода от высокоуровневой спецификации на ЯВУ к аппаратной реализации на заданной элементной базе является использование C-подобных языков для проектирования аппаратных средств. Такие языки являются подмножествами SystemC — языка проектирования и верификации моделей системного уровня. Используемый в данной работе язык CatapultC [7,8,9] фирмы Mentor Graphics является одним из самых популярных SystemC-подобных языков, так как поддержан необходимыми инструментальными средствами (среда разработки CatapultC Synthesis).

CatapultC имеет одно существенное преимущество по сравнению с другими SystemC-подобными языками проектирования цифровых устройств: код на CatapultC, описывающий проектируемое устройство не отличается значительным образом от стандартного C-кода, используемого в чисто программных реализациях алгоритма, с помощью которого ведется проектирование устройства [7,8,9].

Тем не менее, есть один существенный фактор, затормаживающий бурное развитие SystemC-подобных языков: достаточно сложные устройства, заданные на CatapultC, скорее всего, будут уступать по быстродействию и аппаратным затратам аналогичным устройствам заданным на VHDL или Verilog HDL. Синтезируемое из кода на CatapultC RTL-описание очень сложно для человеческого восприятия, поскольку оно синтезировано в автоматическом режиме. В связи с этим ручная корректировка получаемого RTL-описания с целью оптимизации крайне затруднена и практически невозможна. Компания Mentor Graphics – разработчик языка CatapultC и среды CatapultC Synthesis не предполагает ручную доводку описания на уровне RTL.

Указанный выше фактор ограничивает использование SystemC-подобных языков при синтезе цифровых устройств, в которых необходима высокая производительность или низкие аппаратные затраты. По той же причине ограничено использование SystemC-подобных языков при проектировании высоконадежных цифровых устройств. Особенно актуальна эта проблема для отечественной электронной промышленности. Невысокая логическая емкость отечественных ИС по сравнению западными аналогами делает необходимой значительную минимизацию аппаратных затрат, что не позволяет на данный момент применять языки класса SystemC в маршруте проектирования. Другой причиной, не позволяющей применять языки класса SystemC в маршруте проектирования отечественных цифровых устройств, являются высокие требования к их надежности. Кроме того, изменение маршрута проектирования на уровне промышленности всей страны — процесс сложный и длительный, требующий большой технической и административной работы.

Несмотря на ограниченность применения языков класса SystemC непосредственно для синтеза цифровых устройств, есть возможность их альтернативного применения в маршруте проектирования любых цифровых устройств. Так как описание на таких языках полностью соответствует функционально-логической спецификации на устройство, их можно использовать для формирования ЭМ [1], используемой при тестировании разрабатываемого устройства. В данной работе реализована ЭМ генератора синуса на языке CatapultC. Она была успешно синтезирована и использована для тестирования прототипа на ПЛИС. После того, как прототип на ПЛИС прошел тест, он был взят за эталон и использовался для тестирования БМК.

### *2.4. Доработка проекта под требования ОАО «Ангстрем». Изготовление БМК 1592ХМ1Т-021*

После того, как проект был передан в ОАО «Ангстрем» и там был проведен его анализ, потребовались некоторые доработки проекта:

1. Комбинаторная цепочка, синтезированная разработчиками ОАО «Ангстрем» по выданному им исходному описанию на VHDL, реализующая функцию sin(x), оказалась слишком длинной и не давала гарантированного срабатывания на частоте 40 МГц. В связи с этим пришлось конвейеризировать функцию синуса.
2. Потребовалась доработка тестов в соответствии с требованиями системы тестирования ОАО «Ангстрем»:
   1) формирование единого теста для обеих частей проекта,
   2) увязывание тактовых частот тестирования,
   3) расширение тестов для обеспечения заданного тестового покрытия БМК.
3. Согласование разводки выводов в корпусе 4236.208

После проведения доработок были изготовлены опытные образцы БМК 1592ХМ1Т-021.Сформированные тесты обеспечили тестовое покрытие 96%.

## 3. Исследование разработанной СнК

### *3.1. Формирование окружения для тестирования и отладки. Тестирование в системном окружении*

Генератор синуса и БСУ — логически независимые блоки, поэтому тестируются отдельно. Формированием системного окружения для тестирования блока БСУ занимается ОАО «РИРВ». Для генератора синуса на базе ПЛИС EP1S10F780 разработан тестовый стенд, формирующий управляющие сигналы и код частоты. Кроме того в ПЛИС расположен прототип разработанный и верифицированный ранее. Результаты работы БМК и прототипа можно наблюдать в реальном времени в программном логическом анализаторе SignalTap II на рис. 4.

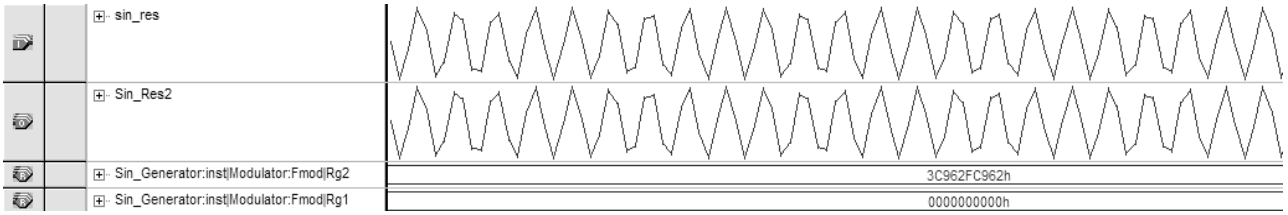



Рис.4. Временная диаграмма работы генератора синуса в SignaTap II

На рис. 4 верхний сигнал соответствует цифровому выходу синуса БМК, а нижний — цифровому выходу прототипа на ПЛИС. Как видно из рисунка, они полностью совпадают. Форма сигнала не гладкая потому, что схема работает на предельных выходных частотах: синус строится по 3-4 отсчетам. Это наиболее тяжелый для схемы режим, который нуждался в проверке в первую очередь. Частота близка к требуемой. Более точно определить ее соответствие можно будет с использованием высокоточного частотомера и спектроанализатора.

Применение такого метода тестирования и отладки позволило быстро убедиться в работоспособности БМК, а также выявить ошибки в печатной плате, на которую был установлен тестируемый БМК.

Кроме того была разработана и изготовлена специализированная плата «Монитор», также реализованная на базе ПЛИС (EP3C5E144). Она может выступать в роли монитора

сигналов, проходящих между БМК и его окружением, а также в роли самого БМК для проверки корректности работы системного окружения.

*3.2. Анализ результатов тестирования. Доработка проекта. Переход к БМК 5516БЦ1Т1-002*

Результаты тестирования БМК 1592ХМ1Т подтвердили полное соответствие спецификации, однако они обнаружили ошибки, допущенные при формировании ТЗ, а также при переходе от ТЗ к спецификации, т.е. ошибки, допущенные на тех этапах проектирования, которые невозможно автоматизировать. Это еще раз подтверждает необходимость автоматизации всех, этапов проектирования, которые возможно автоматизировать с целью минимизации воздействия человеческого фактора, а также демонстрирует работоспособность предложенного маршрута проектирования.

По результатам тестирования было сформировано ТЗ на доработку. Доработки не затрагивают ядра генератора синуса, а касаются лишь вопросов загрузки кода частоты и выдачи служебных частот. На данный момент доработки выполнены, доработанный проект передан в ОАО «Ангстрем» для реализации на БМК 5516БЦ1Т1-002.

*Заключение.* В данной работе успешно применен новый для отечественных БМК маршрут проектирования, отличающийся высокой скоростью реализации и защищенностью от ошибок. Его основная особенность – осуществление верификации на всех этапах проектирования, а также максимальная автоматизация всех этапов проектирования с целью исключения человеческого фактора. Он полностью адоптирован для современного отечественного производства. При успешной реализации БМК 5516БЦ1Т1-002 разработанный маршрут проектирования может быть рекомендован как базовый при проектировании относительно сложных СнК на отечественной элементной базе. Так как БМК 5516БЦ1Т1 является новой разработкой и находится в стадии ОКР, работоспособный и эффективный маршрут проектирования под эту микросхему будет нести в себе научную новизну и практическую ценность.

СПИСОК ЛИТЕРАТУРЫ

1. Антонов А. А. Методика построения встраиваемых средств тестирования высоконадежных цифровых устройств с использованием высокоуровневых спецификаций // Экстремальная робототехника. Труды XXI Международной научно-технической конференции. СПб., 2010. С. 448–458.

2. Григорьянц В. В., Жаботинский М. Е., Золин В. Ф., Квантовые стандарты частоты, М.,1968.

3. Микросхемы интегральные на основе БМК 1592ХМ1Т. Технические условия. АЕЯР.431250.263ТУ, 2003.

4. Микросхемы интегральные на основе БМК 5516БЦ1Т, 5516БЦ1Т1. Технические условия. АЕЯР.431260.385ТУ, 2009.

5. Семейство матричных кристаллов 1592ХМх. Библиотека стандартных элементов AGA12C, ОАО «Ангстрем», 2004.

6. Ридико Л. DDS: Прямой цифровой синтез частоты // Компоненты и технологии. №7. 2001. С. 50-54.

7. Catapult C Synthesis. Automated Verification Extension. User's and Reference Manual: Release 2004b. Mentor Graphics Corporation. 2004. http://www.megratec.ru/data/files_db/7338/Catapult_Verification.pdf.

8. Designing High-Performance DSP Hardware Using Catapult C Synthesis and the Altera Accelerated Libraries. Altera Corporation; Mentor Graphics Corporation. 2007. http://www.altera.com/literature/wp/wp-01039.pdf.

9. Takach A. An Overview and Demonstration of Catapult C. [Видеоматериал]. http://www.mentor.com/player/2007/catapultc/. Проверено 14.06.2010.

**Великовская С.А.**
**Россия, Москва, Московский государственный университет технологий и управления им. К.Г. Разумовского,**
**Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»**

**ГОРОДСКОЙ ИНТЕРНЕТ ДНЕВНИК**

Современный мир постоянно меняется, меняется и отношение к школьному образованию. Сегодня говорят о реальной необходимости перехода школы к Электронному журналу, Электронному дневнику школьника.

Электронный журнал это периодическое рецензируемое издание, электронный аналог печатного журнала, доступный для просмотра на компьютере. Распространяется через Интернет или на любых носителях информации (магнитных, оптических).

Электронный дневник это система, позволяющая перевести большую часть оперативной информации, используемой в образовательном процессе, в электронный вид с последующей доставкой до участников системы (родители, обучающиеся, педагогические

работники) посредством сети Интернет и на различные устройства (стационарный компьютер, мобильный телефон, интернет-планшет и т.п.).

Использование электронного журнала и электронного дневника это не дань моде. Однако это требует нового образа мышления, ломки привычных, выработанных десятилетиями навыков работы. Связано это с тем, что Электронный журнал и Электронный дневник – это не просто копия бумажного журнала и дневника, это уже информационная среда, в которую включены учителя, администрация, обучающиеся, родители учеников. Введение Электронного журнала и Электронного дневника открывает переход классической школы в Электронную школу.

Вовлечение ребенка, педагогов и родителей в образовательный процесс через новые информационные технологии направлено на повышение качества образования, обеспечение соответствия его содержания актуальным потребностям развития российского общества.

В муниципальной системе образования городов России Электронный Журнал и Электронный Дневник чаще всего реализованы в форме программного комплекса АСИОУ+ГИД (автоматизированная система информационного обеспечения управления + городской интернет-дневник).

Возможности программного комплекса АСИОУ+ГИД:

– для родителей: просмотр расписания, тем уроков, домашних заданий, объявлений, новостей любой другой информации, выложенной для всеобщего ознакомления; просмотр отметок своих детей с указанием типа произведенного контроля знаний и комментариями учителя; общение с учителем, администрацией, другими родителями, обучающимися;

– для обучающихся: просмотр расписания, тем уроков, домашних заданий, объявлений, новостей и любой другой информации, выложенной для всеобщего ознакомления; просмотр своих отметок с указанием типа произведенного контроля знаний и комментариями учителя; размещение в «Личном кабинете» своих материалов; общение с учителем, директором, другими обучающимися;

– для учителей: ввод отметок с указанием типа произведенного контроля знаний и по желанию, снабжение их комментариями; размещение домашних заданий и тем уроков просмотр расписания, тем уроков, домашних заданий, объявлений, новостей и любой другой информации, выложенной для всеобщего ознакомления размещение в «Личном кабинете» своих материалов; общение с учениками, их родителями, администрацией школы, другими учителями; тестирование обучающихся по различным тестам с автоматической обработкой закрытых вопросов;

– для администрации: просмотр всей информации по школе, за исключением личной переписки статистика активности пользователей интернет-дневника по школе; просмотр динамики успеваемости обучающихся по классам/ по школе; получение результатов обработки успеваемости в табличных и графических формах; возможность массовой рассылки сообщений по всем участникам зарегистрированных по школе в Интернет-дневнике; общение с учениками, их родителями, учителями; проведение опросов обучающихся, родителей, педагогов по различным основаниям с автоматической обработкой закрытых вопросов.

Данный комплекс позволяет не только формировать банк данных обучающихся и учителей, их достижений и всевозможных показателей степени обученности и качества знаний, но и проводить аналитическую обработку информации. Программный комплекс позволяет осуществлять выборку данных, как по конкретному ребенку, так и по их различным объединениям (классам, группам) и тем самым оперативно получать полную и достоверную информацию о состоянии и динамике образовательного процесса.

Система позволяет автоматически рассчитывать и использовать обобщенные показатели успеваемости, степени обученности, качество знаний, получать статистику отметок (по классам, параллелям, ученикам, предметам, преподавателям, отчетным периодам) для формирования таблиц и диаграмм.

Такой интегрированный банк данных позволяет решать задачи оценки качества образования, осуществлять мониторинг образовательной деятельности, проводить объективный анализ состояния образовательного процесса в школе, получать достоверную информацию о полученном уровне образования и, что самое главное, о результатах учебной деятельности каждого участника образовательного процесса.

Проблема не в том, в каком виде эта информация представлена: в бумажном или электронном, а в том, каким образом она рассчитывается и сколько времени тратит администратор на расчеты. При использовании АСИОУ все вычислительные операции автоматизированы и возможность ошибок практически исключена.

Для того чтобы внедрить Региональный интернет – дневник существует алгоритм:

Электронный журнал – это новая система учета успеваемости для школ и других образовательных учреждений. Это прекрасный инструмент для администрации и учителей, который облегчает их каждодневную бумажную рутину, а также удобный помощник для родителей, чтобы контролировать успехи своего ребенка в учебе и быть на связи со школой.

Главная задача, решаемая Электронным классным журналом, – это своевременное информирование родителей по вопросам успеваемости и посещаемости их детей.

Таким образом, использование Электронного журнала классным руководителем ориентировано на решение одной из проблем школы – информативность.

В планах развития программного комплекса АСИОУ+ГИД — создание общего информационного поля образовательных учреждений с участием органов управления образования, методических центров и других уполномоченных организаций. Специалисты самых разных уровней смогут получать сводную отчетность, анализировать статистику и более эффективно управлять качеством образования.

Конечно, существуют проблемы введения Электронного журнала в школе. Учителю-предметнику приходится выполнять двойную работу, заполняя бумажный и электронный журналы. Некоторые учителя пока ещё настороженно относятся к нововведению, многие боятся дополнительных трудностей. Но те из учителей, кто овладел компьютерными навыками, уже понимают, что есть масса возможностей сэкономить время на бумажной работе, ведь многие отчеты здесь генерируются автоматически.

В настоящее время техническое оснащение кабинетов недостаточно для масштабной планомерной работы. Но в школах создаются компьютерные классы, где подключен Интернет, постепенно возможности расширяются. Не будет ли поздно начинать осваивать Электронные журналы, когда система заработает в полную силу?

Не вызывает сомнения, что вскоре Электронный журнал придет в каждую школу. И это неудивительно. Помимо курса на модернизацию образования (в том числе и в отношении использования информационных технологий в школе), озвученного президентом, есть ряд неоспоримых преимуществ Электронного журнала перед своим бумажным прототипом.

Доступ к данным системы регулируется согласно полномочиям пользователей. Информация предоставляется администрации, учителям, родителям и ученикам в строгом соответствии с их правами.

Информация, поступающая в Электронный журнал, передается в Электронный дневник на сайт Регионального Интернет Дневника (РИД). Доступ к данным системы регулируется согласно полномочиям пользователей. Информация предоставляется администрации, учителям, родителям и ученикам в строгом соответствии с их правами.

Всегда актуальная информация об изменениях расписания, заменах, любых значимых событиях в школе доступна всем пользователям. Вместе со скоростью, с которой информация становится доступна, здесь заключено еще одно заметное преимущество для администрации школы: при работе со многими журналами больше не требуется выстраивать порядок работы с разными классами, так как всегда наглядно видно, в какой части журналы уже заполнены, а кроме этого, можно контролировать работу учителей.

Таким образом, Электронный журнал обеспечивает открытость информационного пространства, стимулирование новых отношений меду всеми участниками учебно-воспитательного процесса.

Электронный дневник школьника формируется автоматически на сайте «Региональный Интернет Дневник»: выгрузка данных из АСИОУ в РИД происходит под административным паролем и не требует дополнительного заполнения Электронного дневника ни классными руководителями, ни учителями – предметниками.

Электронный дневник представляет собой систему для взаимодействия школьников, их родителей, учителей и администрации школы посредством Интернета. С помощью Электронных дневников родители отслеживают успеваемость ребенка: расписание занятий, домашнее задание, оценки, посещение уроков. Школьники всегда имеют под рукой

расписание и домашнее задание, а также возможность посмотреть статистику и рейтинги своих оценок по неделям, месяцам или четвертям.

Электронный дневник дисциплинирует обучающихся: уменьшаются пропуски по неуважительным причинам, ученики, которые отсутствовали по болезни, могут без проблем узнать домашнее задание. Учителя получили удобный и быстрый способ общения с родителями.

Чем же может привлечь Электронный дневник родителей:

1. Электронный дневник – это открытая электронная версия школьного журнала с явными преимуществами: в отличие от его бумажного аналога доступен в любой момент времени и предоставляет больше информации в наглядной и понятной форме: выписки всех оценок, точные данные о посещаемости уроков, возможность цветового кодирования информации.
2. Дневник ребенка является для них доступным через сеть Интернет в любое удобное для них время: дома или на работе, с компьютера, ноутбука, сотового телефона.
3. Электронный дневник помогает родителям проверять ребенка – отговорки вроде того, что дневники сданы на проверку, теперь не пройдут.
4. Из вкладки «Сообщения» родители имеют возможность прочитать запись в Электронном дневнике обучающегося, которую может оставить классный руководитель.
5. Расписавшись за одну неделю в дневнике, родители, как правило, не возвращаются к предыдущей, а в случае с Электронным дневником все оценки с начала четверти никуда не пропадают, а только ведется последующее наполнение, все пропуски отмечены, объявления сделаны. Таким образом, и родители, и ученики могут следить за накопляемостью оценок.
6. Информация в Электронном дневнике защищена от взлома. Родителям и обучающимся, желающим воспользоваться данным сервисом, классными руководителями выдается уникальные логин и пароль, который не подлежит разглашению. Благодаря паролю родители имеют доступ только к собственным данным, оценки других детей для них недоступны.

Таким образом, внедрение Электронных дневников позволяет школьникам стать более ответственными и открытыми перед родителями. Родители могут наладить эффективное взаимодействие с образовательным учреждением. В конечном итоге благодаря Электронному дневнику повышается успеваемость и посещаемость школьников, что, несомненно, повышает престиж школы.

Этот комплекс использует персональные данные, поэтому требуется защита персональных данных. Выделение категории персональные данные из более общей категории частная жизнь связано, прежде всего, с распространением автоматизированных систем обработки и хранения информации, в первую очередь компьютерных баз данных, к которым возможен несанкционированный доступ.

Именно эти системы, по сути, сделавшие революцию в вопросах структурирования, хранения и поиска необходимых данных, создали предпосылки для возникновения проблемы защиты сведений персонального характера – персональных данных с целью защиты прав и свобод граждан.

Технические меры защиты информации предполагают использование программно-аппаратных средств защиты информации.

При обработке ПДн с использованием средств автоматизации применение технических мер защиты является обязательным условием, а их количество и степень защиты определяется в процессе предпроектного обследования информационных ресурсов предприятия.

Технические средства защиты информации делятся на два основных класса:

– средства защиты информации от несанкционированного доступа (НСД): системы разграничения доступа к информации; антивирусная защита; межсетевые экраны; средства блокировки устройств ввода-вывода информации, криптографические средства и т.п.

– средства защиты информации от утечки по техническим каналам: использование экранированных кабелей; установка высокочастотных фильтров на линии связи; установка активных систем зашумления и т.д.

Организационные меры по защите персональных данных включают в себя разработку организационно–распорядительных документов, которые регламентируют весь процесс получения, обработки, хранения, передачи и защиты персональных данных.

Перечень мероприятий по защите персональных данных:

– определение круга лиц, допущенных к обработке персональных данных;
– организация доступа в помещения, где осуществляется обработка ПДн;
– разработка должностных инструкций по работе с персональными данными;
– установление персональной ответственности за нарушения правилобработки ПДн;
– определение продолжительности хранения ПДн и т.д.

Реализация организационных мер защиты информации осуществляется с учетом категорий персональных данных – чем выше категория, тем выше требования их защиты.

**Виноградов А.А.**
**Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»**

## ДОВЕРИТЕЛЬНАЯ ПРОГРАММНО-АППАРАТНАЯ ПЛАТФОРМА АСУ КРИТИЧЕСКИХ ИНФРАСТРУКТУР

Сетецентрическая концепция ведения военных действий и стратегического противостояния, активно внедряемая государствами НАТО, выдвигает ряд новых угроз, требующих адекватного парирования в информационных системах критических инфраструктур.

Целью первого парализующего и сокрушительного удара становятся не военные объекты и непосредственно оружие, а информационные ресурсы стратегических систем государственного и военного управления.

В современных условиях на первый план выходит доверительность работы АСУ. Свойство доверительности означает:

– Кибер-устойчивость (парирование информационных атак и других угроз, порождаемых сетецентрическим противостоянием);

– Функциональная полнота заложенных алгоритмов для решения задач применения системы по основному назначению;

– Полное соответствие работы системы заложенным в неё алгоритмам и функциям;

– Предсказуемость поведения системы в соответствии с ТЗ на полном наборе внешних и внутренних дестабилизирующих факторов (эффективное парирование угроз).

Функциональные задачи, условия и порядок применения стратегических систем государственного и военного управления существенно отличаются друг от друга, что неизбежно отражается на технической политике по созданию систем и по обеспечению парирования угроз.

Подавляющее большинство глобальных информационно-управляющих систем критических инфраструктур России построено на импортных программно-аппаратных решениях. Современные импортные информационные технологии (ИТ) – это инструмент, который является обоюдоострым. Импортные ИТ содержат встроенную избыточность, необходимую для выполнения работы системы по основному назначению, однако эта избыточность позволяет получать дополнительную информацию и вести стороннюю деятельность, в том числе и враждебного характера. Типичный пример - мобильные телефонные сети. Платные услуги мобильной связи демонстрируют возможность эксплуатации технологической избыточности ИТ:

– Позиционирование абонента, не нужное для передачи речи, - проводится и продаётся как информация о месте нахождения ребёнка;

– Тотальное архивирование цифровой информации, не нужное для передачи речи, проводится и часто используется в коммерческих интересах, следственных действиях, и т.д.

