Воронежский институт МВД России

МОДЕЛИ И МЕТОДЫ ФОРМИРОВАНИЯ КОМПЛЕКСОВ СРЕДСТВ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕТЯХ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Монография

Воронеж
2020

ББК 32.973
М-74
УДК 002.001;002:001.8

Коллектив авторов: Н. С. Хохлов, доктор технических наук, профессор; О. И. Бокова, доктор технических наук, профессор; С. В. Канавин, кандидат технических наук; И. В. Гилев.

Рецензенты: заместитель начальника тыла ГУ МВД России по Воронежской области – начальник ЦИТСиЗИ полковник внутренней службы И. А. Домнин; начальник управления ГИБДД ГУ МВД России по Воронежской области кандидат технических наук полковник полиции Е. В. Шаталов; начальник кафедры информационной безопасности, кандидат технических наук полковник полиции О. И. Нестеровский.

Модели и методы формирования комплексов средств противодействия угрозам информационной безопасности в сетях связи специ-
М-74 ального назначения : монография / Н. С. Хохлов, О. И. Бокова, С. В. Канавин, И. В. Гилев ; под редакцией доктора технических наук, проф. Н. С. Хохлова. – Воронеж : Воронежский институт МВД России, 2020. – 175 с.

ISBN 978-5-88591-800-8

В монографии изложены проблемы анализа и синтеза формирования комплекса средств противодействия угрозам информационной безопасности в сетях связи специального назначения. Рассматриваются модели и способы функционирования сетей связи специального назначения в условиях информационного конфликта. С позиций системного подхода анализируется современная постановка проблемы, концептуальные основы синтеза комплекса средств противодействия угрозам информационной безопасности в сетях связи специального назначения с учетом специфики противоправных действий в данной сфере, приводятся принципы построения методик, методов и моделей для оценки функционирования такого рода систем защиты.

Предназначена для курсантов и слушателей, обучающихся по специальности 11.05.04 Инфокоммуникационные технологии и системы специальной связи, адъюнктов, обучающихся по направлению подготовки 11.07.01 Электроника, радиотехника и системы связи, профессорско-преподавательского состава образовательных организаций системы МВД России, сотрудников территориальных органов внутренних дел.

М $\frac{2302020000-35}{221-20}$ 49(II) – 20

ББК 32.973
УДК 002.001;002:001.8

ISBN 978-5-88591-800-8

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Национальная безопасность Российской Федерации в эпоху всеобщей цифровизации существенным образом зависит от обеспечения информационной безопасности. С ростом технического прогресса эта взаимосвязь будет прослеживаться все сильнее. Обеспечение информационной безопасности от внутренних и внешних угроз, связанных с применением информационных технологий в военно-политических целях, противоречащих международному праву, в том числе осуществлением враждебных действий и актов агрессии, является одной из важнейших государственных задач. Потребности общества определяют быстрый рост информационного обмена, осуществляемого устно и с помощью систем инфокоммуникаций, при этом постоянно растет не только количество, но и ценность передаваемой информации. Одновременно увеличивается и опасность серьезного ущерба в случае нарушения безопасности информации, что определяет актуальность решения задач противодействия угрозам информационной безопасности. В Доктрине информационной безопасности Российской Федерации отмечено, что мероприятия по обеспечению безопасности информационной инфраструктуры, включая ее целостность, доступность и устойчивое функционирование, с использованием отечественных информационных технологий должны формироваться на комплексной основе.

В настоящее время сети связи специального назначения (СССН) получили большое распространение в органах государственной власти, органах, осуществляющих функции обороны страны, безопасности государства и обеспечения правопорядка [1]. В связи с особенностями функционирования инфокоммуникационных систем и сетей связи специального назначения необходимо учитывать, что они развернуты и обеспечивают управление и взаимодействие в рамках существующих ведомственных и межведомственных систем связи. В монографии под СССН понимают специализированную защищенную инфокоммуникационную сеть и систему управления ею. В литературе встречается термин «инфокоммуникационная система и сеть» специального назначения [2]. Можно сказать, что сама телекоммуникационная сеть превращается в совокупность защищенных сетей обмена данными, техническую основу которых составляют защищенные линии связи и специализированные средства, управляющие обработкой информации.

Главным условием создания комплекса средств противодействия угрозам информационной безопасности СССН является его надежность. Но надежность может быть обеспечена лишь в том случае, если защита является комплексной и системной. Исходя из сказанного, можно дать такое определение: Комплекс средств противодействия угрозам информационной безопасности СССН – это организованная совокупность органов и объектов (компонентов) защиты информации, использование методов и

средств защиты, а также осуществление защитных мероприятий. Для формирования требований к комплексам средств противодействия угрозам информационной безопасности в сетях связи специального назначения необходимо полагаться на современную нормативную правовую базу: международные стандарты в области информационной безопасности, отраслевые стандарты Российской Федерации (ГОСТ Р 53113.1-2008 «Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов», ГОСТ ИСО/МЭК-Р 15408-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки информационной безопасности информационных технологий»), руководящие документы ФСТЭК России, а также ведомственные нормативные акты.

Развитие сетей связи специального назначения связано с использованием в них ресурсов сетей связи общего пользования, интеграцией различного рода трафика (речь, видео, данные), применением новых сетевых технологий (концепция NGN, пакетные технологии передачи, использование технологий виртуализации, самоорганизации и др.). Новые функциональные возможности NGN в сравнении с традиционными сетями создают новые угрозы информационной безопасности или открывают широкие возможности к реализации известных угроз. Данные факторы требуют комплексного решения проблемы на основе разработки соответствующих политик и методов защиты информации, а также построения системы обеспечения информационной безопасности [19].

Вместе с неоспоримыми преимуществами применения этих новых технологий в современных сетях связи специального назначения возникают и новые угрозы информационной безопасности. Наиболее характерным отрицательным фактором выступают повышение уровня подготовки современной организованной преступности, рост профессионализма и дальнейшее совершенствование ее технической оснащенности, базирующиеся на новейших достижениях научно-технического прогресса. Особого внимания заслуживают вопросы противодействия угрозам информационной безопасности в области применения робототехнических комплексов (систем), в том числе беспилотных летательных аппаратов.

Очевидно, что задача противодействия угрозам информационной безопасности в СССН носит стратегический характер. В этом аспекте можно отметить работы [3–5], в которых рассматриваются вопросы противодействия угрозам информационной безопасности с позиции комплексного подхода. В трудах исследователей не в полной мере раскрыто существо проблемы, что дало предпосылку для проведения дальнейших исследований.

Монография посвящена проблеме формирования комплекса средств противодействия угрозам информационной безопасности в сетях связи специального назначения. Приведено описание подобных комплексов, рас-

смотрены ситуации и основания для их применения. Обращается внимание на выявление общих технологических особенностей формирования комплекса средств противодействия угрозам информационной безопасности в сетях связи специального назначения. Авторами проведено моделирование функционирования комплекса противодействия на основе аппарата лингвистических переменных и нечетких экспертных систем. На основе полученных результатов могут быть предложены требования к формированию комплекса средств противодействия угрозам информационной безопасности в сетях связи специального назначения.

В основу монографии положены труды Н. С. Хохлова, О. И. Боковой, С. В. Канавина, В. С. Дунина и других ученых – представителей научной школы, функционирующей на кафедре инфокоммуникационных систем и технологий Воронежского института МВД России под руководством доктора технических наук, профессора, заслуженного работника высшей школы Российской Федерации Н. С. Хохлова.

В главе 1 (Н. С. Хохлов, С. В. Канавин) представлены методологические вопросы анализа и синтеза построения комплексов средств противодействия угрозам информационной безопасности в сетях связи специального назначения. Систематизирован материал по проблематике противодействия сетей связи специального назначения угрозам информационной безопасности.

Рассмотрены особенности функционирования базовой инфраструктуры сетей связи специального назначения, а также классификация информационных атак и методы их обнаружения.

Приведена модель угроз информационной безопасности сети связи специального назначения на основе формализованного построения угроз безопасности сети связи специального назначения с позиции теории множеств с учетом сложности, неоднозначности (нечеткости), неопределенности оценки событий информационной безопасности в условиях информационного противоборства. Математическая основа построения моделей процессов информационного противоборства трудно формализуема. Сама модель строится на основе использования интеллектуальных методов, учитывающих суждения специалистов и предоставляющих окончательный результат в виде простых операций над неопределенностью, неточностью и размытостью событий информационной безопасности (теория нечетких множеств, лингвистическая неопределенность, нечеткая логика).