Вводится и эксплуатируется также наложенная избыточность – будильник срабатывает и включает выключенный Вами мобильник, то есть в телефоне реализуется не тот режим, который вы задали. Выключения на самом деле не произошло! Хотя для вас демонстрируется вид гашения всех индикаторов и прекращения реакции на кнопки.

Соответственно более сложные информационные системы имеют гораздо больше ресурсов встроенной технологической избыточности для реализации не декларированных возможностей и поддержки информационных атак, которые и лежат в основе реализации

концепции информационной разведки и стратегии влияния при сетецентрическом противостоянии.

Свойство доверительности распространяется не только на сами системы, но и на технологии их проектирования, изготовления, испытаний.

В системах требуется особо обратить внимание на такие составляющие свойства доверительности, как кибер-устойчивость, информационная безопасность, отказобезопасность, устойчивость систем к не выявленным при проектировании инженерным ошибкам.

Кибер-устойчивость систем на импортных решениях обычно обеспечивается методами упреждающего выявления действий вредоносных программ до наступления катастрофических последствий с дальнейшим их блокированием. Учитывая, что защита против новых вирусов реализуется только после их выявления, не следует предполагать, что в реальном конфликте противник будет применять старые методы атак и системы будут «знать» о необходимых методах противодействия. На этапе мирного времени и в условиях начального периода ведения военных действий, когда еще не наступили последствия от применения противником кибер-ударов по информационным ресурсам систем можно рассматривать выстраивание системного противостояния кибер-атакам, однако из-за технологического отставания следует предполагать высокую вероятность последующего вывода из строя систем, совместимых по системе команд с технологиями кибер-вторжения. В условиях дополнительной деградации от применения высокоточного оружия прекращение функционирования систем на импортных решениях неизбежно наступит на начальных этапах военного конфликта.

По мнению ФГУП «НПО «Импульс» надёжная кибер-устойчивость систем, от которых требуется работа в чрезвычайных условиях, может быть достигнута только при их невосприимчивости к методам и технологиям кибер-вторжений, что возможно реализовать только на программно-аппаратной платформе, программно не совместимой с технологиями вторжения и доступной для тотального технологического контроля на не декларированные возможности. Для глобальных систем, построенных на импортных решениях с высокой производительностью и большими информационными ресурсами хорошее решение даёт виртуализация вычислительной среды, позволяющая построить виртуальные ресурсы не на стандартных, а на специализированных программных решениях. Методы воздействия, направленные против уязвимой физической платформы, не воспринимаются на виртуальном уровне как коды вредоносных программ и оказываются не эффективными. Виртуализация вычислительной среды позволяет также сократить количество уязвимых точек физического вхождения и обеспечить тотальный организационно-технический и информационный контроль над их использованием.

Отказобезопасность – это свойство систем не допускать возникновения катастофических последствий от проявления любых неисправностей и искажений информации. Отказобезопасность в системах разработки ФГУП «НПО «Импульс» закладывается и обеспечивается на всех стадиях их создания.

Инженерные ошибки становятся постоянно присутствующим фактором, так как существенно повысилась алгоритмическая насыщенность систем, сложность программного обеспечения и степень интеграции аппаратных платформ. Абсолютно всё ошибки выявить и устранить на этапах отладки и испытаний становится невозможным. Даже в массовых высоко интегрированных программных продуктах и аппаратных платформах мировых разработчиков и производителей постоянно обнаруживаются не выявленные на этапах отладки ошибки в микросхемах и в программном обеспечении. Для борьбы с не выявленными ошибками важнейшим свойством систем становится контролируемость целостности вычислительных процессов и массивов данных по ходу их выполнения со своевременным принятием парирующих мер. Контролируемость должна обеспечиваться на всех уровнях функционирования систем, начиная от ЭРИ и заканчивая системными алгоритмами.

Свойство доверительности должно обеспечиваться как в самих системах, так и в технологиях их создания, исключающих утечку проектной информации, минимизирующих инженерные ошибки и исключающих внедрение не декларированных возможностей в конечный продукт. Общепринятым является мнение о том, что достаточно закупить и установить на предприятии современный САПР, чтобы качественно повысить уровень

проектирования. На самом деле САПР – это только инструмент. Очень важно правильно поставить процесс проектирования и обучить этому процессу специалистов. Каждый САПР требует создания стандарта предприятия по его применению.

Важнейшим аспектом является моделирование в САПР. Это сложный процесс, который требует разработки моделей объекта в целом и его составных частей, начиная с ЭРИ. Лицензионные САПР рассчитаны на дополнительную закупку библиотек информационных моделей, но только для импортных компонентов. Требуется дополнительная разработка отечественных моделей. Применение моделирования не сокращает сроков выпуска КД, а наоборот требует дополнительных интеллектуальных и временных затрат на стадии разработки КД. Эффективность от внедрения процессов проектирования на современных САПР, экономия средств и сокращение сроков работ достигается на стадиях автономной и комплексной отработки реально изготовленной аппаратуры, благодаря существенному сокращению объёма требуемых доработок аппаратуры и программного обеспечения.

Важнейшей стадией отработки доверительности систем является тестирование и верификация программно-аппаратной платформы, функционального программного обеспечения и системы в целом. На эти работы в полном объёме, включая проверку алгоритмов негативного управления по парированию сбоев, отказов и других угроз, требуется время и усилия, которые категорически надо планировать и эффективно использовать в целях проверки и подтверждения доверительности работы создаваемых систем.

Понятие доверительности сложилось в НПО «Импульс» в процессе создания инфомационно-управляющих систем на протяжении 50-летней напряженной инженерной деятельности. Доверительность не является новым свойством для систем разработки нашего предприятия, так как они проектируются на отечественной радиационно-стойкой ЭКБ и на программном обеспечении на базе доверительных операционных систем собственной разработки.

Доверительность системы закладывается, отрабатывается и проверяется на всех уровнях проектирования:

1. Функциональность и встроенный контроль ЭРИ.
2. Схемные решения на уровне электронных модулей.
3. Горячее и холодное резервирование на уровне вычислительных структур.
4. Алгоритмические решения на уровне системных протоколов и функционального программного обеспечения.
5. Конструкционная надёжность.
6. Производственно-технологическая надёжность.
7. Эксплуатационная надёжность.

НПО «Импульс» на протяжении своей деятельности на разных этапах развития отечественной промышленности вынуждено было заниматься созданием необходимой ЭКБ, технологий и самих систем, которые по определению уже в первых поколениях носили доверительный характер.

Подавляющее большинство созданных стратегических глобальных систем в России построены на импортных аппаратно-программных платформах, которые настойчиво предлагаются по дешёвым ценам иностранными государствами и заняли на сегодня практически всё информационное пространство страны.

В условиях, когда неоднократно подтверждалась возможность блокирования военных управляющих систем и систем связи со стороны противника в ходе локальных военных конфликтов, требуется понимать, что такие же методы информационных блокировок и организации утечки информации реализованы в информационных ресурсах импортных систем, развернутых на территории России.

Адекватное парирование новых угроз обеспечивается надёжно только при условии применения доверительных отечественных программно-аппаратных платформ.

На переднем плане остаётся также надёжность, радиационная стойкость, устойчивость к внешним воздействующим факторам систем специального назначения.

Доверительные технологии должны также давать возможность просматривать и совершенствовать алгоритмы негативного управления при деградации компонентов платформы, а также автоматического восстановления конфигурации при устранении

неисправностей. Важнейшим является вопрос живучести систем и реализации встроенного и наложенного аппаратного, программно-аппаратного и программного контроля в платформах.

Только комплексный подход к обеспечению действительной доверительности отечественных программно-аппаратных платформ обеспечивает позволяет создавать высоконадёжные технические средства и системы специального назначения.

Нужно говорить о целостной государственной технологической политике по созданию доверительной отечественной программно-аппаратной платформы с целевым финансированием. Доверительная платформа м.б. сделана только на доверительных технологиях.

Государственная технологическая политика должна охватывать весь комплекс работ, которые необходимо возобновить или поставить заново территории страны, чтобы обеспечить действительную технологическую независимость систем управления критическими инфраструктурами.

Совершенно не достаточно ограничиваться только вопросом создания отечественной ЭКБ, хотя это одна из ключевых задач.

Государственная технологическая политика должна включать в себя следующие направления работ:

– Технологии моделирования возможных возмущений от воздействующих факторов, выработки, оптимизации и верификации на моделях требований к системам и к ЭКБ в зависимости от условий их применения;

– Интегрированные доверительные технологии проектирования систем специального назначения, их программных и аппаратных средств;

– Доверительные технологии проектирования специализированной ЭКБ;

– Независимые технологии изготовления специализированной ЭКБ, материалов и конструкций для компонентов систем специального назначения;

– Технологии автономной и комплексной отладки систем специального назначения;

– Технологии испытаний специализированных систем в привязке к стойкости к воздействующим факторам и к требуемому функционалу основной работы с учётом алгоритмов негативного управления, предельных и разрушающих испытаний.

Технологии моделирования возмущений должны включать в себя виртуальные компьютерные методы, создание современных моделирующих установок реальных воздействующих факторов. В результате должны быть разработаны требования по стойкости к воздействующим факторам для разных видов платформы в зависимости от условий их применения.

Не менее важным является этап системного проектирования, по результатам которого разрабатываются функциональные требования к различным видам платформ в зависимости от предметной области применения.

В результате появляется система требований к ЭРИ, материалам, конструкции, к функционированию платформ для каждого вида применения.

Центральным обычно становится вопрос оптимизации соотношения стойкости платформы к условиям применения и ее вычислительной мощности. Хочется иметь всегда максимальную вычислительную мощность, однако на практике мощность процессора и мощность готовой платформы существенно отличаются между собой. Основная задача технологий проектирования аппаратных и особенно программных средств концентрируется вокруг максимального использования всех возможностей аппаратуры, программного обеспечения, конструкции для достижения максимальной вычислительной мощности создаваемой платформы в целом при обеспечении требований по стойкости к воздействующим факторам.

Технологии проведения испытаний должны включать в себя значительно большую моделирующую составляющую для выявления проблем на ранних стадиях создания систем и для сокращения затрат на натурные испытания.

Отдельного внимания требует также вопрос создания эквивалентных технологий испытаний для условий применения, моделирование или создание которых затруднено (термо-вакуумные испытания).

Таким образом, в современных условиях сетецентрического противостояния реализация доверительности информационных систем критических инфраструктур

становится важнейшим требованием по обеспечению работоспособности при наличии информационных и фозических дестабилизирующих факторов.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ 19176 - 80. Системы управления техническими средствами корабля. Термины и определения.
2. Черкесов Г.Н. О системном анализе безопасности. – Безопасность жизнедеятельности, 2004, № 1.
3. Черкесов Г.Н. Методы и модели оценки живучести сложных систем. – М.: Знание, 1987.
4. Половко А.М., Гуров С.В. Основы теории надежности. Глава 13. Надежность и риск. – СПб: БХВ-Петербург, 2006.
5. ГОСТ 27.310-95. Надежность в технике. Анализ видов, последствий и критичности отказов. Основные положения.
6. ГОСТ ЕН 1070-2003. Межгосударственный стандарт. Безопасность оборудования. Термины и определения. – Минск: Изд-во стандартов, 2003. –23 с.
7. ГОСТ ИСО/ТО 12100-1-2001. Межгосударственный стандарт. Безопасность оборудования. Основные понятия, общие принципы конструирования. Часть 1. Основные термины, методика. – Минск: Изд-во стандартов, 2001. – 17 с.
8. Авиженис А. Отказоустойчивость – свойство, обеспечивающее постоянную работоспособность цифровых систем. Пер. с англ.- Труды ИИЭР, 1978, т. 66, № 10, с. 5-25.
9. Avizienis A. Design of fault-tolerant computers.- AFIPS Conf. Proc., 1967, FJCC, v. 31, p. 733-744.
10. Рябинин И.А. Надежность и безопасность структурно-сложных систем. - СПб: изд-во СПбГУ, 2007.
11. Надежность систем энергетики: Терминология. Сборник рекомендуемых терминов. – Вып.95. – М.: Наука, 1980. – 42 с.
12. Словарь по кибернетике. Под ред.В.М. Глушкова. – Киев: Главная ред. Укр. сов. энциклопедии, 1979.
13. Справочник по безопасности космических полетов//Береговой Г.Т. и др. М.: Машиностроение, 1989, 336 с.
14. Бахметьев А.М., Самойлов О.Б., Усынин Г.В. Методы оценки и обеспечения безопасности ЯЭУ. М.: Энергоатомиздат, 1988, 136 с.
15. Супаков Н.К. Безопасность эксплуатации ракетного оружия. М.: Изд. МО, 1972, 220 с.
16. Майоров А.В., Москатов Г.К., Шибанов Г.П. Безопасность функционирования автоматизированных объектов. М.: Машиностроение, 1988, 262 с.

**Волкова А.В.**
**Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»**

## СИНТЕЗ ОПТИМАЛЬНОГО МАНИПУЛЯЦИОННОГО КОДА ДЛЯ СИГНАЛЬНО-КОДОВОЙ КОНСТРУКЦИИ НА ОСНОВЕ ТРЁХМЕРНОЙ СИМПЛЕКС-РЕШЁТКИ

Настоящая работа посвящена нахождению оптимального манипуляционного кода для сигнально-кодовой конструкции на основе трёхмерной симплекс-решётки для модема КВ-радиосвязи. Предполагается, что оптимальный манипуляционный код поможет повысить помехоустойчивость сигнала. В заключение работы будут представлены сравнительные характеристики, полученные в результате моделирования.

Благодаря преимуществам КВ радиосвязи, среди которых можно выделить возможность организации связи на расстоянии до нескольких тысяч километров при относительно небольшой мощности передатчиков (1 кВт), её применяют для передачи команд звеньям управления. Однако в связи с особенностями КВ канала, рассматриваемый тип радиосвязи подвергается ряду помех, связанных с многолучёвостью и состоянием ионосферы. Таким образом, требуется повысить помехоустойчивость применяемых сигналов. Это, в свою очередь, приводит к снижению частотной эффективности или же уменьшению скорости передачи.

К системам КВ радиосвязи могут применять требования относительно внедрения структуры ISDN. Но существующие виды модуляции КВ модемов позволяют передавать не более 4800 бит/с. Такая скорость не является достаточной для организации сервисов, соответствующих более высоким уровням модели OSI. Таким образом, возникает задача увеличения скорости при сохранении помехоустойчивости и частотной эффективности.

Одним из факторов, определяющих реально достижимое значение скорости передачи, являются применяемые виды модуляции и кодирования сигналов. Как известно, при применении обычных видов модуляции улучшение скорости передачи при заданной допустимой помехоустойчивости приводит к снижению спектральной и энергетической эффективности. Следовательно, поставленная задача увеличения скорости передачи при сохранении помехоустойчивости и полосы является актуальной.

Одним из способов решения поставленной задачи является повышение качества функционирования модемов. На рисунке 1 приведена блок схема модемов на передающей и приёмной стороне. С точки зрения нашей задачи модулятор выполняет две функции:

1. Формирует набор сигналов с определёнными параметрами (т.е. задаёт положение всех возможных сигнальных точек на фазовой плоскости) (фактически, вид модуляции: ОФМ, КАМ и т. д.);
2. Сопоставляет каждой такой точке скаляр (т. е. кортеж бит).

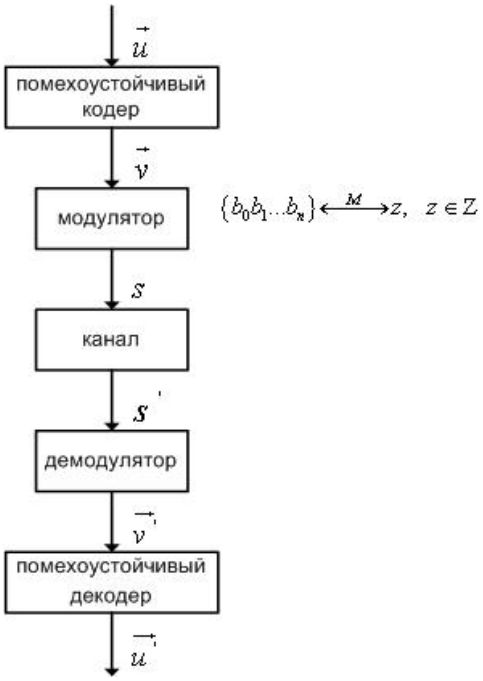



Рис.1. Блок-схема модема

Таким образом, повышение качества работы модулятора можно проводить по двум направлениям: выбор оптимального расположения точек созвездия и способ сопоставления каждой такой точке скаляра.

При применении обычных видов модуляции улучшение скорости передачи при заданной допустимой помехоустойчивости приводит к снижению спектральной и энергетической эффективности. В работе [1] был предложен новый принцип формирования набора сигналов. Такие сигналы получили называние сигнально-кодовой конструкции на основе трёхмерной симплекс-решётки. В работе [2] было показано, что данная сигнальная конструкция обладает лучшей помехозащищённостью при заданной полосе и скорости по сравнению с сигналами обычных видов модуляции. Следующим возможным способом повышения помехоустойчивости сигнала является оптимизация манипуляционного кода с точки зрения минимизации расстояния по Хэммингу между соседними точками созвездия. Настоящая работа посвящена оптимизации манипуляционного кода, приводящей к улучшению помехозащищённости сигнала.

Манипуляционное кодирование – сопоставление картежу бит физического сигнала. В случае если имеет место канал с белым гауссовым шумом, наиболее вероятные ошибочные сигналы – ближайшие к переданному сигналу. Под оптимальным манипуляционным кодом в настоящей работе подразумевается код, дающий наименьшую вероятность ошибки при заданной энергии и полосе.

В случае отсутствия помехоустойчивого кодирования оптимальным манипуляционным кодом считается код Грея. Т. е. такой код, при котором «соседним» сигналам соответствуют кортежи бит, имеющие наименьшее расстояние по Хэммингу. Однако, в случае применения кодов, исправляющих ошибки, такой манипуляционный код не является оптимальным. Задачу можно сформулировать так: в случае, если искажение физического сигнала приводит к неисправляемой ошибке, то неверно декодированное информационное слово должно иметь наименьшее расстояние по Хэммингу от переданного информационного слова:

$$P_{erik} \uparrow \Rightarrow h_{ik} \uparrow .$$

На рисунке 2 проиллюстрирован принцип разработанного манипуляционного кода. Данный метод манипуляции синтезировался для амплитудной модуляции и

помехоустойчивого кода Хэмминга (7, 4). Алгоритм разработки метода манипуляции состоит из трёх этапов:

1. Нахождения кодовых слов для всех возможных информационных слов.
2. Сопоставление им сигнала с амплитудой, равномерно распределённой по множеству возможных значений, так чтобы расстояние по Хэммингу между соседними кортежами не превосходило единицы;
3. Оставшиеся свободные физические сигналы соответствуют кодовым словам, в которых произошли ошибки; так, для каждого из $2^k$ кодовых слов можно поставить в соответствие по $2^{n-k}-1$ искажённые кодовых слов, где произошла однократная ошибка; следовательно, на сигнальной прямой вокруг неискажённых кодовых слов расставляются кодовые слова, где произошли однократные ошибки, соответственно.

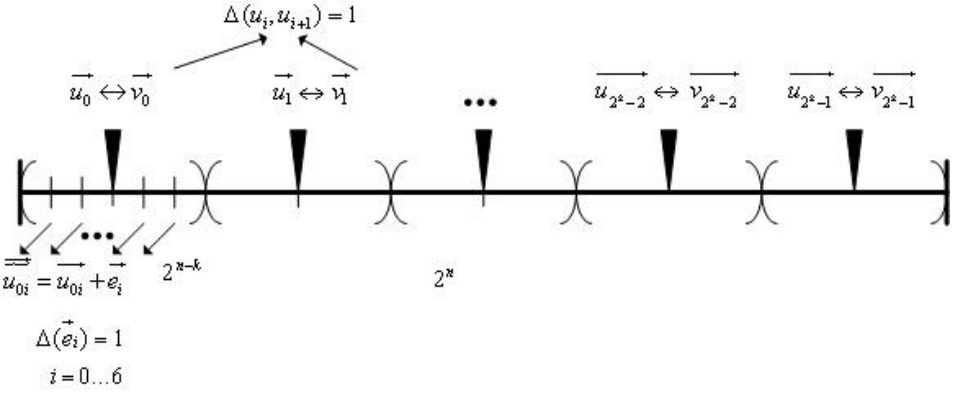



Рис. 2. Принцип формирования оптимального манипуляционного код

При синтезе оптимального манипуляционного кода было принято во внимание, что в условиях канала БГШ с наибольшей вероятностью искажается сигнал с соседними амплитудами. Таким образом, при данном методе манипуляционного кодирования наиболее вероятные искажения приводят к однократным ошибкам. Т. е. искажения находятся в области исправления ошибок. Если же ошибка приводит к области неисправляемых ошибок, то в результате декодирования получаем информационное слово, отличающие на один бит. Эта особенность предложенного манипуляционного кодирования даёт возможность предположить, что помехоустойчивость такого сигнала улучшиться. Т.е при заданном отношении сигнал/шум, то средняя вероятность ошибки (СВО) уменьшится.

Для проверки данного предположения была построена модель в среде MatLab. На рисунке 3 приведена зависимость вероятности ошибки на бит от отношения сигнал/шум для предложенного метода манипуляции сигнала и для манипуляции кодом Грея.

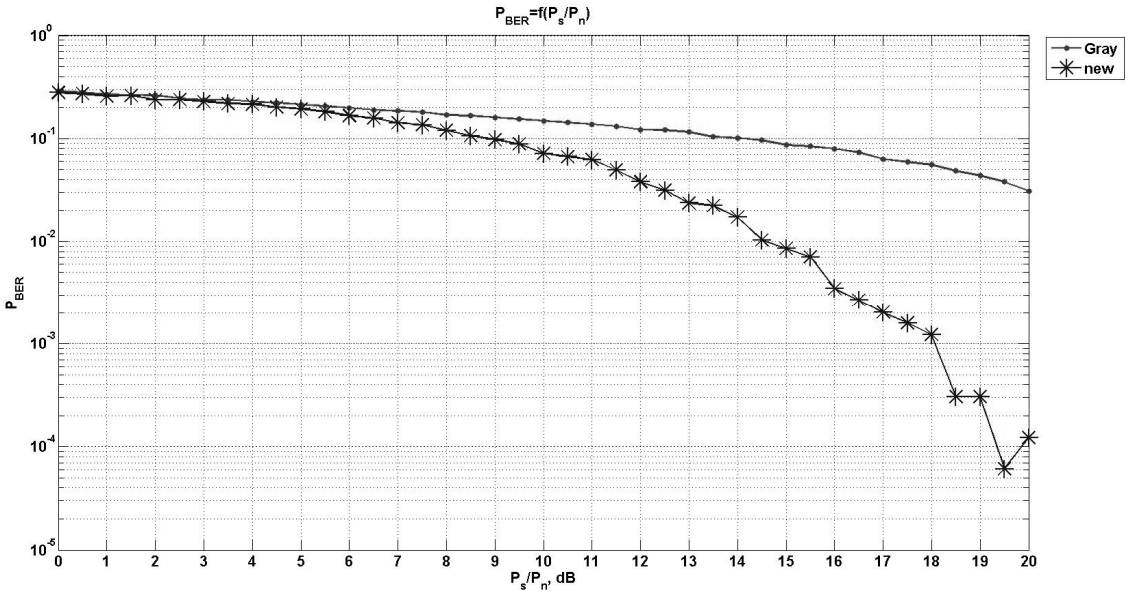



Рис.3. Зависимость вероятности ошибки от отношения сигнал-шум для амплитудной модуляции при использовании манипуляции кодом Грея (‘Gray”) и синтезированного оптимального модуляционного кода (“new”)

## СПИСОК ЛИТЕРАТУРЫ

1 Путилин А.Н., Волкова А.В. Сигнально-кодовая конструкция на основе трёхмерной симплекс-решётки // 12-я Международная конференция «Цифровая обработка сигналов и её применение» («DSPA-2010»). М, 2010.

2 Волкова А.В. Анализ сигнально-кодовых конструкций, применяемых в модемах систем с псевдослучайной перестройкой рабочей частоты и предложения по их улучшению // Интегрированные автоматизированные системы управления: сборник докладов научно-технической конференции. Ульяновск, 2011.

**Гук И.И., Путилин А.Н., Сиротинин И.В., Хвостунов Ю.С.**
**Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»**

## АДАПТИВНАЯ СИСТЕМА ДЕКАМЕТРОВОЙ РАДИОСВЯЗИ С ПОЛНОДИАПАЗОННОЙ ПЕРЕСТРОЙКОЙ РАБОЧЕЙ ЧАСТОТОЙ И ПРЕДВАРИТЕЛЬНЫЕ РЕЗУЛЬТАТЫ ТРАССОВЫХ ИСПЫТАНИЙ ЕЁ ФРАГМЕНТА

Адаптивная система коротковолновой радиосвязи с полнодиапазонной псевдослучайной перестройкой рабочей частоты (АСДР ППРЧ) предназначена для создания симплексных, полудуплексных и дуплексных каналов радиосвязи декаметрового диапазона на дальности до 300 км в движении и до 3000 км между стационарными пунктами связи со скоростями работы абонента от 2400 до 19 200 бит/с.

*1. Принципы АСДР ППРЧ*

Для каждой отдельной сети:

– выделяется пул рабочих частот (N рабочих частот);
– назначается n (n < N) начальных рабочих частот;
– назначается ключ закона перестройки рабочей частоты;
– устанавливается время t работы на одной рабочей частоте.

Для каждого абонента отдельной сети:

– назначается двухбайтный сетевой адрес;
– назначается одна из ортогональных строк частотно-временной матрицы рабочих частот.

При воде абонента в сеть через радиоканал осуществляется начальная синхронизация переключения начальных рабочих частот (сетевая синхронизация). В дальнейшем в течение 1 –1,5 месяцев абонент готов к обмену информацией из состояния радиомолчания без предварительного этапа зондирования канала связи и установления синхронизации. Если с течение этого времени в сети состоялся обмен информацией, то для всех абонентов сети время готовности продлевается на 1 –1,5 месяца.

Адресная передача («точка» - «точка», «точка» - «многоточка») ведется пакетами длительностью 53 мс на каждой из n начальных рабочих частот.

Принимающая радиостанция в процессе обмена информацией без снижения пропускной способности подтверждает передающей успешный прием по каждой используемой рабочей частоте. В случае отсутствия приема на данной рабочей частоте принимающая радиостанция дает команду передающей радиостанции на замену на резервную рабочую частоту из общего набора.

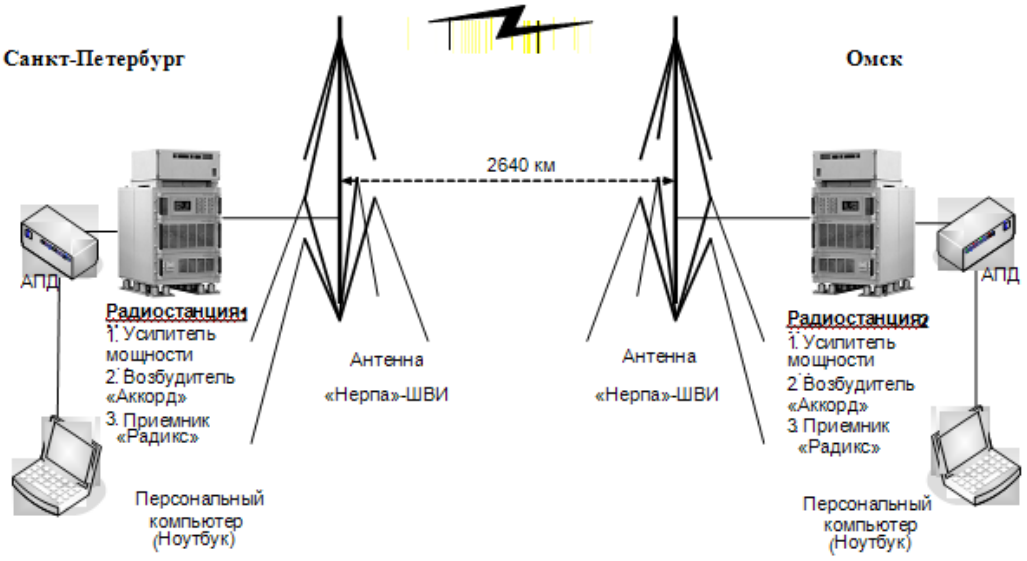



Рис.1. Схема трассовых испытаний

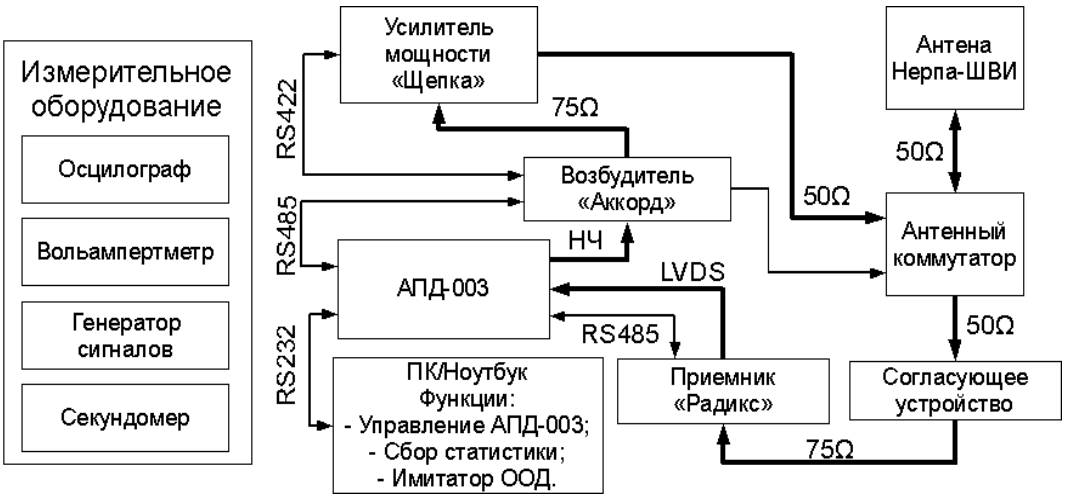
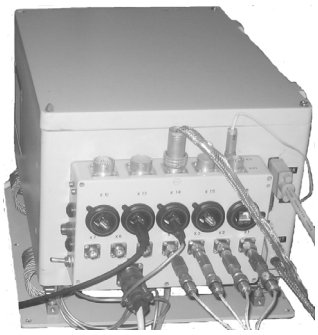


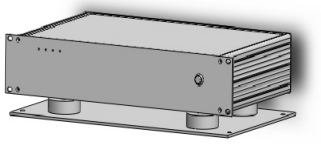

Рис.2. Состав оборудования

*2. Характеристика аппаратуры*



- Диапазон рабочих частот, МГц 1.5…30,
- Количество каналов приема 2,
- Полоса пропускания приемного канала, Кгц 3.1; 4.5; 9.0,
- Динамический диапазон по основному каналу приема, дБ, не менее 124,
- Чувствительность, мкВ, не более 0.7,
- Избирательность по соседнему каналу на отстройке 5 Кгц дБ, не менее 95,
- Количество значимых разрядов цифрового выхода LVDS (динамический диапазон 127дБ) 22,
- Время перестройки рабочей частоты, мс не более 0.1,
- Температурная нестабильность частоты опорного генератора, не более ±2·10-8.

Рис.3. Приёмник



- Диапазон рабочих частот изделия, МГц 1,5-30,
- Полоса пропускания приемного канала, Кгц 3.1; 4.5; 9.0,
- Напряжение сигнала на входе НЧ, мВ 50 ±5,
- Напряжение сигнала на ВЧ-выходе, мВ 3000 ±450,
- Отношение сигнал/шум на ВЧ-выходе в полосе частот 3,1 Кгц, при отстройках ±10 %, не более, дБ минус 120,
- Время перестройки рабочей частоты не более, мс 0.1,
- Относительное отклонение частоты настройки от номинального значения, не более ±2·10-8.

Рис. 4. Возбудитель

- Диапазон рабочих частот, МГц 1,5-30,
- Пиковая выходная мощность при работе на согласованную нагрузку (50 Ом), Вт 1000 (+259; минус 205),
- КПД, в режиме полной мощности, не менее 35%,
- Время готовности изделия к работе из выключенного состояния после подачи на него электропитания, с, не более 6,
- Время перестройки рабочей частоты, не более, мс 3,0,
- Относительный уровень гармонических составляющих, в выходном сигнале не превышает, дБ:
  - на частотах до 3F минус 55,
  - на частотах от 4F до 8F минус 70
  - (F – частота настройки изделия),
- Относительный уровень шума на выходе, измеренный относительно номинальной мощности при отстройке на ± 10 % от основной частоты изделия, дБ/Гц, не более 170.

Рис.5. Усилитель мощности

- Рабочий диапазон частот, МГц 3,0 - 30,0,
- КСВН, не более:
  - в диапазоне частот от 3 до 4,99 МГц 3,5,
  - в диапазоне частот от 4,99 до 30 МГц 2,
- Диаграмма направленности в горизонтальной плоскости круговая,
- Входное сопротивление, Ом 50,
- Подводимая мощность, кВт 1,2,
- Габаритные размеры изделия в рабочем состоянии не более:
  - радиус без противовесов, м 9,5,
  - радиус с противовесами, м 15,
  - высота, м 15.

Рис.6. Широкополосная антенна

- Скорость передачи информации оконечного оборудования данных (ООД) по декаметровому радиоканалу с полосой пропускания:
  - 3,1 Кгц, бит/с 2400 – 7200,
  - 4,5 Кгц, бит/с 2400 – 9600,
  - 9,0 Кгц, бит/с 2400 – 19 200,
- Длительность работы на одной рабочей частоте в режиме псевдослучайной перестройки рабочей частоты, мс 53,3,
- Вид модуляции ООФМ, ДОФМ, ТОФМ, КАМ,
- Диапазон перестройки рабочей частоты, МГц 1,5- 30,
- Период псевдослучайной последовательности перестройки рабочей частоты $2^{128}$-1,
- Количество рабочих частот, используемых в пакете перестройки 32,
- Время замены забракованной рабочей частоты в пакете перестройки на резервную рабочую частоту без перерыва обмена информации ООД (режим адаптации), с 5,1-54,
- Диапазон адаптации по скорости, бит/с 2400 – 19 200,
- Количество выделенных резервных рабочих частот 96,
- Интерфейс управления радиосредствами RS-485.

Рис.7 Аппаратура передачи данных

*3. Предварительные результаты трассовых испытаний фрагмента системы*

Трассовые испытания фрагмента системы проходили в период с 10.08.2011 г. по 06.09. 20011г. Работа велась круглосуточно с перерывами.

Оконечное оборудование данных (ноутбук) формировало файловую последовательность, которая поступала в аппаратуру передачи данных. Пройдя через канал связи, последовательность сравнивалась в приемной части оконечного оборудования

данных (ООД), где и формировался поток ошибок. ООД обрабатывало полученный поток и формировало по анализу состояния АПД для каждого сеанса связи статистические данные:

– текущая скорость работы;

– текущий режим работы модулятора;

– время поиска максимального количества рабочих частот удовлетворительного качества;

– процент времени с удовлетворительным качеством приема (вероятность ошибки на бит меньше $10^{-3}$ – $10^{-5}$);

– текущее количество рабочих частот удовлетворительного качества (из 32-х используемых в пакете перестройки);

– соотношение сигнал/шум для каждой рабочей частоты (на которой были сеансы связи или ведется работа в настоящий момент времени);

– средняя вероятность ошибки на бит на рабочих частотах удовлетворительного качества;

– частота использования каждой рабочей частоты удовлетворительного качества.

Таблица

Предварительные результаты трассовых испытаний фрагмента системы

| № п.п. | Параметр | Оценка параметра |
|---|---|---|
| 1. | текущая скорость работы, Кбит/с | 2,4 ÷ 19,2 |
| 2. | текущий режим работы модулятора | ООФМ, ДОФМ, ТОФМ, КАМ |
| 3. | процент времени с удовлетворительным качеством приема | 60 ÷100 |
| 4. | текущее количество рабочих частот удовлетворительного качества (из 32-х используемых в пакете перестройки) | 40 ÷100 |
| 5. | соотношение сигнал/шум для каждой рабочей частоты, дБ | < 0 ÷ 26 |
| 6. | средняя вероятность ошибки на бит на рабочих частотах удовлетворительного качества | < ($10^{-3}$ ÷ $10^{-5}$) |
| 7. | частота использования каждой рабочей частоты удовлетворительного качества, % | < 1÷ 3,1 |

В результате трассовых испытаний АСДР ППРЧ доказана высокая эффективность предложенной системы адаптивной декаметровой радиосвязи с использованием ППРЧ. Подтверждена возможность использования декаметровой радиосвязи в системах автоматизированного управления.

**Ефимов Е.А.**
**Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»**

## ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ОТ УТЕЧКИ ИНФОРМАЦИИ ПРИ ЗАСЕКРЕЧИВАНИИ

Информационная безопасность обеспечивается применением аппаратуры засекречивания для информационных потоков, выходящих за пределы охраняемых зон.

Применяются два вида засекречивания – линейное и блочное.

Линейное засекречивание производится кодированием потоков информации, передаваемых по каналам связи. Для линейного засекречивания применяется покупная аппаратура засекречивания, которая кодирует информацию, выходящую из модемов, и декодирует информацию, входящую в модемы. Для предотвращения выхода высокочастотных составляющих, подлежащих засекречиванию информационных потоков, питание схем обработки этих потоков проводится через специальные фильтры, подавляющие высокочастотные составляющие сигналов.

Секретная информация передается в аппаратуру линейного засекречивания по специальному стыку с сигналом ограниченного спектра. Незасекреченная и засекреченная информация передается в аппаратуру через раздельные экранированные кабели.

До передачи засекреченной информации в каналы связи в некоторых случаях используются специальные фильтры, подавляющие высокочастотные составляющие незасекреченного сигнала, которые могут проникнуть на выходы и на входы передатчиков из-за паразитных связей.

Частоты срезов и глубина подавления этих фильтров зависит от скорости передачи и спектров сигналов во время обработки, подлежащих засекречиванию.

Кроме линейного засекречивания используется блочное засекречивание блоков информации отдельными приборами засекречивания.

В стыках аппаратуры блочного засекречивания и аппаратуры помехоустойчивого кодирования используются фильтры высокочастотного подавления спектров засекречиваемых сигналов для предотвращения попадания составляющих засекречиваемых сигналов на входы аппаратуры передачи данных.

Частоты срезов этих фильтров определяются скоростью передачи информации и спектрами засекречиваемых сигналов.

Далее приведены характеристики фильтров, использованных в цепях питания и информационных цепях.

1. *Фильтр помехоподавляющий ФП-009 ИМНЕ.468822.009* предназначен для снижения радиопомех по стыку с интерфейсом М-2 со скоростью передачи 1 Мб/сек.

Частота среза 4МГц.

Вносимое затухание цепей в диапазоне частот 10-1000 МГц:

– 40 дБ в диапазоне частот 10-20 МГц включительно;
– 60 дБ в диапазоне частот 20-40 МГц включительно;
– 40 дБ в диапазоне частот 40-80 МГц включительно;
– 60 дБ в диапазоне частот 80-1000 МГц включительно.

2. *Фильтр помехоподавляющий ФП-010 ИМНЕ.468822.010* предназначен для снижения уровней р/п в цепях первичного питания – двухпроводной сети постоянного тока, изолированной от корпуса, номинальным напряжением 28,5В. Вносимое затухание в полосе задерживания от 150 kHz до 100 MHz не менее 80dB.

3. *Фильтр помехоподавляющий ФП-012 ИМНЕ.468822.012* предназначен для подавления радиопомех в цепях сопряжения аппаратуры с каналами телеграфных сетей по стыку С1-ТГ.

Частота среза на уровне 3dB – 2 kHz.

Вносимое затухание в полосе задерживания от 100 kHz до 1000 MHz не менее 70 dB.

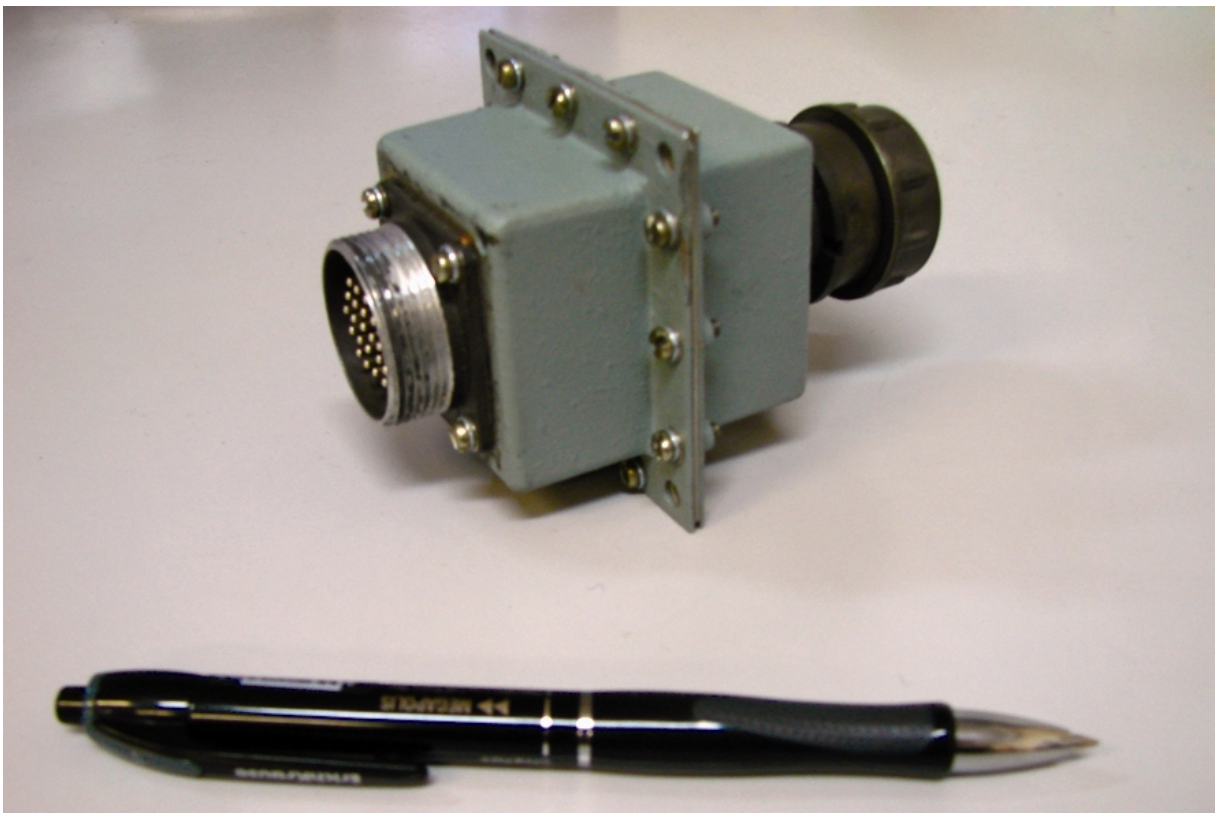


Рис. 4

Фильтр ФП-009 для подавления высокочастотных помех в канале «Манчестер-2», работающего со скоростью 1 Мбит/сек.

**Иванов В.И.**
**Россия, Санкт-Петербург, «Региональный Центр Защиты Информации «ФОРТ»**

## МЕТОДЫ ОБРАБОТКИ И АНАЛИЗА ДАННЫХ ПРИ АДАПТИВНОМ УПРАВЛЕНИИ ИНЦИДЕНТАМИ В ГЕТЕРОГЕННЫХ СЕТЯХ СВЯЗИ

В условиях динамического изменения ресурса информационных систем особое значение по реагированию на инциденты в гетерогенных сетях связи приобретают задачи комплексной обработки и анализа данных о событиях многоуровневой информационной безопасности по универсальным правилам, критериям, процедурам, методам и технологиям их реализации в реальном масштабе времени.

Анализ рынка систем обнаружения вторжений показывает, что заданные в них функции автоматического управления инцидентами в условиях непредвиденного воздействия внешних и/или внутренних угроз, имеющих многообразную природу происхождения, различные форматы представления, а также временные, пространственные и масштабные характеристики, не позволяет простыми методами смены алгоритмов функционирования и подбора оптимальных состояний, поддерживать заданную степень защищенности гетерогенных сетей связи.

Кроме того, следует учитывать, что общая оценка угроз информационной безопасности в этих сетях, определяется согласованными возможностями средств, как правило, автоматизированной регистрации учетных систем в контуре текущей (оперативной) обработки данных и экспертными возможностями аналитических систем в контуре комплексного анализа данных об инцидентах.

Основными причинами, вызывающими проблему адаптивного управления событиями информационной безопасности являются функциональные различия исполнительных систем текущей (оперативной) и комплексной обработки инцидентов, ограниченные вычислительные возможности, прежде всего средств комплексной обработки и анализа данных, распределенная неоднородная инфраструктура гетерогенной сети связи, трудность интеграции приложений, обрабатывающих и предоставляющих информацию о событиях в единую информационную систему.

Пытаясь решить проблему организации адаптивного управления инцидентами, специалисты по безопасности информационных сетей вынуждены отдавать приоритет построению многоуровневой системы обработки и анализа данных на основе создания периметров безопасности. При этом корреляционным, сигнатурным и инвариантным методам решения задач на всех уровнях (прикладного программного обеспечения, системы управления базами данных, операционной системы, сети) предшествуют процедуры нормализации, фильтрации, классификации, агрегации, корреляции и приоритезации данных о событиях информационной безопасности по административно установленным критериям, правилам и метрикам.

Построенные таким образом по принципу «воронки» (рисунок 1), средства мониторинга, аудита и анализа данных об инцидентах оставляют вне поля обработки события с функциями принадлежности нечетких множеств, истинное значение которых было не определено, либо преднамеренно подвергнуто сомнению.