Изложены принципы оптимального интегрирования разнородных информационных процессов в интересах противодействия угрозам информационной безопасности в сетях связи специального назначения

Разработан метод теории эффективности, декомпозиции и оптимизации показателей качества функционирования сетей связи специального назначения при условии защиты от разрушающих информационных воздействий

Предложена типовая модель сети связи специального назначения в условиях информационного конфликта на основе эталонной модели взаимодействия конфликтующих систем CSI (Conflict System Interconnection Reference Model). Она формализует объекты и общие подходы к описанию локальных информационных конфликтов в СССН на каждом из уровней OSI.

Предложены перспективные цифровые информационные технологии как техническая основа повышения эффективности и защищенности функционирования сетей связи специального назначения. Важным требованием к архитектуре информационной безопасности NGN является соблюдение логического и физического (определяемого маршрутизацией) разделения трафика пользователей, сигнализации, управления, а также обеспечения безопасности во всех плоскостях.

В главе 2 (О. И. Бокова, С. В. Канавин) приведены теоретические основы оптимального управления комплексом средств противодействия угрозам информационной безопасности в сетях связи специального назначения.

Авторами разработаны основные положения оптимального управления функционально ориентированными информационными процессами при обеспечении безопасности территориальных сегментов сети связи специального назначения. В условиях выбранного множества показателей эффективности СССН справедливы следующие утверждения:

Утверждение 1. Показатель своевременности обработки информации в СССН будет представлять собой монотонно убывающую в интервале [0, 1] функцию объема информационного пространства, реализующего процессы обработки накопления и выдачи данных.

Утверждение 2. Показатель защищенности СССН будет представлять собой монотонно убывающую в интервале [0, 1] функцию объемов информационного пространства, реализующих процессы обнаружения и парирования воздействий угроз информационной безопасности.

Метод оценки ресурса безопасности территориальных сегментов сети связи специального назначения базируется на методической основе определения оптимального информационного объема СССН, за счет которого реализуется обнаружение воздействий угроз информационной безопасности.

Реализацию ресурса безопасности территориальных сегментов системы связи специального назначения, основанную на методических подходах и алгоритмах выявления, оптимального распределения и идентификации временного ресурса СССН, а также оценки их влияния на ее эффективность, целесообразно решать на основе применения методов математического моделирования.

Авторами систематизирована информация о средствах противодействия угрозам информационной безопасности СССН и классифицированы стратегии их применения.

В главе 3 (С. В. Канавин, Н. С. Хохлов) разработана и обоснована методология моделирования комплекса средств противодействия угрозам информационной безопасности в условиях информационного конфликта

Разработанная методология моделирования комплекса средств противодействия угрозам информационной безопасности отличается применением внутрисистемных и внешних показателей эффективности функционирования и позволяет в итерационном режиме осуществлять оптимизацию эргатических систем предметного назначения.

При рассмотрении алгоритмов противодействия при воздействии сверхширокополосных помех на системы передачи видеоинформации получены следующие выводы. Решением для передачи видео и звука являются системы с модуляцией COFDM. Благодаря большому числу поднесущих частот в комбинации с помехоустойчивым кодированием возможно восстановление отдельных поднесущих, ослабленных вследствие частотно-селективных замираний в канале. При всех достоинствах рассматриваемых систем данный вид модуляции имеет существенные недостатки – большое отношение пиковой мощности сигнала к его усредненной мощности (пикфактор сигнала), а также эффект нарушения ортогональности поднесущих частот в нестационарных каналах связи с многолучевостью, приводящий к взаимным перекрестным помехам между поднесущими частотами. Информационные сигналы также очень чувствительны к системным нестабильностям, что в отдельных случаях может приводить к существенному росту внеполосных излучений. Помехи в радиоэфире от других радиоэлектронных средств на рабочем частотном канале приводят к искажениям изображения и звука. В этом случае необходимо сменить частотный канал, убедиться в отсутствии других радиоизлучающих средств, попадающих в полосу работы системы. Методика количественной оценки влияния радиопомех и сигнала радиоэлектронных средств на показатели радиоэлектронной защиты рассмотрена авторами в работах [84–86, 91–93].