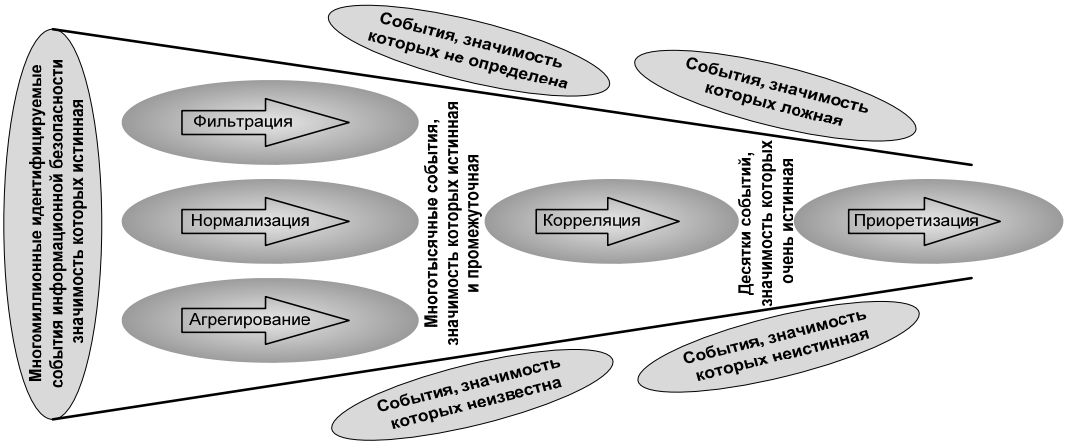



Рис.1. Принцип мониторинга событий информационной безопасности

В конечном результате при существующих методах обработки и анализа данных об инцидентах качество оценивания событий теряет полноценную совокупность своих характеристик и сводится чаще всего к количественной оценке угроз безопасности по пятибалльной шкале (незначительная, несущественная, умеренная, серьезная, критическая), а механизмы безопасности сети настраиваются на регистрацию только видимых явных угроз.

Такой подход в условиях интеграции межведомственных информационных систем значительно усложняет задачу адаптивного управления инцидентами и создает проблему идентификации многомерных событий и ошибок первого, второго рода.

В качестве оценочной шкалы нечеткого множества событий информационной безопасности (табл. 1) могут быть положены принципы построения матрицы суждений по методу Саати Т.Л. [1,2], когда система регистрации событий в гетерогенной сети связи настроена на идентификацию по показателям сравнения истинности события. При этом предлагается следующая градация оценочных суждений значения событий информационной безопасности:

а) «Истинный», «Очень истинный» - показатель оценки «Норма» (события безопасности идентифицированы);

б) «Неистинный», «Ложный», «Неопределено», «Неизвестно» - показатель оценки «Субнормальные»;

в) «Промежуточные» - показатель оценки «Имеющие точки перехода».

Таблица 1

Шкала оценки нечеткого множества событий информационной безопасности

| Сравнительные показатели оценки значений событийной модели | |
|---|---|
| Числовая оценка $S_{in}$ | Качественная оценка ранга $r_i$, ранга $r_n$ |
| 1 | Одинаковая значимость.<br>Значения имеют одинаковый ранг, не влияют на выбор и/или поглощаются без усиления значимости |
| 3 | Слабое преимущество.<br>Преимущество одного ранга перед другим малоубедительно |
| 5 | Сильное преимущество.<br>Преимущество одного ранга перед другим весомо |
| 7 | Очевидное преимущество.<br>Имеются убедительные свидетельства в пользу значения одного ранга. |
| 9 | Абсолютное преимущество.<br>Имеются свидетельства в пользу одного ранга перед другим с наибольшей мерой убедительности |
| $\varnothing$ | Значимость не определена.<br>Истинность значения ранга не определена в точке измерения. |
| [0,1] | Значимость неизвестна.<br>Истинность значения ранга неизвестна в интервале [0,1]. |
| 2, 4, 6, 8 | Промежуточные значения.<br>Точки перехода нечеткого множества данных модели.<br>Преимущество одного ранга перед другим имеет компромисс. |

Такой подход к оценке событий информационной безопасности позволяет моделировать информационную обстановку для разнородных источников событий и средств (систем) их регистрации. Организационные аспекты предлагаемой модели показаны на рисунке 2.

Очевидно, что организующим элементом всестороннего взаимодействия средств (систем) текущей и комплексной обработки данных о событиях является создание интеграционной среды, построенной на платформе промежуточного программного обеспечения Middleware service и ориентированной на технологию объединения и совместного использования удаленных вычислительных, информационных ресурсов в системе безопасности гетерогенной сети связи. Взаимодействие в этой среде организуется

по правилам, описываемым информационной, функциональной, динамической и экспертной моделями, которые являются составными частями обобщенной модели обработки и анализа данных о событиях информационной безопасности.

В основу предлагаемого метода, в отличие от применяемых методов оптимизации и минимизации вычислений, положена концепция организации виртуальной системы текущей обработки и комплексного анализа данных о событиях информационной безопасности, что в свою очередь позволяет моделировать полную событийную обстановку, устанавливать возможный замысел нарушителя, сценарии и трассы вторжения в систему, а также строить долгосрочные прогностические модели безопасности.

Задачами моделируемой интеграционной системы является эффективное распределение имеющихся вычислительных, сетевых и информационных ресурсов безопасности, ресурсов хранения данных о событиях, а также их координация в зависимости от состава и масштаба виртуальной модели, временных факторов реализации текущих и комплексных задач и целей, условий конфиденциальности и наличия, требуемых программных, программно-аппаратных, аппаратных компонентов сервисно-ориентированной архитектуры, которая способна выполнять функции как автоматической, автоматизированной, так и ручной обработки и анализа данных. При этом в структурном слое текущей обработки данных будет преобладать автоматизированная типовая модель оценки событий и противодействия угрозам, а в слое комплексной обработки и анализа данных – гибридные схемы.

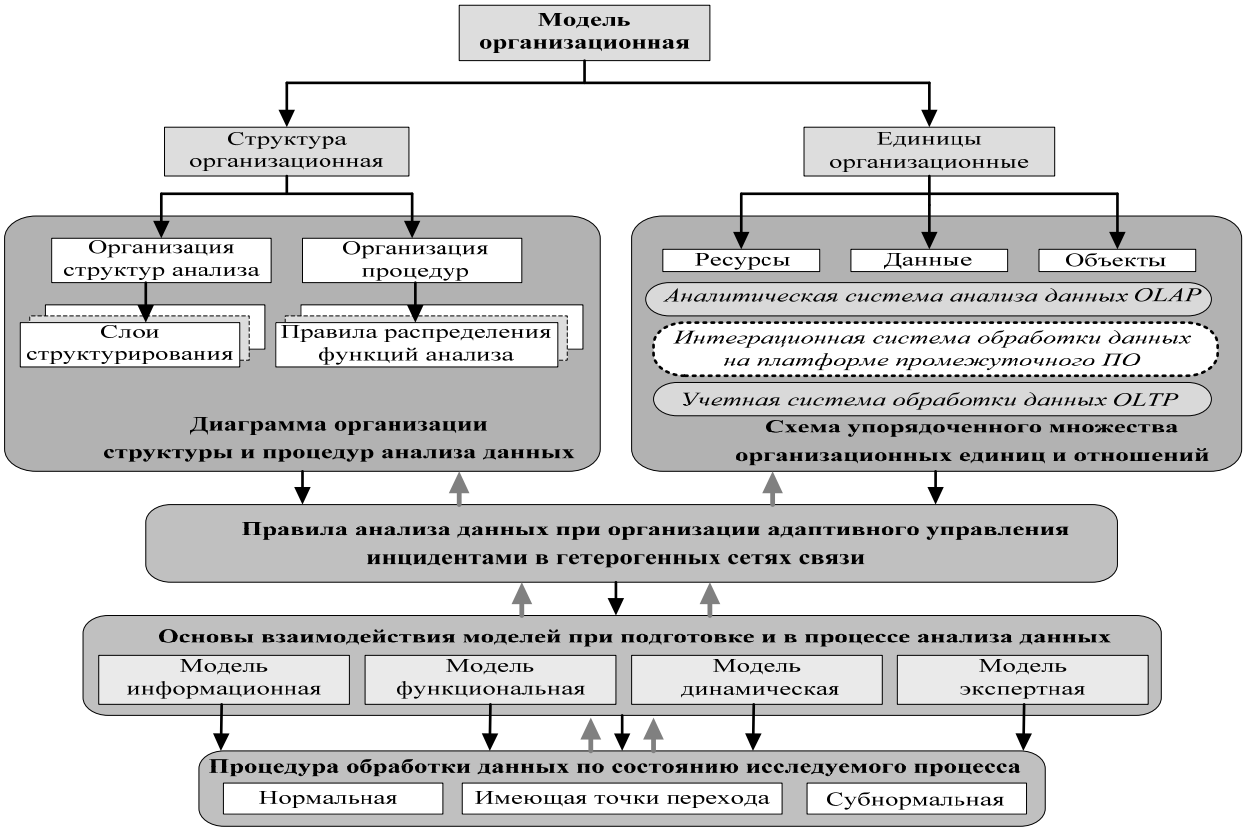



Рис.2. Модель организации системы обработки и анализа данных об инцидентах

Вариант алгоритма обработки и анализа данных об инцидентах в гетерогенной сети связи представлен на рисунке 3.

Создание интеграционной среды на платформе промежуточного программного обеспечения позволяет повысить эффективность и качество управления инцидентами, задает общий постоянный алгоритм функционирования системы безопасности, при котором локальные средства ведут текущую обработку событий, блокируют идентифицируемые угрозы, а затем по трассам событий передают полученные данные в интеграционную среду, ресурсы которой, при участии в ней системы комплексного анализа, позволяют в реальном масштабе времени исследовать многообразие сложных угроз и осуществлять обновление механизмов противодействия.

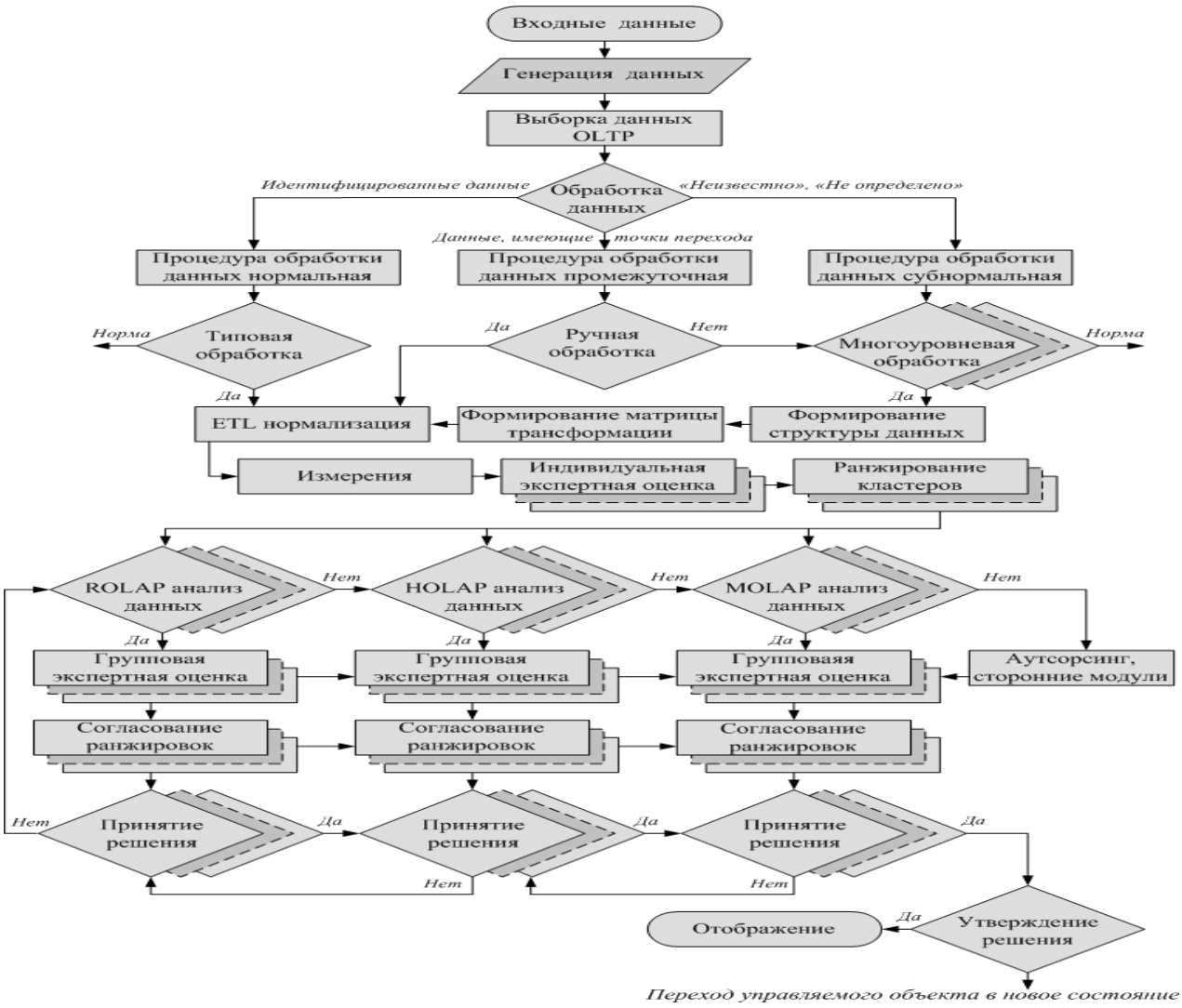



Рис. 3. Алгоритм организации процесса обработки и анализа данных (вариант)

## СПИСОК ЛИТЕРАТУРЫ

1 Шумский А.А. Системный анализ в защите информации: Учебное пособие – М.: Гелиос АРВ, 2005, 224 с.

2 Корченко А.Г. Построение систем защиты информации на нечетких множествах: Теория и практические решения – К.: «МК-Пресс», 2006, 320 с.

3 Саати Т.Л. Принятие решений. Метод анализа иерархий: Перевод с английского – М.: Радио и связь, 1993, 320 с.

4 Антимонов С.Г. Мониторинг событий информационной безопасности и защита персональных данных: www.DialogNauka.ru

5 Демичев А.П. Введение в грид-технологии: Препринт НИИЯФ МГУ, 2007, 11/832.

**Копыльцов А.А., Нечитайленко Р.А.**
**Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»**

## ОБЕСПЕЧЕНИЕ ПОРОГОВОЙ БЕЗОПАСНОСТИ ОБРАБОТКИ СЛАБО ФОРМАЛИЗОВАННОЙ ИНФОРМАЦИИ ПРИ РАСПРЕДЕЛЕННОМ УПРАВЛЕНИИ С ЦЕЛЬЮ ПРИНЯТИЯ РЕШЕНИЙ

Проблема сбора, хранения, передачи слабо формализованной информации, и на основе ее обработки - принятия решения, актуальна как никогда ранее, из-за бурного развития геоинформационных систем. Эта проблема имеет как теоретический, так и практический интерес (Журкин И.Г., Шайтура С.В., Орлов А.И., Петровский А.Б.). Одной из важных практических задач является задача обеспечения безопасности при передаче и обработке информации, с целью принятия решений при распределенном управлении. Важной временной характеристикой обеспечения безопасности является интервал времени, в течение которого собирается, передается и обрабатывается информация, перед

принятием решения. Учитываются два важных аспекта подготовленности информации к абстрагированию: к назначенному времени обработки и достаточной полноте с надлежащей предварительной обработкой. Стратегическая подготовленность информации в психологии управления уравновешена и решена как «Квадрат Наполеона» (Теплов Б.М. Ум полководца. М: Наука, 1980), и в значительной степени опирается на интуитивные формы управления.

В связи с разнородностью принимаемых решений и различной степенью формализованности управленческой информации предполагается подход, допускающий единые формы обработки информации с широкими границами формализации, структурирования и связности. Одновременно учитывается сложившиеся формы предпочтения представления информации для различных предметных областей в военном деле, в бизнесе , в промышленности и науки.

Интенсивное развитие средств вычислительной техники, открыло возможность сочетать средства от интуитивных подходов и строгих алгоритмов и математических моделей, а в связи с развитием быстродействующих суперкомпьютеров и кластеров, оказалось возможным реализовать эти алгоритмические подходы и модели в реальном масштабе времени. Далее рассматривается разработанный алгоритм обработки слабо формализованной информации, состоящий из 7 шагов.

1. Информация поступает в модуль «Классификация», где, с помощью разработанных алгоритмов, осуществляется классификация поступающей информации на классы К1,…, KN. Параметры этих алгоритмов изменяются в процессе работы системы, т.е. это самообучающаяся система. На начальном этапе работы системы можно использовать либо обучающую выборку, либо случайным образом сгенерированное распределение поступающей информации между классами.

2. Информация, поступившая в каждый из классов, подвергается своей, присущей данному классу, свертке (алгоритму обработки информации). В итоге получается информация, обработанная специальным образом, присущим данному классу. В алгоритме используется понятие свертки f, суть которой состоит в следующем. Пусть N - достаточно большое число. Согласно исследованиям по методам и модели оценивания качества программного обеспечения. (Воробьев В.И., Копыльцов А.В., Пальчун Б.П., Юсупов Р.М.), можно взять некоторую выборку показателей с N>=20.

P1=0, P2=1/N, $P_3$=2/N,...., Pn+1=1, где P -

- весовые коэффициенты в формуле для расчета величины i-го показателя n-1-го порядка, представляющей собой взвешенную сумму Kj (j=1,...,Si) и Kj принадлежит промежутку [0,1] – нормированных числовых значений показателей n-го порядка, определяющих i-й показатель n-1-го порядка, Sj - число показателей n-го порядка, определяющих fi. Формируется пакет условий, соотносящих номер показателя и степень его важности. Условие «показатель с номером m примерно такой же или чуть важнее показателя с номером n» означает, что Pm - больше или равно Pn. Условие «показатель с номером m важнее показателя с номером n» означает, что Pm больше Pn. Условие «показатель с номером m существенно важнее показателя с номером n» означает, что существует, по крайней мере один Pq, такой что Pm больше Pq и Pq больше Pn.

Величины fi определяются для всех i = 1,...,F с учетом введенных отношений порядка между показателями (примерно такой же или чуть важнее, важнее, существенно важнее) и условий нормировки для Pj.

Поскольку Si меньше N+1, то для каждого i количество fi больше 1, т.е. для каждого показателя n-1 -го порядка получаем несколько значений fi. Можно определить среднее значение fi (которое равно f), дисперсию и среднеквадратичное отклонение. Процедура получения f называется сверткой.

3. После свертки осуществляется оценивание достоверности и безопасности обработанной информации в каждом классе, путем сравнения ее с ранее полученной информацией (предполагается, что есть хранилище ранее полученной информации). Если информация недостоверна или небезопасна (достоверность и безопасность ее ниже некоторых, заранее заданных для каждого класса уровней), то осуществляется возврат в начало алгоритма: информация подвергается повторной классификации и помещается в другой класс.

4. Установление связей между вновь полученной информацией в каждом классе и ранее полученной информацией, находящейся в хранилище. Если количество связей

меньше некоторой, заранее заданной величины, специфичной для каждого класса, то осуществляется переход в п.1, в котором информация подвергается повторной классификации и помещается в другой класс.

5. Оценивание вероятности, с которой можно доверять полученной информации в каждом классе – устанавливается требуемый порог безопасности для этого класса. Если вероятность меньше некоторой, заранее заданной величины, специфичной для каждого класса, то осуществляется повторная классификация, возврат в начало алгоритма для отнесения к другому классу.

6. Поддержка принятия решений в каждом классе: генерируются рекомендации для каждого класса (что и когда нужно делать, если получена такая информация).

7. Сбор сгенерированных решений, синхронный по назначенному времени и назначенной полноте в заданном формате из всех классов. Анализ сгенерированных решений в классах и генерация на их основе новой совокупности решений в поддержку принятия решения. Вывод рекомендаций (что и когда нужно делать). Окончательное решение (выбрать какое-то решение из рекомендованных, или принять свое собственное решение) принимает человек.

Предлагаемый алгоритм можно использовать, как оболочку специфичны технических решений с рекомендуемыми инструментальными средствами в различных областях и условиях применения. Представляется интересным и обоснованным использование алгоритма в гибридных системах принятия решения и экспертного оценивания, предназначенных для широкого круга организационных задач, обладающих количественными и качественными данными. Вживление алгоритма в среду отлаженных технологических решений позволяет продуктивно использовать растущую производительность современных компьютеров и включается в распределенные коммуникационные системы принятия как автономных, так и взаимосвязанных решений, с соблюдением устанавливаемых порогов безопасности обрабатываемой информации.

**Мартьянов А.Г.**
**Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»**

## ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ

Информационная безопасность предприятия включает в себя большой спектр различных направлений:

– это и современные средства защиты информации;
– информационная безопасность телекоммуникационных сетей;
– подготовка и переподготовка кадров в области обеспечения информационной безопасности;
– безопасные информационные технологии.

Рис. 1

Но в современном мире вопросы информационной безопасности необходимо представлять в более широком спектре. Представим себе на минуту, что все наши средства и системы, разработанные и изготовленные по суперсовременным технологиям, остались без электрической энергии. Или часть лабораторий с уникальным оборудованием оказалась залита водой из-за прорыва сетей водоснабжения, или еще хуже – произошел большой пожар. Поэтому необходимо включать в понятие «информационная безопасность предприятия» и такие направления как:

– энергетическая безопасность и эффективность (развитие энергетической составляющей, включающей в себя, в том числе и аварийные источники электроэнергии – дизельные электростанции, аккумуляторы);

– все мероприятия по линии МЧС (пожарная безопасность, защита от стихийных бедствий, наводнений, чрезвычайных ситуаций);

– создание современных систем охраны и видеонаблюдения;

– кадровая политика в области инженерной безопасности.

Большое значение в этом имеет своевременное, качественное и в необходимых количествах обеспечение предприятия энергетическими ресурсами. Особое значение этот факт имеет в наши дни с целью безусловного выполнения требований Федерального закона № 261-ФЗ от 23.11.2009 г. «Об энергосбережении и о повышении энергетической эффективности и о внесении изменений в отдельные законодательные акты Российской Федерации».

С этой целью на предприятии разработана и утверждена Генеральным директором «Программа в области энергосбережения и повышения энергетической эффективности ФГУП «НПО «Импульс».

Выполняется много мероприятий, основными из которых являются:

– полное оснащение предприятия приборами учета электрической энергии (смонтирована автоматизированная информационно-измерительная система коммерческого учета электроэнергии), воды и тепловой энергии (завершен монтаж и проводятся испытания узла учета тепла);

– предприятие является членом Саморегулируемой организации «Некоммерческое партнерство «Экспертиза энергоэффективности»;

– проведение постоянного анализа работы энергоемких систем, переход на менее энергоемкие или локальные системы (внедрена система плавного пуска двигателя вентсистемы, система канального кондиционирования, система поддержания температурного режима в помещениях стенда Главного конструктора и.т.д.);

– проведение закупок современного, имеющего высокую энергетическую эффективность оборудования;

– ежегодный комплекс работ по обеспечению нормальных условий работы в зимний период;

– введение в эксплуатацию системы аварийного энергоснабжения с использованием дизель-генератора;

– другие мероприятия.

Заключен договор и проводятся работы по испытаниям высоковольтных электроустановок предприятия, реконструкции релейной защиты, ремонту кабельных линий, что позволяет обеспечить бесперебойную работу электрических сетей предприятия, повысит их надежность.

Проводится большой объем работ по модернизации лифтового оборудования.

Большое значение для нормальной работы современного станочного парка имеет обеспечение их качественным сжатым воздухом. С этой целью на предприятии сделаны две локальные системы сжатого воздуха, заключен договор на приобретение и монтаж мощного осушителя для улучшения качества сжатого воздуха.

Проведен комплекс работ и введены в эксплуатацию системы контроля доступа на центральной проходной, на стендах Главного конструктора, в отделе кадров; система видеонаблюдения. В результате полученного опыта эксплуатации в план техперевооружения предприятия внесен вопрос по улучшению характеристик и модернизации данных систем.

Проводится большой объем работ по улучшению условий труда, в том числе:

– аттестация рабочих мест;

– медицинский осмотр сотрудников предприятия;

– улучшение санитарно-бытовых условий (душевые, раздевалки, кондиционирование воздуха);

– ремонт помещений и освещения;

– другие мероприятия.

Для обеспечения безопасности выполнения работ ежегодно проводится обучение главного энергетика и его заместителей, электрогазосварщиков, инженеров лифтового хозяйства, с последующей сдачей экзаменов и получением удостоверений, проводится обучение специалистов в области энергоэффективности, охраны труда, экологической безопасности и др.

Учитывая различный характер работ, проводимый на предприятии, наличие пожароопасных помещений огромное значение имеет выполнение требований пожарной безопасности.

С целью выполнения требований Федерального закона № 123-ФЗ от 22.07.2008 г. «Технический регламент о требованиях пожарной безопасности» на предприятии разработана и зарегистрирована в отделе Государственного пожарного надзора ГУ «СУ ФПС № 50 МЧС России» «Декларация пожарной безопасности» и выполнен расчет уровня обеспечения пожарной безопасности работников предприятия.

Для достижения требуемого, согласно Федерального закона, уровня обеспечения пожарной безопасности работников предприятия необходимо выполнить целый комплекс мероприятий. Учитывая большой объем финансирования, необходимый для реализации, реальность сроков выполнения работ, разработана и утверждена в мае 2010 года «Целевая программа по обеспечению противопожарной защиты ФГУП «НПО «Импульс» на период с 2010 по 2014 г.г.». В основном мероприятия, запланированные этой «Целевой программой…», в 2010-2011 г.г. выполнены.

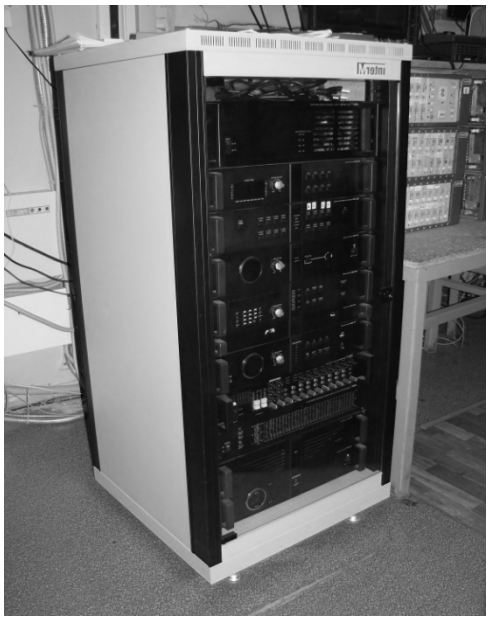


Рис. 2

За два года удалось реализовать много мероприятий, основными из которых являются:

– разработаны проекты автоматической пожарной сигнализации (АПС) и системы оповещения и управления эвакуацией (СОУЭ) по основным корпусам;

– в высотном сооружении произведен монтаж системы подпора воздуха в лифтовых шахтах, системы дымоудаления, выполнена молниезащита корпуса, произведен ремонт и введена в эксплуатацию сплинкерная система пожаротушения, смонтирована автоматическая пожарная сигнализация и система оповещения и управления эвакуацией;

– завершаются работы по монтажу и вводу в строй АПС и СОУЭ в основных корпусах;

– разработаны «План-схемы эвакуации людей на случай пожара» во всех корпусах предприятия;

– закуплены и установлены необходимое количество огнетушителей и пожарных рукавов;

– проводится работа по оборудованию пожароопасных и наиболее значимых помещений современными и безопасными для людей установками автоматического пожаротушения (аэрозольное и порошковое пожаротушение);

– заменены более 1000 светильников, эксплуатирующихся без колпаков и рассеивателей;

– установлено необходимое количество противопожарных дверей в различных помещениях предприятия;

– более 200 человек прошли обучение по пожарно-техническому минимуму;

– ежегодно проводятся 4 противопожарные тренировки (две в составе самостоятельных структурных подразделений и две – объектовые);

– другие мероприятия.

Руководство предприятия делает все, чтобы в полном объеме реализовать «Целевую программу…», что позволит достигнуть требуемый уровень обеспечения пожарной безопасности людей (работников) предприятия.

После монтажа и ввода в эксплуатацию во всех корпусах системы оповещения и управления эвакуацией на ее основе будет реализована объектовая система оповещения по сигналам отдела по гражданской обороне и чрезвычайным ситуациям.

Без реализации этих направлений, модернизации инженерных сетей и оборудования невозможно обеспечить информационную безопасность предприятия.

Поэтому одна из крупных составляющих информационной безопасности предприятия – поддержание, совершенствование и развитие инженерной инфраструктуры предприятия, слаженная и четкая работа всех служб главного инженера.

**Приходько М.А.**
**Россия, Москва, Московский государственный горный университет**

## МУЛЬТИАГЕНТНЫЕ ТЕХНОЛОГИИ В СИСТЕМАХ ДИСТАНЦИОННОГО ОБУЧЕНИЯ

В наше время системы дистанционного обучения зачастую представляют собой большие территориально распределенные комплексы, неоднородные как по составу технических средств, так и используемому программному обеспечению. Задача исследования и моделирования таких систем традиционными методами становится все более трудной, и требует новых подходов для своего решения. Одним из таких подходов является динамично развивающаяся теория мультиагентных систем, позволяющая описать любую большую систему в виде множества интеллектуальных агентов различных видов, взаимодействующих между собой. Подобное описание помимо своей естественности имеет и другие преимущества: возможность описания и моделирования крупномасштабных динамических организаций компонент и групп компонент, возможность оценки свойств групп компонент, предсказания глобальных свойств системы в целом и ее поведения, и многие другие.

Одним из важнейших информационных процессов систем дистанционного обучения является воспроизводство информации, формирование, управление и контроль над информационными потоками, приводящими к перераспределению информации и, в том числе, ее выводу за пределы системы (конечным пользователям). Зачастую процесс перераспределения и доступа к информации, предоставляемой системой, регламентируется рядом правил, в том числе ограничивающих его на платной основе. Это приводит к необходимости создания различных механизмов контроля и ограничения доступа, а также ставит перед проблемой обнаружения нарушений введенных ограничений.

Наиболее распространенным базовым механизмом разграничения доступа является регистрация и последующая аутентификация пользователя в системе. Для незарегистрированных пользователей доступ ограничивается единообразно, а для зарегистрированных – согласно данных их профиля.

Вместе с тем, даже при наличии большого числа ограничений нередко наблюдается эффект несанкционированной «утечки информации», когда пользователь системы, пользуясь регламентированными возможностями и способами получения информации, в конечном итоге получает информацию, доступ к которой для него должен быть ограничен. Проиллюстрируем это явление на примере тестирования.

Представим себе пользователя системы дистанционного обучения, проходящего пробные тесты по некоторому предмету. Пусть общая база вопросов по предмету содержит

500 вопросов, а для пробного теста из общей базы случайным образом отбираются 10 вопросов. В качестве образовательного элемента в конце пробного теста пользователю отображается подробная расшифровка тестирования, содержащая информацию о правильных ответах на вопросы, в которых были допущены ошибки.

Предполагается, что пользователь системы будет использовать пробные тестирования с целью проверки своих знаний, однако существует способ эксплуатации данной функции системы, позволяющий узнать правильный ответ на любой заранее известный вопрос. Для этого достаточно пройти большое число тестов, которое позволит сформировать список всех правильных ответов на вопросы теста. Таким образом, используя регламентированную возможность проверить свои знания, пользователь системы получает доступ к правильным ответам на вопросы по предмету, обладать которыми он, в общем случае, не должен.

Анализ описанной проблемы раскрытия формулировок правильных ответов на вопросы тестирования [2] показывает, что эффективное противодействие несанкционированной утечке информации возможно только при создании многоуровневой интеллектуальной системы фильтрации информации и ограничения прав доступа к ней. В частности, в АСИКЗ «Аргус-М» были реализованы следующие ограничительные механизмы:

– механизм защиты от раскрытия точных формулировок правильных ответов;

– механизм защиты от раскрытия информации о правильности/неправильности варианта ответа;

– механизм защиты от раскрытия набора ответов, гарантирующих определенную оценку;

– механизм защиты от возможного изменения варианта ответа для вопроса, на который ответ уже был дан;

– механизм защиты от нерегламентированной навигации по системе во время прохождения аттестации;

– механизм защиты результатов контроля знаний от попыток несанкционированного изменения без использования системы (т. е. от «взлома» данных системы злоумышленником извне).

Вместе с тем опыт эксплуатации автоматизированной обучающей системы «Аргус-М» [3] убеждает, что традиционных средств противодействия несанкционированной утечке информации в инфокоммуникационных системах недостаточно. Любая возможность получить санкционированный доступ к информации потенциально является источником возникновения ее несанкционированной утечки. А с учетом масштабов современных систем дистанционного обучения само обнаружение утечки информации становится более сложной и важной задачей, чем ее блокирование. Поэтому налицо потребность в разработке новых систем контроля над информационными потоками, призванных не только ограничить доступ к тем или иным данным, но и обнаружить изменения в информационных потоках и появление несанкционированных утечек.

Базисом создания таких систем контроля над информационными потоками инфокоммуникационных систем могут стать мультиагентные системы, построенные на основе интеллектуальных агентов, анализирующих в режиме реального времени информационные потоки. Причем первостепенной задачей данных агентов должно быть не ограничение доступа к информации, а выявление возникновения несанкционированных утечек информации.

Как видно из примера, возникновение таких утечек обусловлено гораздо большим упорядочиванием некоторых действий пользователя, которые в общем случае носят случайный характер. Поэтому критерием выявления несанкционированных утечек информации могут стать энтропийные характеристики системы, описывающие, например, неупорядоченность действий пользователя или функционирования определенных фрагментов инфокоммуникационной системы. Сигналом к активации дополнительных ограничений или блокированию подозрительной активности является снижение энтропии выбранных характеристик, говорящее о росте упорядоченности опасных действий.

Успешное функционирование подобной системы зависит от двух основных факторов. Во-первых, необходимо правильно построить модель мультиагентной системы, разместив интеллектуальные агенты соответствующих типов во всех ключевых узлах инфокоммуникационной системы, участвующих в обработке информации, утечку которой

необходимо предотвратить. Во-вторых, необходимо правильно выбрать характеристики системы, энтропия которых будет использоваться как индикатор несанкционированной утечки информации.

Сама же система должна решать три основные задачи:

– обнаружение возникновения несанкционированной утечки информации;
– выявление причины и адресата несанкционированной утечки информации;
– блокирование нежелательной деятельности с целью предотвращения утечки информации.

Особо обратим внимание, что подобная система не просто состоит из большого числа однотипных агентов, а включает в себя большое число интеллектуальных агентов разных типов, соответствующих разным уровням абстракции (обработки) защищаемой информации. Это позволяет контролировать информацию на всех уровнях, которые могут стать источником утечки, а также использовать большое число различных энтропийных характеристик, повышающих надежность системы защиты. Кроме того, разнотипность агентов и используемых «сигнальных» характеристик затрудняет адаптацию опасных процессов с целью маскировки несанкционированной утечки информации регламентированными действиями. Проиллюстрируем это на ранее рассмотренном примере тестирования.

Информация о правильности выбранного ответа, а также правильном варианте ответа, предоставляется пользователю АСИКЗ «Аргус-М» в нескольких случаях:

– в подробной расшифровке результатов тестирования;
– в сводной таблице результатов тестирования на странице тестирования;
– в сводной таблице результатов тестирования на странице пользователя.

Также информация о возможных вариантах ответа предоставляется пользователю непосредственно в момент прохождения теста. Таким образом, налицо необходимость создания трехуровневой системы, состоящей из интеллектуальных агентов трех типов, собирающих и анализирующих информацию об активности пользователя на уровне прохождения теста, просмотра сводных результатов и просмотра подробной расшифровки результатов.

Данные интеллектуальные агенты должны уметь общаться друг с другом для обмена информацией об активности пользователя. Они также должны уметь анализировать активность многих пользователей с целью выявления корреляций в их действиях следующих типов:

– один человек под видом нескольких пользователей инициирует несанкционированную утечку информации;
– группа пользователей скоординированными действиями инициирует несанкционированную утечку информации.

Наличие нескольких разнотипных агентов усложняет задачу маскировки утечки информации регламентированной деятельностью, т.к. снижение активности пользователя на одном из уровней ведет к повышению активности на другом с целью добычи необходимой информации. А это, в свою очередь, позволяет варьировать качества интеллектуальных агентов, повышая в целом чувствительность системы.

Сформулированная проблема несанкционированной утечки информации открывает новую увлекательную область применения мультиагентных систем в современных системах дистанционного обучения. Требования к мультиагентным системам обнаружения и предотвращения несанкционированных утечек информации закладывают базис их создания, одновременно подсказывая направление развития, заключающееся в поиске и формализации энтропийных характеристик систем дистанционного обучения, которые могут служить индикаторами несанкционированных утечек информации. А область интерактивного тестирования предлагает поле для практической реализации и отработки решений по созданию такой системы.

СПИСОК ЛИТЕРАТУРЫ

1. Приходько М. А. Требования к системам интерактивного контроля знаний в традиционных учебных заведениях (вузах) на примере АСИКЗ «Аргус-М». Международная научно-методическая конференция «Информатизация образования-2009». Июнь 2009. Материалы конференции.

2. Приходько М. А. Автоматизированная обучающая система «Аргус-М»» - первый свободный веб-сервис дистанционного обучения. Пятый международный научный конгресс "Роль бизнеса в трансформации российского общества". Март 2010. Сборник тезисов доклада.

**Расторгуев В.Я., Виноградов А.А.**
**Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»**

## УСИЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КРИТИЧЕСКИХ СИСТЕМАХ НЕПРЕРЫВНОГО ФУНКЦИОНИРОВАНИЯ ПУТЕМ ВИРТУАЛИЗАЦИИ ЭЛЕМЕНТОВ ИХ СИСТЕМ УПРАВЛЕНИЯ

Термин «виртуализация», использованный в названии доклада, требует пояснения ввиду многозначности. В самом общем определении под глаголом «виртуализировать» понимают действие, состоящее в том, чтобы взять нечто, имеющее одну форму, и заставить его казаться имеющим другую форму.

При таком определении близким родственником (а м.б. даже синонимом) виртуализации может показаться на первый взгляд термин «моделирование», намного опередивший по времени появления термин виртуализация. Однако между этими понятиями есть различия.

Моделирование применяют для построения идеализированного образа (модели) некоторого объекта с основной целью удешевления получения прогнозов поведения объекта и сокращения таким образом рисков потери работоспособности объекта в результате экспериментов с ним. Модель всегда связана с моделируемым объектом принципом подобия, является средством исследования моделируемого объекта и не становится самостоятельным объектом эксплуатации.

Виртуализация допускает построение новой производной формы представления для некоторой первичной формы с необязательным использованием принципа подобия. Эта новая форма далее иногда становится самостоятельным объектом со своей историей эволюции, часто отличающейся от истории эволюции первичной формы. Для подтверждения этого достаточно вспомнить, например, кажущийся парадоксальным термин «виртуальная реальность».

Назовем общие направления виртуализации, используемые в компьютерной инженерии. Здесь виртуализировать такой объект, как компьютер, означает заставить компьютер казаться сразу несколькими компьютерами, фрагментом компьютерной сети или же компьютером совершенно иного типа (архитектуры). Виртуализацией м.б. названа также ситуация, когда несколько компьютеров представляются как один отдельный компьютер. Обычно результат этого действия называют серверным кластером.

Отметим отдельно также и то, что виртуализация дается не бесплатно, а иногда требует заметных «накладных» расходов, снижающих производительность Виртуальных Процессоров (ВП) на 2-3 порядка относительно производительности Физических Процессоров (ФП), на которых они развернуты.

На идеях интернета и виртуализации элементов глобальных компьютерных сетей специалистами таких мировых фирм-разработчиков виртуальных сред, как, например: VMWare, Xen, Parallel, Cisco, Citrix и т.д. построена современная и перспективная концепция «облачных» сервисов и вычислений. Использование этой концепции обеспечивает клиентам непрерывно и надежно функционирующую вычислительно-информационную среду, обладающую уникальными характеристиками в части мобильности точек базирования сервисов на ВП, ВП на ФП и, как следствие, их надежности и живучести. Разумеется, это оказывается возможным при одновременном введении мер противодействия жестким условиям эксплуатации ФП в Центрах Обработки Данных (ЦОД), которые из-за своей жесткости представляют угрозу для работоспособности как ФП, так и ЦОД.

Назовем некоторые полезные следствия использования идей виртуализации, на основе которых оказывается возможным в вычислительных сетях:

– Произвести консолидацию различных сервисов, задействовав целиком ФП, и, балансируя при необходимости виртуальные сервисы между ФП, поднять КПД используемого оборудования при одновременном сокращении энергопотребления.

– Перемещать при необходимости ВП с ФП на ФП без их остановки, увеличивая доступность сервисов для конечных пользователей.

– Не привязывая сервисы, размещенные на ВП, к конкретному ФП, свободно перемещать их между ФП с целью технического обслуживания освобождаемых ФП без остановки вычислений. При этом в одном вычислительном пуле оказывается возможно совмещать вычислительное оборудование разных производителей.

– Серьезно упростить обслуживание гостевых Операционных Систем (ОС) внутри ВП, т.к. при этом исчезает необходимость физических манипуляций с ФП и появляется еще один уровень удаленного контроля над сервисами со стороны администраторов.

– Значительно сократить количество проблем, связанных с неисправностью ФП и дефектами драйверов его отдельных устройств. Дело в том, что в относительно консервативной виртуальной среде ОС работают со специальными драйверами виртуальной периферии, поставляемыми квалифицированными разработчиками виртуальной среды. Эти драйверы, как правило, лучше написаны, отлажены, протестированы и апробированы. На время устранения неисправности ФП ОС с активными приложениями м.б. перемещена вместе с ВП на исправный ФП. Современные технологии позволяют делать это автоматически и относительно быстро.

Из сказанного следует, что идея виртуализации вычислительного оборудования может в перспективе стать основой увеличения информационной безопасности в информационных системах продолжительного и непрерывного функционирования и, что особенно ценно, в Системах Управления Критическими Системами Непрерывного Функционирования (СУ КСНФ) за счет практически полного устранения угроз физического и морального старения оборудования из-за эффектов:

– отсутствия отказов ВП, т.к. ВП принципиально физически не стареет,

– устранения морального старения ВП, т.к. темп морального старения ВП никак не связан с темпом морального старения ФП. Это позволяет, если необходимо, исключить моральное старение ФП путем своевременной его модернизации, одновременно законсервировать на долгое время среду выполнения ответственных критических приложений (ВП, гостевую ОС, собственно приложений и т.д.), и, проведя их глубокую отработку, тестирование и опытную апробацию в законсервированной виртуальной среде, обеспечить, таким образом, безопасную эксплуатацию этих приложений.

Однако, следует признать то, что в настоящее время виртуализация практически не используется в СУ КСНФ и этому, по нашему мнению, способствуют, как минимум, три причины:

– «новизна» метода виртуализации для сообщества разработчиков различных СУ КСНФ,

– необходимость наличия запаса производительности ФП в 2-3 порядка из-за больших накладных расходов на поддержку ВП, часто отсутствующего в ФП из состава СУ КСНФ,

– преимущественное использование в СУ КСНФ специализированных процессоров двойного назначения с уникальной архитектурой, в некоммерческом отечественном исполнении, устойчивых к жестким условиям эксплуатации (термическим, механическим, электромагнитным, радиационным и т.д. воздействиям), но, к сожалению, не обладающих достаточной для эффективной виртуализации производительностью и оперативной памятью. Эти процессоры сегодня, как правило, находятся вне зоны коммерческих интересов мировых фирм-разработчиков программных средств виртуализации.

Первая причина имеет временный характер и, очевидно, м.б. устранена. Влияние второй причины в последние годы заметно сокращается за счет освоения отечественными фирмами новых производительных элементных баз и появлении на рынке специализированной вычислительной техники двойного назначения с рабочей частотой ~100-1000 Мгц. По поводу возможности устранения третьей причины, путем привлечении внимания мировых фирм-разработчиков виртуальных сред к учету особенностей вычислительной техники двойного назначения, применяемой в СУ КСНФ у нас есть сильные сомнения в успехе из-за узости рынка специализированной вычислительной техники двойного назначения в сравнении с коммерческой. Поэтому поиск способа виртуализации элементов СУ КСНФ, работающих без прямой опоры на решения мировых фирм-разработчиков виртуальных сред, является актуальной задачей, возможные подходы к решению которой представлены ниже.

Любой из многочисленных способов виртуализации, достаточно полный перечень которых приведен, например, в [1, 2], предполагает такую модель вычислительного процесса, в которой приложение работает в многоуровневой операционной среде, образованной несколькими ОС, развернутыми на ФП (см. рис. 1). Работа приложения состоит в последовательной (в соответствии с алгоритмом приложения) выдаче запросов

либо ФП (команды ФП), либо какой-нибудь ОС (запрос на системное действие). На рис. 1 пунктиром выделены условно-возможные запросы ограниченного применения. Если алгоритмы приложений с номерами от 1 до M, размещены на M экземплярах ВП, то на каждом из ВП м.б. создана своя операционная среда, а рис. 1, соответственно м.б. мысленно рекурсивно расширен, если приложение само является ОС или программно реализует логику ВП некоторой физической или абстрактной архитектуры. Рассматривая подробнее рис. 1 увидим, что:

– каждое приложение выполняется в своем стеке операционных систем, в основном выдает системные запросы к операционной системе, находящейся на вершине своего стека и ограниченно может (если это не запрещено особо) выдавать системные запросы к любой из операционных систем своего стека. Кроме того, разумеется, возможна прямая выдача команд для ФП;

– стеки операционных систем различных приложений могут иметь различный состав уровней и глубину.

В качестве типового решения для построения среды виртуализации, состоящей из нескольких ВП, на отдельном ФП и для последующего развертывания на каждом из ВП своей собственной и независимой от остальных (если это необходимо) системы вычислений достаточно воспользоваться операционной средой из двух уровней, изображенной на рис. 2. Очевидно, что эта двухуровневая операционная среда является частным случаем многоуровневой операционной среды, приведенной на рис. 1, Точнее говоря, она м.б. получена поэтапно путем:

– Выбора относительно функционально-мощной первичной мультисреды (обычно мультизадачной или мультипроцессовой ОС), в роли которой часто используют Linux или Windows, хотя здесь могут быть и другие варианты.

– Выбора наиболее подходящей для последующих этапов и поддержанной в первичной мультисреде единицы многозадачности (задача, процесс, поток и т.д.).

– Построения на основе выбранной единицы многозадачности некоторого ВП путем создания отдельного приложения-эмулятора ВП, программно реализующего логику работы архитектуры либо некоторого физического (intel-x86, mips, arm, sparc и т.д.), либо абстрактного (java-ВП, shell-ВП, linux-ВП, windows-ВП и т.д.) процессора.

– Циклического развертывания на каждом из ВП_k вторичной мультисреды_k для k из диапазона $0 < k < m+1$.

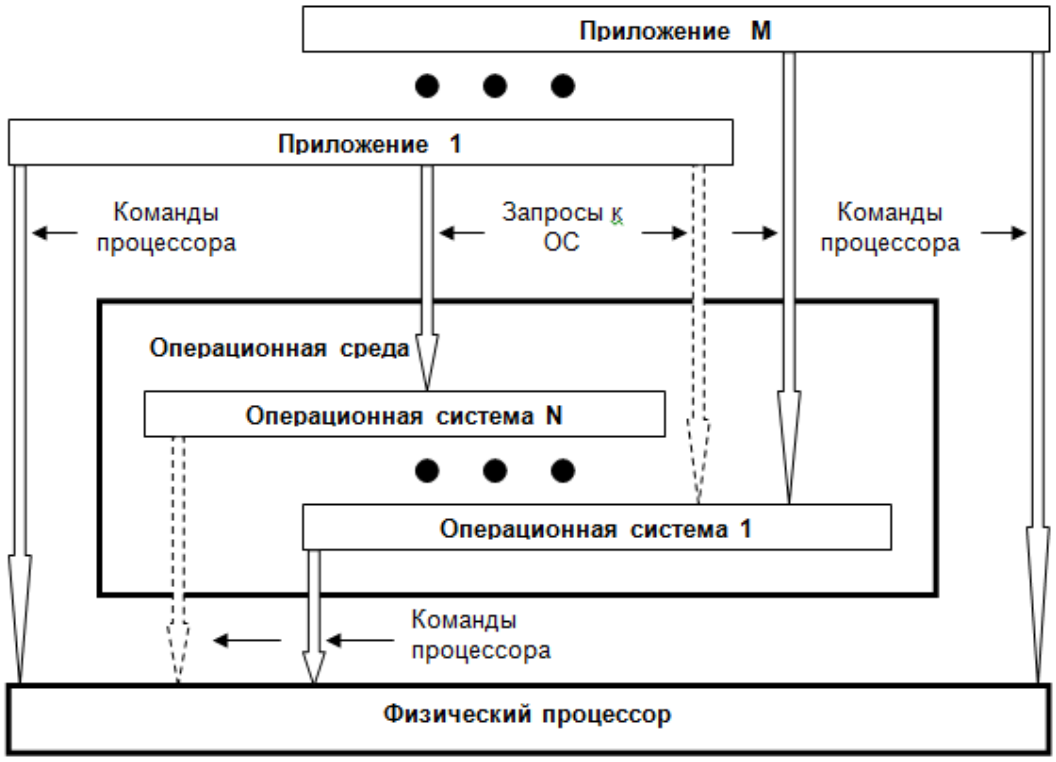



Рис. 1. Состав многоуровневой операционной среды. Общий случай


Рис. 2. Типовой состав операционной среды для построения системы из нескольких ВП

На практике этапы 1-3 выполняются фирмами-разработчиками виртуальных сред с включением полученных результатов в продаваемые ими пакеты средств виртуализации и только этап 4 выполняется покупателями-пользователями. В подавляющем числе случаев при выполнении этапа 3 фирмы-разработчики виртуальных сред предпочитают использовать архитектуры некоторых физических, а не абстрактных процессоров, если не считать особый случай с java-ВП. Более того, из всех принципиально-возможных архитектур физических процессоров, видимо, по коммерческим соображениям эти фирмы выбирают только архитектуру intel-x86 (как наиболее распространенную), игнорируя, например, RISC-архитектуры двойного назначения (mips, arm и т.д.), часто используемые именно в СУ КСНФ, что препятствует проникновению идей виртуализации в СУ КСНФ. Устранить это препятствие теоретически можно, выполнив все этапы с 1 по 4 самостоятельно, не прибегая к услугам фирм-разработчиков виртуальных сред, и выполняя этап 3 одним из двух способов:

– построением ВП, эмулирующего ФП, с необходимой физической архитектурой,

– использованием ВП с абстрактной архитектурой адекватной одновременно как первичной, так и вторичной мультисредам (например: linux-ВП, windows-ВП и т.д.).

Первый способ практически нереализуем, т.к. для получения качественного результата требует недостижимо высокой в среде программистов-прикладников квалификации, которой обладают только профессиональные системные программисты-разработчики виртуальных сред вообще и ВП в частности. Второй способ м.б. применен как указано выше при выполнении двух условий:

– вхождении ВП с выбранной абстрактной архитектурой в список ВП, поддерживаемых в первичной мультисреде,

– возможности размещения необходимой вторичной мультисреды на ВП с выбранной абстрактной архитектурой.

Первое условие может быть автоматически выполнено в случае правильного выбора функционально-мощной первичной мультисреды.

Второй условие требует наличия у вторичной мультисреды свойства мобильности, т.е. способности параметрической адаптации к ВП выбранной архитектуры, выполняемой методом портирования. Можно говорить, что и это условие тоже, как правило, автоматически выполняется, если учесть то, что в СУ КСНФ в качестве вторичной мультисреды часто используют специализированные мобильные операционные системы двойного назначения, например: VxWorks, RTEMS и т.п.

На рис. 3 приведен пример двухуровневой операционной среды, демонстрирующий один из возможных способов самостоятельного построения виртуальной среды, состоящей из:

– первичной мультисреды – ОС Linux, формирующей набор из N экземпляров linux_ВП, каждый из которых, будучи linux-процессом, одновременно является логическим процессором последовательного действия, работающим квази-параллельно и независимо от других linux_ВП и представляющим собой по сути процессор Фон Неймана с системой команд с повышенной семантикой, образованной из объединения команд ФП и набора системных вызовов ядра ОС Linux,

– вторичной мультисреды – ОС RTEMS, портированной в части пакета сопряжения с аппаратурой (т.е. Board Support Pakage) на программно-аппаратную платформу, формирующую linux_ВП, которая в свою очередь состоит из ФП и ОС Linux.

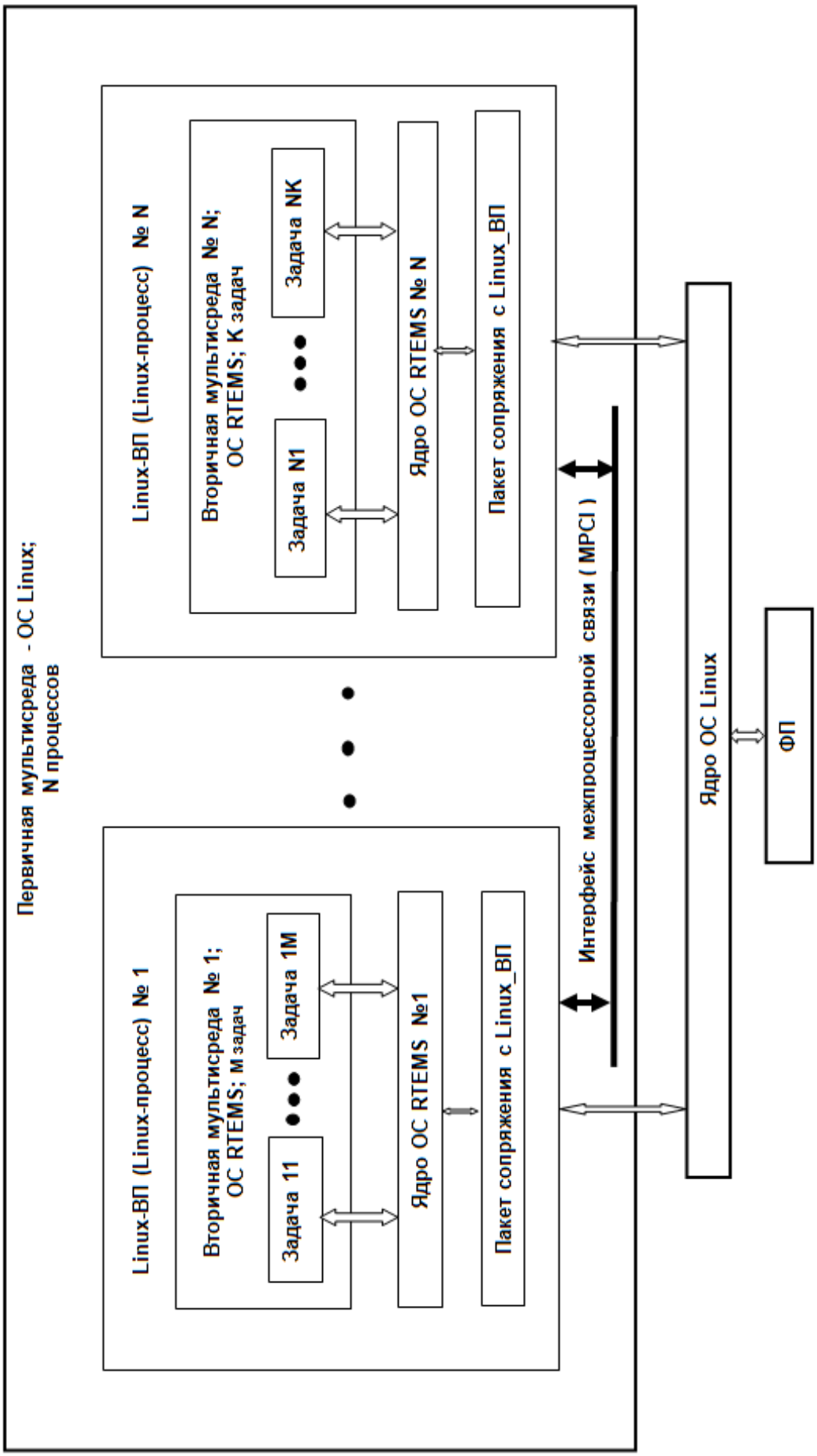



Рис. 3. Пример двухуровневой операционной среды, состоящей из ОС Linux и ОС RTEMS

В заключение отметим, что, с нашей точки зрения, несмотря на низкую степень проникновения идей виртуализации в область СУ КСНФ в настоящее время, рост этой степени в будущем неизбежен после снятия ресурсных аппаратных ограничений ввиду тех очевидных достоинств и перспективности самой идеи виртуализации, которые указаны выше.

СПИСОК ЛИТЕРАТУРЫ

1 M. Tim Jones. Virtual Linux. An overview of virtualization methods, architectures, and implementations: http://www.ibm.com/developerworks/linux/library/l-linuxvirt/index.html?S_TACT=105AGX99&S_CMP=CP.

2 Тормасов А. Виртуализация операционных систем. Электронный журнал «Открытые системы» № 1, 2002 г.

**Тимохин А.П., Бочкарёв В.В.**
**Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»**

## МЕТОДЫ ОБЕСПЕЧИВАЮЩИЕ ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ КОНСТРУКЦИИ АППАРАТУРЫ ДЛЯ СИСТЕМ АВТОМАТИЗИРОВАННОГО УПРАВЛЕНИЯ И ДВОЙНОГО НАЗНАЧЕНИЯ

Конструктивно составные части аппаратуры представляют собой унифицированные базовые несущие конструкции (БНК) трех уровней разукрупнения. Координационные размеры уровней разукрупнения выбраны согласно ГОСТ Р 51623-2000 «Конструкции базовые несущие РЭС. Система построения и координационные размеры».

Аппаратура предусматривает поузловое экранирование электрических и магнитных полей. Экранирующие корпуса стоек и приборов аппаратуры представляют собой замкнутые объемы со съемными крышками.

*1. Конструкция прибора*

Корпус прибора изготовлен из алюминиевого сплава литьем (с последующим фрезерованием) или фрезерованием. Верхнее и нижнее основание выполнены в виде радиаторов с ребрами для отвода тепла от модулей.

Соединение боковых стенок, верхнего и нижнего оснований производится с применением токопроводящего клея НТК ОСТ 107.460007.004-91 для обеспечения электрического контакта частей корпуса.

Боковые стенки корпуса прибора имеют съемные крышки для свободного доступа к соединителям модуля питания (МПН), фильтра питания и монтажной части входных (выходных) соединителей прибора. После настройки прибора крышки устанавливаются на токопроводящую эмаль ХС-928 и герметизируются по контуру герметиком УП-5-201 ТУ6-05-246-80.

Толщина корпуса прибора выбрана и достаточна для защиты информации, содержащейся в аппаратуре, от воздействия внешних воздействующих факторов (ВВФ) в соответствии с условиями эксплуатации.

Сзади (со стороны пайки объединительной платы) корпус прибора закрыт корпусом МПН, который устанавливается на фланец прибора. Уплотнение для обеспечения герметичности и экранирования происходит с помощью электропроводного резинового шнура.

На лицевой панели прибора устанавливаются внешние соединители типа СНЦ127 АШДК.434410.082ТУ.

Площадь поверхности для установки соединителей 280×100 мм.

Фланцы внешних соединителей расположены снаружи и имеют гальванический контакт с корпусом прибора.

На лицевой панели прибора устанавливается съемная пломбируемая крышка, закрывающая доступ к модулям. Для обеспечения герметичности и экранирования крышка устанавливается через резиновый электропроводный шнур.

*2. Конструкция стойки*

Основой конструктивного построения стойки являются приборные шкафы, которые после установки в них каркасов блочных и проведения монтажа преобразуются в аппаратные стройки.

Шкаф представляет собой конструкцию с переменным количеством этажей, в которых размещаются каркасы блочные (КБ).

Основной модификацией шкафа (стойки) является конструкция, в которой на пяти этажах размещается 5 каркасов блочных.

Шкаф представляет собой штампованный сварной каркас, в котором размещаются элементы конструкции для установки и крепления необходимого количества КБ.

К нижней и верхней части шкафа болтами крепятся верхние и нижние основания. В верхнем основании расположена коробка распределительная (КР) с выходными соединителями и воздуховодные окна для подключения стойки к системе вентиляции.

В нижнем и верхнем основаниях размещаются заборные окна системы охлаждения и устройство регулировки (заслонки) системы вентиляции стойки.

Вентиляционные окна закрыты сеткой с размером ячейки 3×3 мм. Сетка покрыта электропроводным покрытием.

Спереди шкафа предусмотрена экранированная металлическая дверь, закрывающая в рабочем состоянии устанавливаемые в стойку КБ с модулями.

Дверь шкафа оснащена концевым выключателем , который при открывании выдает сигнал в систему диспетчеризации.

Двери, съемные крышки стоек , закрывающие аппаратуру содержащую информацию , имеют места пломбирования заводом-изготовителем и службой эксплуатации , ограничивающих доступ к составным частям аппаратуры посторонним лицам.

Материал, из которого изготовлены верхнее, нижнее основание и шкаф стойки – сталь, толщиной 1,5 мм. Толщина стали достаточна для защиты информации содержащейся в аппаратуре стойки от воздействия ВВФ в соответствии с условиями эксплуатации.

Материалы из которых изготовлены стойки выбраны в соответствии с «Перечнем материалов и покрытий разрешенных к применению в аппаратуре изделий разрабатываемых НПО «Импульс». Аппаратура стойки, содержащая информацию защищена от воздействия пожара и взрывов.

Конструктивные решения принятые при проектировании аппаратуры обеспечивают экранирование корпуса стойки с целью обеспечения информационной безопасности.

**Черкесов Г.Н.**
**Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»**

## ОЦЕНКА ЖИВУЧЕСТИ И ОТКАЗОБЕЗОПАСНОСТИ МАЖОРИРОВАННОЙ ПАМЯТИ С КЛАСТЕРНОЙ СТРУКТУРОЙ

*Введение.* Для повышения надежности и достоверности функционирования оперативной памяти в системах связи, системах управления, бортовых вычислительных системах самолетов, судов, космических аппаратов и других объектов с высокими требованиями к отказобезопасности применяют резервирование типа параллельного мажорирования про схеме «два из трех». При кластерной структуре памяти возможно мажорирование на уровне одного кластера.

Таким образом, структурно память может быть представлена как последовательное соединение мажорированных групп из трех кластеров. При этом процедура голосования может быть проведена как в процессоре, так и в специализированных мажорирующих элементах (МЭ). В необслуживаемых вычислителях возможно накопление отказов отдельных кластеров, возникающих вследствие естественных процессов или в результате внешнего воздействия (например, потоков космических частиц), без потери работоспособности системы. В связи с этим возникает вопрос о том, каков риск потери работоспособности памяти при заданном числе отказавших элементов (кластеров). Это зависит от распределения отказавших элементов по полю памяти.

Мерой риска могут быть условные вероятностные показатели при известном числе пораженных кластеров во всем поле памяти. Они являются показателями живучести (отказоустойчивости). С учетом однородности структуры памяти они могут быть определены с помощью комбинаторных методов. Представляют интерес показатели уровня деградации структуры, такие как вероятность неработоспособности некоторого числа групп при условии неисправности заданного количества структурных элементов (кластеров); вероятность потери работоспособности не более заданного количества групп.

Для обеспечения отказобезопасности и живучести могут использоваться следующие методы: процедуры периодической принудительной регенерации, регулирование размера кластеров, использование резервных кластерных групп, помехоустойчивое кодирование с коррекцией ошибок. При увеличении числа резервных групп вероятность можно сколь угодно близко приблизить к единице. Поэтому важно решить задачу о таком значении числа резервных групп кластеров, который обеспечит практически гарантированный уровень вероятности сохранения важной для системы информации (программ и данных). Достоинство этих показателей состоит в том, что этот уровень гарантируется при любых показателях надежности элементов памяти. Иначе говоря, для принятия решения об уровне резервирования в памяти вообще не надо знать статистики отказов памяти. Если источником поражения кластеров являются внутренние причины, приводящие к отказам ячеек памяти в кластерах или искажению информации в оперативной памяти вследствие сбоев, то необходимо оценивать показатели отказобезопасности [1], учитывающие потоки отказов и сбоев.

При достаточно высокой интенсивности поражения кластеров и (или) длительной эксплуатации изделий в условиях невозможности восстановления деградированной структуры обеспечение высоких показателей надежности и отказобезопасности достигается с помощью определённого сочетания различных методов структурного, информационного и функционального резервирования.

В процессе проектирования резервированной памяти уже на ранних стадиях надо установить приемлемые параметры системы памяти: число групп, размеры кластера, объем резервной части емкости памяти, а также оценить эффект от применения гибкой адресации, помехоустойчивого кодирования и возможности перезагрузки файлов в работоспособную часть памяти. При использовании схем мажорирования важно определить порог голосования в схеме «m из n». Для оптимального выбора параметров требуется количественное обоснование с помощью количественных критериев.

При назначенном ресурсе эксплуатации возникает проблема оценки фактического состояния деградированной структуры с целью принятия решения по критерию приемлемого риска о продлении или сокращении срока эксплуатации. Эти вопросы излагаются в основной части доклада.

*1. Постановка задачи и показатели живучести и отказобезопасности*

Рассматривается оперативная память, состоящая из трех комплектов (линеек) кластеров, трех магистралей (М) и трех полноразрядных мажорирующих элементов (МЭ). Чтение осуществляется с трёх комплектов одновременно и синхронно по запросу процессора или другого смежного устройства. Запись осуществляется по требованию процессора или других смежных устройств, а также по требованию системы восстановления для повышения достоверности и защиты от сбоев. С целью упорядочения анализа будем различать четыре основных режима функционирования: режим чтения (РЧ); режим записи (РЗ); режим диагностирования (РД); режим повышения достоверности (РПД).

Режим РД используется для установления комплекта, данные которого отличаются от данных двух других комплектов. Режим РПД включается либо по сигналу РД, либо по инициативе контроллера периодически. В первом случае делается попытка устранить ошибку, если она произошла вследствие сбоя. При многократной неудаче делается вывод, что в кластере произошел устойчивый отказ и кластер вносится в регистр ошибок. Во втором случае реализуется профилактическая мера по устранению сбойных ошибок. Она состоит из последовательных действий: чтение – запись - чтение. Если при первом чтении есть одно несовпадение, то далее следует запись и чтение. Далее как в первом случае. В режиме записи может три ситуации: в три комплекта записывается одна и та же информация (три МЭ исправны и есть совпадение не менее двух входных данных); запись не производится из-за отсутствия двух одинаковых данных; запись производится только в два комплекта (один МЭ не исправен).

Обнаружение отказов осуществляется: в кластерах памяти путем использования режимов РД и РПД; в контроллерах памяти с помощью встроенных средств аппаратурного контроля и режимов РД и РПД; в МЭ путем сравнения выходов МЭ: при работоспособных МЭ их выходы должны совпадать. Повышение достоверности осуществляется путем

мажорирования; путем исправления сбойных ошибок в кластерах в режиме РПД; путем применения корректирующих кодов (например, кодов Хэмминга).

Для расчета показателей надёжности, отказоустойчивости (живучести) и достоверности необходимо знать следующие исходные данные: количество кластеров в памяти; количество БИС в одном кластере; состояние работоспособности каждого кластера (в каждом из трех комплектов); интенсивность отказов одного БИС памяти; интенсивность отказов контроллера и мажоритарного элемента; интенсивность сбоев в памяти; нормативная длительность функционирования.

Для анализа живучести и отказобезопасности и последующего выбора параметров системы памяти необходимо найти расчетные формулы для трех групп показателей. Условные показатели живучести:

– вероятность $Q^{*(i)}_{nmk}$ того, что в системе из $n$ последовательно соединённых мажорированных групп при условии неисправности $k$ элементов будет неработоспособно ровно $m$ групп, причём в $i$ группах из $m$ будут поражены все три элемента, а $m$-$i$ группах – только два элемента;

– вероятность $Q^{*}_{nmk}$ того, что в системе из $n$ последовательно соединённых групп будет неработоспособно ровно $m$ групп при условии неисправности $k$ элементов, очевидно, что:

$$Q^{*}_{nmk} = \sum_{i=0}^{m} Q^{*(i)}_{nmk}\ , \tag{1}$$

вероятность $Q_{nmk}$ того, что при условии неисправности $k$ элементов в системе будет неработоспособно не более $m$ групп; очевидно, что

$$Q_{nmk} = \sum_{j=0}^{m} Q^{*}_{njk} = \sum_{j=0}^{m}\sum_{i=0}^{m} Q^{*(i)}_{njk}\ . \tag{2}$$

Показатели надёжности при нулевой начальной деградации: вероятность $P^{*(i)}{}_{nmk}(t)$ того, что в момент времени $t$ в системе из $n$ групп будет неработоспособно ровно $m$ групп при наличии $k$ неисправных элементов. Причём в $i$ группах из $m$ поражены все три элемента. Известно, что в начальный момент времени все 3$n$ элементов структуры памяти (кластеров) работоспособны. Безусловная вероятность связана с условной вероятностью соотношением:

$$P^{*(i)}_{nmk}(t) = Q^{*(i)}_{nmk} P_k(t)\,, \tag{3}$$

где $P_k(t)=P(X(t)=k)$ – вероятность того, что за время $t$ будут поражены по тем или иным причинам ровно $k$ элементов; иначе можно определить вероятность (3) как вероятность достижения к моменту $t$ уровня деградации ($n,m,k,i$);

– вероятность $P^{*}_{nmk}(t)$ того, что в момент времени $t$ будут поражены $m$ групп из $n$ при наличии ровно $k$ неисправных элементов и при условии, что в начальный момент все 3$n$ элементов памяти работоспособны; очевидно, что

$$P^{*}_{nmk}(t) = \sum_{i=0}^{m} P^{*(i)}_{nmk}(t) = \sum_{i=0}^{m} Q^{*(i)}_{nmk} P_k(t) = Q^{*}_{nmk} P_k(t)\,, \tag{4}$$

– вероятность $P^{*}_{nm}(t)$ того, что в момент $t$ в памяти будут неработоспособны ровно $m$ групп при условии работоспособности всех 3$n$ элементов в начальный момент времени; очевидно, что

$$P^{*}_{nm}(t) = \sum_{k=0}^{n+2m} P^{*}_{nmk}(t) = \sum_{k=0}^{n+2m}\sum_{i=0}^{m} P^{*(i)}_{nmk}(t)\,, \tag{5}$$

– вероятность $P_{nm}(t)$ того, что в момент $t$ в памяти будут работоспособно не менее $n$-$m$ групп при условии работоспособности всех элементов в начальный момент времени.

Из определений показателей следует, что:

$$P_{nm}(t) = \sum_{j=0}^{m} P^{*}_{nj}(t) = \sum_{j=0}^{m}\sum_{k=0}^{n+2m}\sum_{i=0}^{m} P^{*(i)}_{njk}(t), m = 0...n\,. \tag{6}$$

При необходимости с помощью (6) для различных $m$ можно рассчитать среднюю наработку до отказа системы:

$$\overline{T}_{c,nm} = \int_0^\infty P_{nm}(t)dt, m = 0...n\,. \quad (7)$$

Если минимальный рабочий объём памяти задан и требует работоспособности не менее $n_0$ групп, то объём памяти $m$=$n$-$n_0$ групп можно считать резервным и предназначенным для обеспечения заданного уровня вероятности безотказной работы

$$P_c(t, n_0, m) = P_{n_0+m,m}(t, n_0, m)\,, \quad (8)$$

или средней наработки до отказа:

$$\overline{T}_c(n_0, m) = \int_0^\infty P_c(t)dt\,. \quad (9)$$

Гамма - процентный ресурс безотказности $T_\gamma(n_0,m)$ определяется как интервал времени, в течение которого вероятность безотказной работы будет не менее $\gamma$, то есть $T_\gamma(n_0,m)$ является решением уравнения:

$$P_c(T_\gamma, n_0, m) = \gamma, m \ge 0\,. \quad (10)$$

Если требования к надежности содержат нормативное значение $T^0_\gamma$, то в соответствии с (10) подбирают такое значение $m$, чтобы:

$$T_\gamma(n_0, m) \ge T^0_\gamma\,. \quad (11)$$

Аналогично вводятся показатели надёжности при ненулевой деградации (пост-деградации). Назначение этой группы показателей состоит в том, чтобы давать прогноз показателей надёжности изделия на время $t$ эксплуатации, следующего за интервалом $t_0$ с начала эксплуатации. При этом надо иметь в виду, что расчёт показателей надёжности в интервале ($t_0$, $t_0$+$t$) может быть проведен и до начала эксплуатации как условные показатели надёжности:

– вероятность безотказной работы:

$$P_c(t_0, t) = P_c(t_0 + t) / P_c(t_0)\,, \quad (12)$$

– средняя наработка до отказа:

$$\overline{T}_c(t_0) = \int_0^\infty P_c(t_0, t)dt\,, \quad (13)$$

– гамма-процентный ресурс безотказности $T_\gamma(t_0)$ как решение уравнения:

$$P_c(t_0, T_\gamma(t_0)) = \gamma\,. \quad (14)$$

В реальной ситуации по истечении времени $t_0$ фактический уровень деградации характеризуется вектором ($n,m,k,i$). При таком начальном уровне деградации можно рассчитать показатели надёжности в течение последующей эксплуатации и сравнить их с (12) – (14).

Для этого вводятся следующие показатели надёжности:

– вероятность $P^{*(i)}_{nmk,\ m+r}(t)$ того, что за время $t$ уровень деградации достигнет величины $m$+$r$ (увеличится на $r$ число неработоспособных групп) при начальном уровне деградации ($n,m,k,i$);

– вероятность $P^{*}_{nmk,\ m+r}(t)$ того, что за время $t$ уровень деградации достигнет величины $m$+$r$ при начальном уровне деградации ($n,m,k$); эта вероятность рассчитывается в том случае, если при диагностировании не удается установить $i$, и связана с предыдущей вероятностью соотношением:

$$P^*_{nmk,m+r}(t) = \sum_{i=0}^{m} \frac{Q^{*(i)}_{nmk}}{Q^*_{nmk}} P^{*(i)}_{nmk,m+r}(t)\,, \quad (15)$$

вероятность $P^{(i)}_{nmk,\ m+r}(t)$ того, что за время $t$ число дополнительно отказавших групп будет не более $r$ при начальном уровне деградации ($n,m,k,i$); очевидно, что

$$P^{(i)}_{nmk,m+r}(t) = \sum_{j=0}^{r} P^{*(i)}_{nmk,m+j}(t)\,, \quad (16)$$

вероятность $P_{nmk,\ m+r}(t)$ того, что за время $t$ число дополнительно отказавших групп будет не более $r$ при начальном уровне деградации ($n,m,k$); она связана с ранее введенными вероятностями соотношением

$$P_{nmk,m+r}(t)=\sum_{j=0}^{r}P^{*}_{nmk,m+j}(t)=\sum_{j=0}^{r}\sum_{i=0}^{m}\frac{Q^{*(i)}_{nmk}}{Q^{*}_{nmk}}P^{*(i)}_{nmk,m+j}(t)=\sum_{i=0}^{m}\frac{Q^{*(i)}_{nmk}}{Q^{*}_{nmk}}P^{(i)}_{nmk,m+r}(t)\,. \qquad (17)$$

В частности, $P_{nmk,\,m}(t)$ есть вероятность сохранения начального уровня деградации, а $P_{nmk,\,n}(t)$ вероятность потери всей памяти. С помощью (16) – (17) и (13) – (14) могут быть найдены ещё два показателя надёжности, а затем определено то значение $r$, при котором выполняется условие (11).

*2. Результаты анализа*

Вероятность потери $m$ групп из $n$, в том числе $i$ групп с тремя отказавшими элементами, определяется по формуле:

$$Q^{*(i)}_{nmk}=\frac{C^{m}_{n}}{C^{k}_{3n}}C^{i}_{m}(C^{2}_{3})^{m-i}C^{k-2m-i}_{n-m}(C^{1}_{3})^{k-2m-i}=\frac{C^{m}_{n}}{C^{k}_{3n}}C^{i}_{m}C^{k-2m-i}_{n-m}3^{k-m-2i}\,, \qquad (18)$$

для $0\le m\le n$-1, $0\le i\le m$ и $i+2m\le k\le m+n+i$. Вероятность потери ровно $m$ групп:

$$Q^{(i)}_{nmk}=\frac{C^{m}_{n}}{C^{k}_{3n}}\sum_{i=0}^{m}C^{i}_{m}C^{k-2m-i}_{n-m}3^{k-2m-i},2m\le k\le n+2m,0\le m\le n-1\,. \qquad (19)$$

Условная вероятность потери не более $m$ групп определяется по формуле (2). Далее надо использовать формулы (3) – (11) для расчета показателей надежности и отказобезопасности при нулевой начальной деградации и формулы (12) – (17) при расчете показателей пост-деградации.

Анализируя зависимость вероятности потери $m$ групп из $n$ при $k$ отказавших кластеров, можно определить наиболее вероятное значение числа отказавших кластеров $k_0$ , при котором не исправны $m$ групп. Оказывается, что это число во много раз превосходит минимальное число $k_{\min}=2m$, которое достаточно для вывода из строя $m$ групп. Для $m=1$ отношение $\delta=k_0/k_{\min}=7$ при $n=64$ и $\delta=10$ при $n=128$. Для $m=2$: $\delta=5$ и 7 соответственно, а для $m=3$: $\delta=4{,}25$ и 5,83 соответственно. Доля отказавших кластеров (из $k$), которые оказались в работоспособных группах, снизив в них избыточность, но не вызвав отказа группы, значительна. При различных $m$ и $n$ она колеблется в пределах от 50 до 90%. С увеличением $n$ эта доля растет. Этот феномен очень важен для правильной оценки возможности изделия успешно выполнять свои функции в будущем. При относительно малом $m$ создается видимость благополучия, поскольку отказавших групп не много, но надежность памяти низкая. При фиксированном $k$ существует наиболее вероятное число $m_0$ отказавших групп. Оно значительно меньше максимально возможного $m_{\max}=[k/2]$. Например, при $n=64$, $k=19$: $m_0=2$, $m_{\max}=9$; при $n=128$, $k=19$: $m_0=1$, $m_{\max}=9$; при $n=128$, $k=34$: $m_0=3$, $m_{\max}=17$.

Рассчитывая значения вероятности, можно найти такое максимальное значение числа отказавших кластеров, при котором вероятность отказа не более $m$ групп остается на уровне не менее заданного значения $p$. Результаты оценки показывают, что весьма много отказавших кластеров расположено в работоспособных группах. Так при $n=64$, $m=2$, вероятность потери не более двух групп будет не менее 0,9. При этом возможны отказы 16 кластеров, из которых только 4-6 кластеров находятся в отказавших группах, а остальные 10-12 (что составляет 63-75%) находятся в работоспособных группах. При $n=128$ еще большая доля отказавших кластеров (73-82 %) находится в работоспособных группах.

*3. Классификация и вероятностные характеристики уровней деградации*

Все уровни деградации могут быть разделены на две категории: докритические и критические. Чтобы дать определения этих понятий, введем следующие величины: $T$ – заданное полное время функционирования, $t_0$ – промежуточное время, для которого проводится классификация уровней деградации, $t=T-t_0$ - предстоящее время эксплуатации, $\varepsilon_0$ – вектор параметров, характеризующий уровень деградации в момент $t_0$, $P_c(t_0,\ t)$ – вероятность безотказной работы, определяемая по формуле (12), $P_c(\varepsilon_0,\ t)$ - вероятность безотказной работы, определяемая по формуле (17).

Уровень деградации будет докритическим, если при заданных $\varepsilon_0$, $t_0$ и $t$ имеет место неравенство:

$$P_c(t_0,t)\le P_c(\varepsilon_0,t)\,. \qquad (20)$$

Уровень деградации будем называть первым критическим, если:

$$P_c(t_0,t) > P_c(\varepsilon_0,t), \quad (21)$$

и в изделии в полном объёме сохраняются все функции при надлежащем качестве.

Уровень деградации будем называть вторым критическим, если требуется переход от штатного режима функционирования к аварийному с возможной потерей одной из функций либо со снижением качества функционирования: снижение достоверности, снижение производительности и др.

Введем теперь понятия критических моментов времени и критических областей. Представим неравенство (20) в виде:

$$P_c(t_0,T-t_0)/P_c(\varepsilon_0,T-t_0) = b(t_0,T,\varepsilon_0) \le 1, \quad (22)$$

и попытаемся найти значение $t^*_0$, при котором имеет место равенство. Здесь возможны три случая:

1. Решения, принадлежащего интервалу (0, $T$), нет и для любых $t_0 < T$ выполняется неравенство.

$$P_c(t_0,T-t_0) < P_c(\varepsilon_0,T-t_0).$$

Это значит, что уровень деградации $\varepsilon_0$ является всегда докритическим.

2. Есть решение $t^*_0 < T$. Тогда при $t_0 < t^*_0$ будет выполнятся неравенство (21), а для $t^*_0 \le t_0 \le T$ выполняется неравенство (20). Это значит, что при $t_0 < t^*_0$ уровень деградации $\varepsilon_0$ является критическим, а при $t^*_0 \le t_0 \le T$ докритическим.

Область значений [0, $t^*_0$), будем называть критической областью, $t^*_0$ – границей критической области, а любую точку критической области – критической точкой (критическим моментом времени).

3. Решения, принадлежащего интервалу (0, $T$), нет и для любых $t_0 < T$ выполняется неравенство (21). Тогда весь интервал (0, $T$) является критической областью, а момент $T$ – границей критической области.

Знание критической области для каждого уровня деградации $\varepsilon_0$ полезно в том смысле, что если уровень $\varepsilon_0$ достигается «слишком рано», то он становится критическим, но не навсегда. Если он сохраняется в течение некоторого времени до момента $t^*_0$, то после $t^*_0$ уровень $\varepsilon_0$ перестает быть критическим и становится докритическим. Если происходит ещё один отказ и уровень деградации изменяется, то важно знать, в какой области находится момент отказа. Если он находится в докритической области, то выполняются требованию по надежности и эта ситуация не вызывает озабоченности. Если же он находится в критической области, то это сигнал тревоги, требующий, возможно, дополнительных мероприятий.

Желательно иметь такую траекторию деградации изделия, чтобы ни одна её точка не попадала в критическую область. Прогнозировать поведение изделия в течение $T$ и оценивать моменты отказов с точки зрения попадания их в критическую область можно с помощью имитационного моделирования [2].

*Заключение.* Анализ показателей живучести и отказобезопасности резервированной памяти позволяет уже на ранних стадиях проектирования установить приемлемые параметры системы памяти: число групп, размеры кластера, объем резервной части емкости памяти, а также оценить эффект от применения гибкой адресации, помехоустойчивого кодирования и возможности перезагрузки файлов в работоспособную часть памяти.

## СПИСОК ЛИТЕРАТУРЫ

1 Черкесов Г.Н., Виноградов А.А. Отказобезопасность как важное свойство ответственных технических систем. // XII Санкт-Петербургская Международная конференция «Региональная информатика («РИ-2010») . Труды конференции. СПб, 2010.

2 Черкесов Г.Н. Об одном способе обоснования решений о продлении сроков эксплуатации резервированной системы. – М. Надежность, 2002, №1, с.33 – 43.

**Чистяков И.В., Орлов Д.Р.**
**Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»**

## МЕТОДЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ НА УСТРОЙСТВАХ ХРАНЕНИЯ

Современный подход к разработке безопасных информационных технологий требует обеспечения безопасности информации не только при ее передаче по каналам и сетям связи, но и при хранении на запоминающих устройствах различного типа.

Устройства хранения как среда безопасности имеют ряд особенностей, в том числе:

– длительный срок хранения информации с возможностью ее частичной модификации;

– возможность произвольного доступа к записям;

– отсутствие on-line взаимодействия между субъектами при работе с разделяемыми ресурсами,

– способ организации хранения

и ряд других, которые должны быть учтены при разработке системы криптографической защиты. При этом необходимо минимизировать увеличения времени доступа и требуемый объем дополнительной памяти.

Основными сервисами, обеспечиваемыми криптографическими механизмами для устройств хранения, являются:

– конфиденциальность,

– контроль целостности,

– защита от навязывания устаревших (неактуальных) версий,

– криптографическое разграничение доступа к совместно используемым ресурсам.

Механизмы и сервисы безопасности хранения могут быть размещены на разных уровнях стека протоколов: на уровне записи или на более высоком уровне, например, на уровне файловой системы.

Конфиденциальность обеспечивается путем шифрования.

Размещение шифрования на уровне записи обеспечивает максимальную «прозрачность» для приложений (файловая система, база данных и другие). Наиболее подходящим для этого уровня представляется режим шифрования для блок-ориентированных устройств хранения [1], адаптированный к стандарту шифрования РФ. Указанный режим обладает следующими свойствами:

– длина шифртекста равна длине открытого текста;

– не требует хранения дополнительной информации;

– каждый блок шифруется независимо;

– преобразование шифрования зависит от положения шифртекста на устройстве хранения (от номера сектора и номера блока в секторе);

– изменение любого бита открытого текста «рандомизирует» соответствующий блок шифртекста.

Для контроля целостности записи, учитывая свойства режима шифрования [1], можно использовать функцию хэширования или некриптографическую контрольную сумму.

Для контроля целостности объектов с произвольным доступом к записям целесообразно использовать функцию хэширования с древовидной структурой.

При реализации криптографического разграничения доступа к защищенным разделяемым ресурсам возникает проблема хранения и распространения большого число криптографических ключей.

Сложность данной проблемы может быть уменьшена, если полномочия субъектов могут быть представлены как иерархическая структура.

Тогда множество субъектов разбивается на непересекающиеся классы безопасности, отличающиеся полномочиями по доступу к ресурсам. При этом подчиненные могут иметь более одного начальника. Упорядоченные таким образом классы безопасности можно рассматривать как частично упорядоченное множество.

Каждому классу безопасности назначается свой ключ для шифрования принадлежащих ему файлов. Пользователи старших классов должны иметь возможность доступа к информационным ресурсам всех своих подчиненных.

Для доступа к файлам подчиненных классов субъект должен иметь ключи всех подчиненных классов или, с целью сокращения число хранимых ключей, должен уметь

строить (выводить) ключи этих классов. При этом субъекты подчиненных классов не должны иметь возможность вывести ключ старших классов безопасности.

Поэтому основой криптографического разграничения доступа в иерархических системах является схема назначения и вывода ключей (СНВК) [2].

Математическая модель СНВК включает две основные процедуры.

1. Процедура назначения реквизитов доступа (выполняется центром назначения реквизитов доступа).

2. Процедура вывода реквизитов доступа (выполняется субъектом при доступе к информации субъекта подчиненного класса безопасности).

Этот же механизм может быть использован при уменьшении пиковых нагрузок при смене криптографических ключей.

Проблема заключается в том, что при смене ключа шифрования необходимо перешифровать все информационные ресурсы, зашифрованные на этом ключе. Перешифрование может быть растянуто во времени, если положить, что информационный ресурс перешифровывается только при его модификации [3].

Тогда авторизованный субъект при чтении, модификации и записи информации должен иметь два ключа: сменяемый ключ расшифрования и новый ключ засшифрования.

Однако при использовании механизма СНВК субъекту достаточно обладать только одним новым ключом зашифрования, а ключ расшифрования может быть получен с помощью процедура вывода реквизитов доступа.

Для защиты от навязывания неактуальных версий файла используется механизм нумерации версий. Однако в больших многопользовательских системах использование данного подхода встречает трудности, обусловленные необходимостью организации отдельного нумератора версий для каждого файла и on-line взаимодействия между субъектами.

Для преодоления этого в [4] предложено использовать один централизованный защищенный монотонный счетчик, на базе которого строятся виртуальные нумераторы версий. Однако так организованные нумераторы являются возрастающими, но недетерминированными.

Поэтому для проверки версии файла необходим специальный журнал, в котором фиксируются номера версий всех файлов в порядке их получения. Данный журнал ведется в незащищенной области, а его записи заверены цифровой подписью увязаны между собой.

При контроле версии файла по указанному журналу проверяется, что данный номер версии является последним для данного файла. При этом не требуется on-line взаимодействия между пользователями

Таким образом, применение криптографических методов для защиты информации на устройствах хранения требует адаптации известных протоколов.

СПИСОК ЛИТЕРАТУРЫ

1. IEEE P 1619 Standart for cryptographic protection of data on block-oriented storage devices.

2. Crampton d P. On key assignment for hierarchical access control // IEEE Computer Security Foundations Workshop (CSFW'06), 2006.

3. Fu K, Kamara S., and Kohno T. Key regression: Enabling efficient key distirbution for secure distributed storage. // ISOC Network and Distributed System Security Symposium (NDSS 2006), 2006.

4. van Dijk and al. Offline untrusted storage with immidiate detection of forking and replay attacks // STC 2007.

**Штогрин И.Р.**
**Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»**

## ОБЕСПЕЧЕНИЕ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ ИНФОРМАЦИИ НА ЭТАПЕ СТЕНДОВОЙ ОТРАБОТКИ ИЗДЕЛИЙ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ СИСТЕМ

Обеспечение безопасности информации в критических информационно-управляющих системах имеет главенствующие значение для их устойчивости к разного рода воздействиям.

На этапе разработки и отработки изделий и систем в целом, процесс обеспечения безопасности информации включает:

– определение требований по безопасности информации и выработку технических решений по порядку их реализации;

– реализацию требований по безопасности информации в конструкторской документации и технологиях проектирования;

– обеспечение требований нормативно-технической документации по безопасности при отработке и испытаниях;

– подтверждение реализации заданных требований по безопасности в процессе испытаний изделий и систем в целом.

В данной статье рассматриваются принимаемые меры по обеспечению безопасности информации на этапе отработки изделий на комплексных стендах «ФГУП НПО «Импульс».

Комплексный стенд представляет собой совокупность технических средств (технологическое оборудование) для настройки составных частей изделия и обеспечения их совместной отработки, разработки и отработки программного обеспечения, отработки алгоритмов функционирования изделия и взаимодействия со смежными системами, испытаний изделий.

Таким образом, привлекаемое для настройки и отработки изделия технологическое оборудование напрямую влияет на уровень создаваемой в изделии системы безопасности информации, и в то же время может при определенных условиях стать источником угрозы для нее.

Алгоритм отработки изделия (рис.1, 2) предполагает, что на начальных этапах комплексной отработки изделий технические решения по обеспечению безопасности информации в большинстве не внедрены, или не проведена оценка их эффективности, т.е изделия не защищены собственной системой безопасности информации от вторжения извне, в т.ч. посредством технологического оборудования.

Поэтому на данных этапах защиту информации в изделиях возможно обеспечить в основном только мерами, предусмотренными в нормативно-технической документации, ограничивающими доступ к информации, и обеспечивающими сохранение информации и которые подразделены на технические и организационные.

Среди основных технических и организационных мер защиты информации на этапе стендовой отработки необходимо отметить:

– размещение объектов и технологического оборудования для разработки в экранированном помещении, обеспечивающем защиту от утечек информации, в том числе по цепям электроснабжения, телефонным линиям связи и местным компьютерным сетям;

– применение технологической аппаратуры (ПЭВМ), прошедшей соответствующие проверки и имеющей предписание на эксплуатацию, исключение использования съемных носителей информации;

– применение в технологической аппаратуре (ПЭВМ) в т.ч. при разработке ПО сертифицированного ПО;

– исключение прямого выхода соединения локальной компьютерной сети с внешними сетями;

– ограничение и контроль допуска сотрудников в помещения с использованием автоматизированной системы контроля допуска и системы видеонаблюдения;

– многоуровневый контроль за перемещением и хранением всех видов носителей информации.

Обеспечение реализации указанных мер на практике осуществляется соответствующим графиком проверки уровня экранирования помещений, периодическим обновлением списков допущенных, совершенствованием системы допуска и документирования посещения.

Многолетний опыт по созданию информационно управляющих систем для обеспечения управления в критических условиях подтверждает, что применение и выполнение выше указанных в докладе мер позволяет обеспечить выполнение всех требований по обеспечению безопасности информации на этапе стендовой отработки.

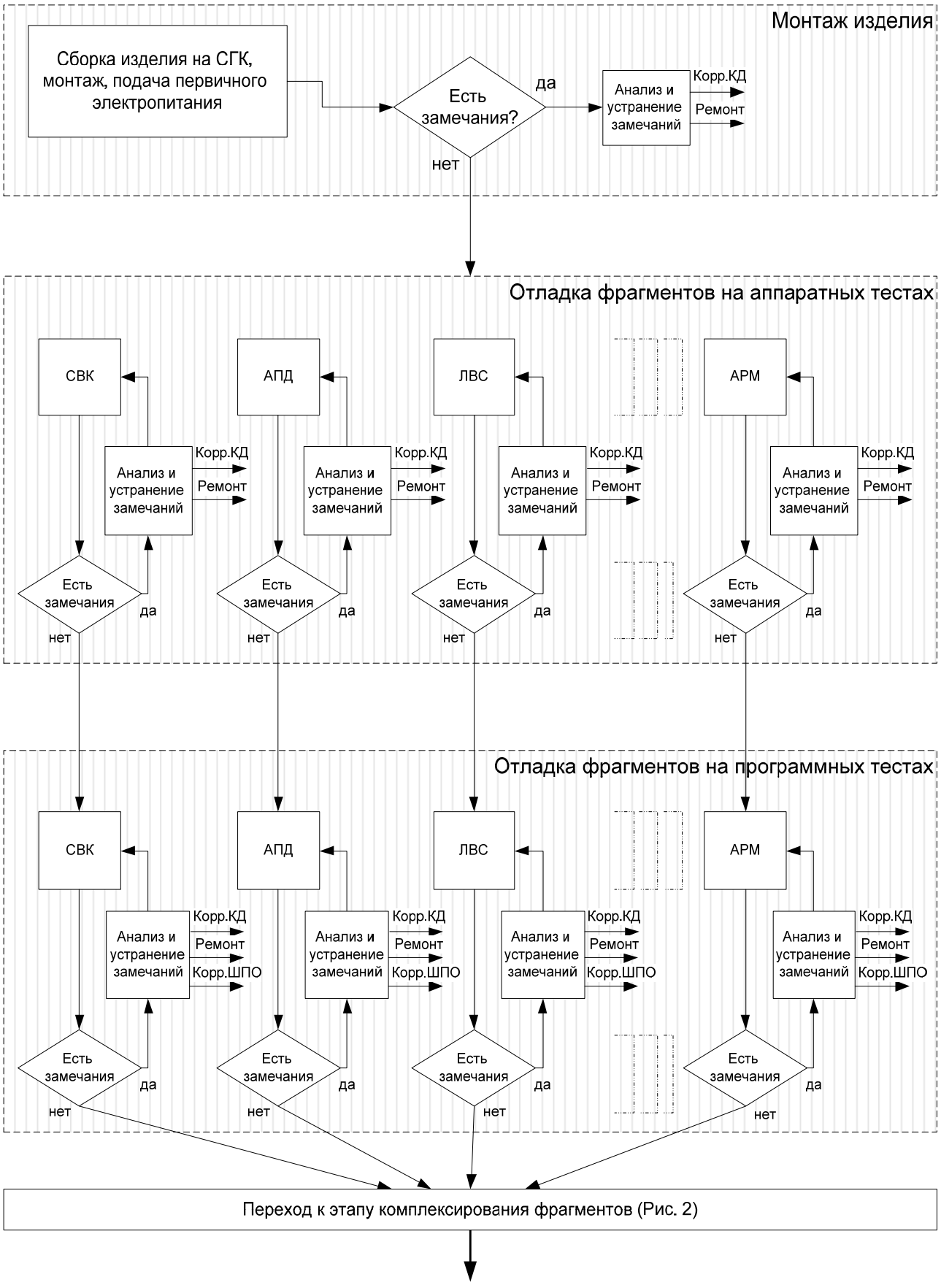



Рис.2

Рис.1. Начало алгоритма комплексной отладки изделия на СГК

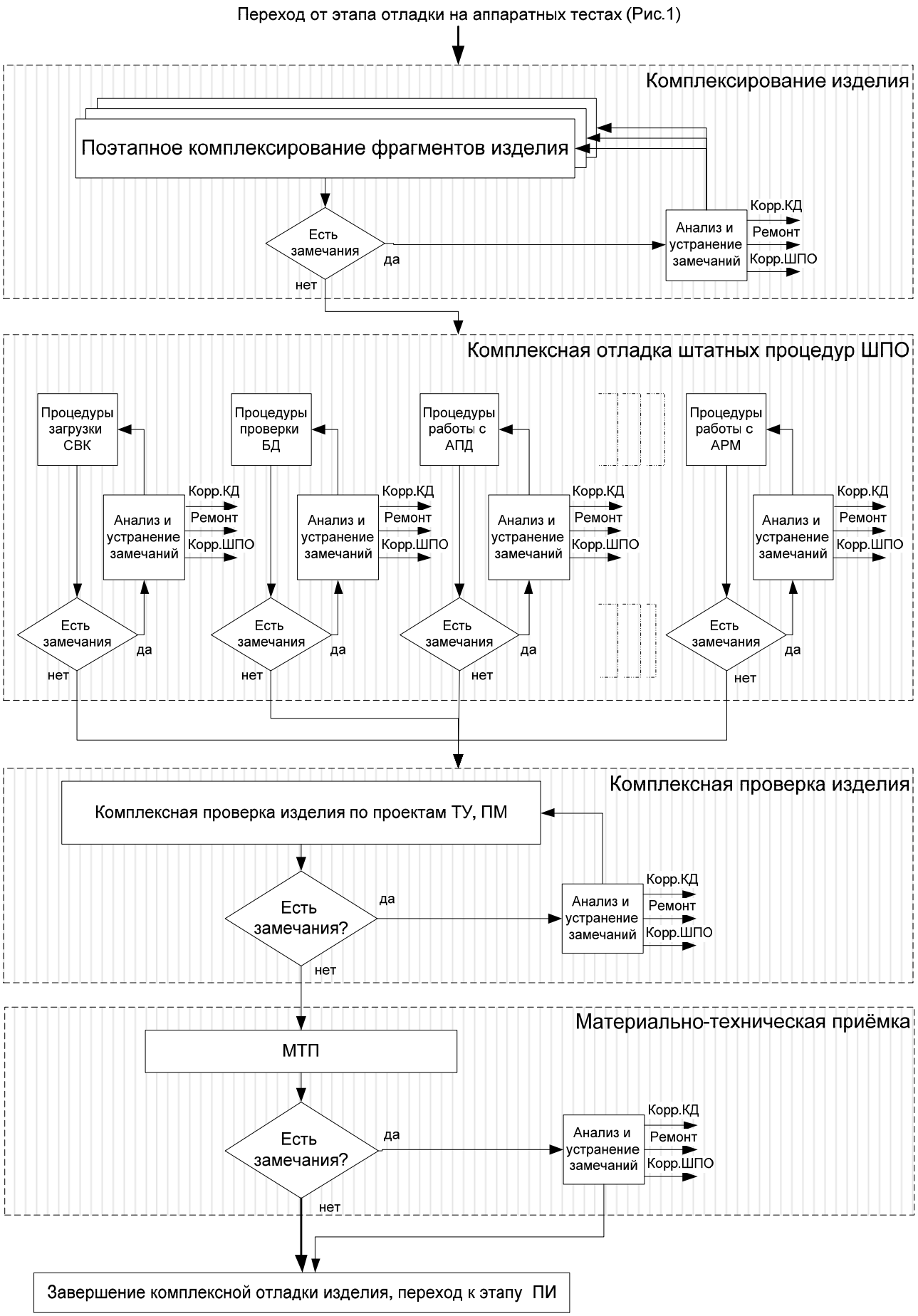



Рис.2. Окончание алгоритма комплексной отладки изделия на СГК

**Щёткин И.Е.**
**Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс», Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова**

## ИНВЕСТИЦИОННО-ИННОВАЦИОННАЯ ДЕЯТЕЛЬНОСТЬ ПРЕДПРИЯТИЯ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ В ЦЕЛЯХ ПОВЫШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Исторически сложившаяся система генерации и обмена информацией во внутренней и внешней средах предприятий оборонного комплекса позволила сформировать основные принципы и методы защиты информационных ресурсов. С появлением и широким применением вычислительной техники резко увеличились объемы информации и методы ее передачи, хранения, доступа. Изменились и требования к защите информационных ресурсов и методологический подход к организации информационный безопасности предприятия.

Вопрос обеспечения информационной безопасности остается актуальным и сложным аспектом реализации бизнес идеи предприятий. Технологии передачи информационных ресурсов современного мира постоянно совершенствуются и находятся в конкурентной борьбе, в связи с этим растет сложность осуществления необходимой защищенности информационной среды.

Универсальных методов защиты не существует, все зависит от индивидуальных особенностей рассматриваемой системы, а учет всех особенностей трудно подогнать под какую либо формализацию. Поэтому информационная безопасность чаще всего рассматривается как совокупность неформальных рекомендаций по построению систем защиты информации в той или иной системе с ее конкретными особенностями.

Глобальность вопроса защиты информации и информационная безопасность как предмет анализа и принятия решений за счет наличия универсальных принципов своего построения превратилось в отдельное направление, которое подвергается самому тщательному анализу в современном быстроразвивающемся и постоянно изменяющемся мире.

Для предприятий России из сферы оборонно-промышленного комплекса (ОПК) информационная безопасность является обязательным аспектом деятельности. Уже работают механизмы, который и сегодня позволяют обеспечивать необходимый уровень защиты государственной и коммерческой тайны, но внедрение современных автоматизированных систем создает необходимость дополнительно развивать структуру и основные подходы и методы.

Информационные потоки, которые создают конкурентоспособность предприятия на рынке товаров и услуг, задают новые требования и предпосылки модернизационных и инновационных внедрений в уже сложившиеся системы. Инновационные подходы в производстве, создании единых информационных пространств, внедрение безбумажного документооборота формируют задания к осуществлению безопасности особенно в критической инфраструктуре, где несанкционированное использование информационных ресурсов может привести к необратимым последствиям, как для предприятия, так и для всей страны.

Основой новых решений становятся автоматизированные системы (АС). Автоматизированные системы обработки информации являются конкурентным преимуществом каждой компании их индивидуальность, защищенность, адаптивность позволяют выходить на рынок быстрее, а продукция становится более качественной, репутация предприятия и спрос на товар повышается.

Под элементами автоматизированных систем следует понимать: средства вычислительной техники, программное обеспечение, каналы связи, информация на различных носителях, пользователи системы, серверные реализации обмена и хранения информации.

Анализ нормативной документации и опыта работы структур по защите информации показывает: основные принципы информационной безопасности заключаются в том, что система способна противостоять дестабилизирующему воздействию как внешней, так и внутренней среды и функционирование системы не создает угроз для внутренней и внешней среды, а направления обеспечения защиты информации сводятся к разделению всех угроз по пунктам общей классификации, которым соответствуют определенные методы и средства.

Методы обеспечения информационной безопасности достаточно разнообразны, но классификация в общем виде может быть представлена, как показано на рисунке 1.

Классификация показывает достаточно широкий спектр задач и возможных путей решения проблем защиты, а индивидуальность каждой реальной ситуации и задачи задает широкое поле для получения результатов и внедрения новых методов и средств.

В связи с большим вниманием к этой теме и необходимостью совершенствования с целью осуществления безопасности и конкурентоспособности, как отдельного предприятия, так и государства в целом необходимым условием развития является инвестирование в инфраструктуру информационной защиты и обучение людей современным методам и технологиям.

Развитие инвестиционно-инновационной среды для реализации новых проектов и модернизации уже существующей структуры с учетом ширины спектра возможных методов и большого числа современных решений по обмену и хранению информационных ресурсов заключается в наработки и использованию законодательных, нормативных и регламентирующих документов, созданию технических средств и методов защиты, которые позволяют получать конечный продукт удовлетворяющий потребностям заказчика и находящийся в рамках регламентирующих ограничений. При реализации данных задач при формировании инновационных продуктов внедрения необходимо учитывать фактор быстроменяющейся информационной среды.

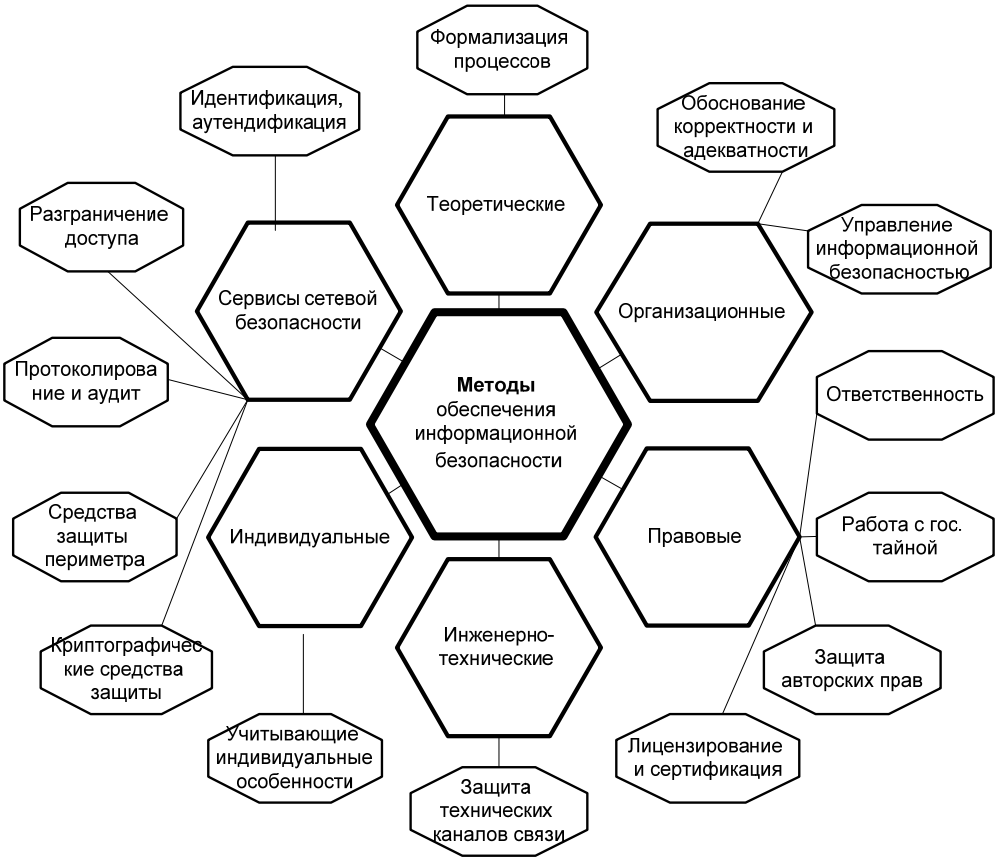



Рис.1. Методы и средства обеспечения защиты информации

Совершенствование методов инвестиционно-инновационной деятельности предприятия в части информационной безопасности – это затратная, сложная, но необходимая мера поддержания конкурентоспособности. С одной стороны недофинансирование данного направления может привести к отсталости методов и необеспеченности персонала для осуществления работ, с другой стороны каждая организация ограничена финансовыми и трудовыми ресурсами, а высокая рискованность осуществления проектов в данной сфере является ключевым фактором при принятии решений по инновационным разработкам. Одной из основных особенностей является скорость изменения и внедрения инноваций в сферу по всему миру, что делает обязательным учет тенденций и необходимость мониторинга и постоянное проведение обучения по данному направлению.

Инвестиционно-инновационная деятельность предприятия в целях повышения уровня информационной безопасности в критических инфраструктурах заключается в поиске новых решений и оптимизации уже существующих на рынке или собственных разработок, проведение научно-исследовательских и опытно-конструкторских работ, выход на рынок с новым товаром, преодоление конкурентных барьеров, создание систем для собственного применения немеющих аналогов и обеспечивающих защиту информации и синтеза выгодных подходов к финансированию проектов за счет привлечения инвестиций разного вида. Данный вид деятельности является связующим звеном инноваций и источников их финансирования. Инвестиционные проекты в сферу новых технологий и производств, генерацию нового знания являются высокорискованными капиталовложениями. Данный вид инвестирования относится к венчурному и основным его признаком считается высокий риск и неопределенность конечного результата.

Внедрение новых и перспективных систем защиты являются одним из основных движущих рычагов дальнейшего развития сферы информационной безопасности. В данной сфере инновации являются залогом успеха выхода на рынок. Для осуществления данных целей необходимо для каждого предприятия рассмотреть и учесть ряд факторов, предопределяющих судьбу нововведений.

Среди основных факторов необходимо учитывать:

– необходим выход на рынок или нет;

– существует персонал способный взяться за данный вид деятельности;

– соответствие инновациям предприятия, восприимчивость предприятия к инновациям;

– экономически обоснованную систему отбора инновационных идей и проектов;

– эффективные методы управления инновационными проектами и контроль за их реализацией;

– индивидуальную и коллективную ответственность за реализацию проектов в данной сфере.

Формирование инвестиционных потоков и пунктов инвестиционного плана развития необходимо начинать с установления основных критериев в соответствии с деятельностью предприятия по инновационному менеджменту. Инновационный менеджмент – это область управленческих решений, связанная с реализацией инновационных решений и сфера сопряжения с другими отраслями менеджмента. Для осуществления инновационного менеджмента на уже функционирующем предприятии необходимо иметь платформу (задел) на котором можно строить новое направление. К такому заделу относится совокупный процесс функционирования предприятия в отрасли, а именно его позиции и наработки по планированию, организации работ, контролю, мотивации работников. Анализ данной платформы позволяет сделать вывод о какого рода инновациям может идти речь при построении инновационного менеджмента предприятия. Следующим этапом в построении идет уже процесс совершенствования инвестиционно-инновационной среды.

При реализации инновационных проектов необходимо опираться на основные принципы инновационного менеджмента:

– инновации являются решающим условием выживания предприятия на рынке товаров и услуг;

– ресурсы на НИР и ОКР оправданы лишь в той мере, в которой они приводят к поставленным результатам;

– успех инновации в постоянном мониторинге и анализе мира инноваций и совершенствование методов и схем их инвестирования.

Инвестиционная деятельность предприятия является неотъемлемой составляющей продвижения инновационных решений. Далеко не каждая идея и решение может получить реализацию даже при высоких показателях эффективности проектов и большинство таких решений требуют от предприятий привлечения капитала со стороны, когда собственные средства не могут покрыть рисованные шаги. Именно поэтому тесное взаимодействие инвестиционной и инновационной деятельности предприятия позволяет выводить идею на поверхность.

Параллельно с зарождением инновационной идеи встает вопрос поиска и формирования плана по источникам финансирования. Он соответствует этапам жизненного цикла инновационных решений. Проработка множества возможных источников позволяет сделать

вывод о наличии основных базовых, к которым могут быть сведены большинство из возможных. Анализ источников финансирования инноваций для ОПК можно представить в виде таблицы 1.

Таблица 1

Источники финансирования этапов инновационного процесса

| № | Название | Проводимая работа | Финансирование |
|---|---|---|---|
| 1 | Поисковые НИР | Выдвижение научно-технических идей, проведение экспериментов | Государственные программы, и государственные субсидии |
| 2 | Прикладные НИР | Проведение прикладные работ по выбранному направлению | Государственное целевое финансирование (для государственных научно-технических программ на конкурсной основе), промышленные предприятия, венчурные фирмы, «бизнес-ангелы» |
| 3 | Опытно-конструкторские и проектно-конструкторские работы (ОКР и ПКР) | Разработка аванпроектов, эскизно-технических проектов, РКД, изготовление и испытание образцов | Источники финансирования прикладных НИР и собственные средства предприятия |
| 4 | Коммерциализация нововведения | Запуск производства, выход на рынок и далее по жизненному циклу товара | Необходимость большого потока инвестиций для производственных мощностей. Венчурное инвестирование, в связи с рискованностью инновации на рынке |

Определение этапов инновационного менеджмента и вида инвестирования позволяют сделать анализ и уделить внимание каждому пункту плана финансирования. Основное поступление средств на первых этапах инвестиционных вложений направляется в рамках государственных программ и венчурных компаний. Каждый из двух источников требует тщательной предварительной проработки. Инвестор в каждом из этих случаев анализирует показатели компании перспективность проектов при переходе на конечном этапе к финансированию из собственных средств предприятия. Венчурное финансирование инноваций опирается на авторитет фирмы и прибыльность итогового результата с учетом высоких рисков данного вида вложения средств.

Одной из основных особенностей вложения инвестиций в сферу обеспечения безопасности информации заключается в том, что получаемый результат формируется как взаимосвязанный технический и интеллектуальный продукт и для него вступают в силу законы поведения участника рынка интеллектуальной сферы. А в современных условиях конкурентной борьбы вторая отличительная особенность сферы информационной безопасности заключается в высоком риске. Именно поэтому данный вид инвестирования осваивают венчурные фирмы, которые специализируются непосредственно на данном виде инвестиционных проектов, особенно на первоначальном уровне.

Применительно к сфере информационной безопасности в критической инфраструктуре основные элементы подхода сохраняются, но специфичность деятельности и ее особая важность ставит новые обязательные задачи для выполнения и учета в реализации. Специфичность данной сферы заключается в значительных последствиях неправильной реализации проектов. Несанкционированный доступ к информационным ресурсам атомной, оборонной и других видов деятельности государства может привести к большим жертвам среди населения и разворачиванием военных действий, экономической блокадой государства. Поэтому сложная задача осуществления информационной безопасности получает еще значительную прибавку ответственности и становится еще более сложной для осуществления, но государство не в силах уйти от этого – эта важная и необходимая задача, как на отдельном предприятии, так и на уровне государства в целом.

Финансирование работ по этапам реализации проекта распределяется неравномерно, так финансирование работ связанных с освоением масштабного производства нового продукта и последующем совершенствованием технологии в 6-8 раз больше, чем расходы

на исследования и разработки, а на этот период реализации проекта основными источниками инвестиций на предприятиях являются собственные средства, аккумулируемые на специальных фондах и заемные средства, в основном банковские кредиты. Проработка детального плана, компьютерное моделирование, просчет основных рисков и финансовых потоков являются конкурентным преимуществом и современным обязательным средством для достижения результата.

Оценка результатов инновационной деятельности предприятия в рамках осуществления информационной безопасности и просчет рисков может производиться путем сравнения показателей факторного анализа, индексного метода, SWOT-анализа, функционально-стоимостного анализа и других видов информации по результатам деятельности предприятия за рассматриваемый период. Сравнительный анализ позволяет определить отклонение от плановых показателей, выявить резервы, установить причины отклонений. Особенности сравниваемых методов в таблице 2.

Таблица 2

Система методов подлежащих сравнительному анализу

| № | Название | Описание |
|---|---|---|
| 1 | Факторный анализ | Установление влияния факторов на функцию (производительность труда, полезный эффект изделия и др.) |
| 2 | Индексный метод | При невозможности измерения отдельных элементов используются относительные показатели для оценки плановых, а также определение динамики процессов, выявление относительных и абсолютных отклонений. |
| 3 | SWOT-анализ | Комплексная процедура стратегического анализа окружающей среды и ресурсного потенциала предприятия указывая сильные, слабые стороны и угрозы. |
| 4 | Функционально-стоимостной анализ | Учет степени значимости выполняемых изделием функций с целью повышения полезного эффекта на единицу затрат |

Системный подход к информационной безопасности предприятия заключается в обобщении и классификации множества факторов, ресурсов и методов в целях унификации способов защиты, постоянное отслеживание современных инновационных методов для оперативного реагирования и коррекции (модернизации) существующих алгоритмов и решений, сформированных на базе прошлого опыта. Регулярное планирование источников финансирования и формирования инвестиционных потоков в сферу, применение АС и программных продуктов для обработки информации и просчета инвестиционных проектов, что стало обязательным условием конкурентоспособности на рынке инновационных решений при условиях венчурного инвестирования. Изложенные подходы должны учитывать особенности венчурного инвестирования в критическую инфраструктуру, где в большинстве случаев невозможно использовать иностранный капитал и привлекать частные инвестиции, а основные условия формирует государство как заказчик проектов. В тоже время появление патентов и закрепление авторских прав за разработками позволяет рассчитывать на долгосрочное финансирование новых проектов в данной сфере.

Инвестирование инновационных проектов в области информационной безопасности и защиты информационных ресурсов предприятий является приоритетной и актуальной задачей для государства и руководителей предприятий. Огромное значение информационной безопасности обусловлено ее прямым влиянием на конкурентоспособность фирм и безопасность государства. При оптимизации процесса финансирования и построения плана с учетом рисков, а также своевременных управленческих решений данная сфера деятельности способна не только обеспечивать безопасность информационного обмена, но и являться источником получения прибыли для предприятия на рынке технических и интеллектуальных услуг.

СПИСОК ЛИТЕРАТУРЫ

1. Гурунян Т.В. Управление инвестиционно-инновационной деятельностью. – СибАГС, 2010.
2. Девянин П.Н. Теоретические основы компьютерной безопасности. – М.: Радио и связь, 2000.
3. Корт С.С. Теоретические основы защиты информации. – М.: Гелиос АРВ, 2004.
4. Цирлов В.Л. Основы информационной безопасности. – Ростов н/Д: Феникс, 2008.

# ОГЛАВЛЕНИЕ