Таким образом, в результате экспериментального исследования выявлено воздействие друг на друга радиосредств органов внутренних дел, работающих в одной полосе частот. Это наглядно показано в случае работы аналогового радиосредства в том же частотном диапазоне. Однако при использовании цифрового радиосредства, не входящего в состав комплекса, влияние на спектр также присутствует, но на передачу видеоданных это не оказывает существенного воздействия. Данные эксперимента показывают, что в случае возникновения селективных замираний и некорректной работы комплекса передачи видео и звука рекомендуется проводить работы по анализу спектра при настройке и монтаже систем связи специально-

го назначения с целью минимизации взаимного влияния радиооборудования.

Предложенный способ защиты информации в каналах связи методом формирования маскирующих сигналоподобных помех характеризуется простотой аппаратурной реализации. Недостатком метода является усложнение проблемы электромагнитной совместимости радиосредств. Эффективность получаемых мультипликативных маскирующих помех необходимо исследовать методами моделирования и экспериментальной проверки в лабораторных и натурных условиях применительно к различным видам модуляции полезных сигналов.

Разработана методика построения нейронной сети для выбора способов противодействия деструктивным электромагнитным воздействиям в системах связи специального назначения. Результаты моделирования показали, что наиболее эффективно задачу выбора способа противодействия деструктивным электромагнитным воздействиям решает нейронная сеть структуры многослойный перцептрон с тремя скрытыми нейронами. Были построены лифтовые карты, описывающие обучение сети на входных данных, определены весовые коэффициенты нейронной сети. Работоспособность сети протестирована на новых, не известных ранее ситуациях, и работа сети продемонстрировала осуществление выбора корректной меры противодействия деструктивным электромагнитным воздействиям. Программная реализация данной методики позволяет автоматизировать выбор способов противодействия деструктивным электромагнитным воздействиям с целью минимизации их негативного влияния на сети связи специального назначения.

В главе 4 (С. В. Канавин, Н. С. Хохлов, И. В. Гилев 4.6, 4.7, 4.8, 4.9.) рассмотрены методы и модели противодействия угрозам нарушения информационной безопасности в сетях связи специального назначения.

Предложена математическая модель комплекса средств противодействия угрозам информационной безопасности в СССН, основанная на применении лингвистических переменных и нечетких экспертных систем формирования комплекса средств противодействия угрозам информационной безопасности в сетях связи специального назначения, осуществлено исследование общих технологических особенностей формирования комплекса средств противодействия угрозам информационной безопасности в СССН. Авторами проведено моделирование функционирования комплекса средств противодействия на основе аппарата лингвистических переменных и нечетких экспертных систем. На основе полученных результатов могут быть предложены требования к формированию комплекса средств противодействия угрозам информационной безопасности в СССН. Математический аппарат, использованный в данном разделе, может в полной мере характеризовать зависимость эффективности средств противодействия от совокупности реализуемых средств защиты. В рамках комплексного подхода

возможно построение такого рода систем с применением элементов искусственного интеллекта, что будет рассмотрено авторским коллективом в дальнейших исследованиях.

Проводя общую классификацию, методы противодействия угрозам нарушения информационной безопасности в цифровых сетях связи специального назначения можно разделить на три группы: предотвращения, парирования и нейтрализации угроз.

Предложены технические решения детерминированного хаоса для защиты информации в каналах связи и управления. Одно из перспективных направлений применения динамического хаоса в системах связи и управления – это использование широкополосности хаотических режимов. Широкополосные сигналы могут быть использованы для борьбы с искажениями и затуханием сигнала в каналах распространения. Перспективным направлением является использование хаотических сигналов сложной формы для шифрации передаваемых сообщений. Ведутся разработки новых методов передачи информации с более высокими скоростями и более надежным восстановлением полезной информации, снижением влияния шумов и других возмущающих факторов. Все вышеперечисленное подчеркивает перспективность применения детерминированного хаоса в системах связи и управления.

Предложены принципы и технические решения оптимальной обработки сигналов на основе информационно-энтропийного критерия для защиты информации в каналах связи специального назначения. В данном разделе монографии изложено теоретическое обоснование нового метода формирования и обработки сигналов в каналах связи с зашумлением на основе применения вероятностной фильтрации.

Рассмотрен методический подход к оценке способа противодействия деструктивным электромагнитным воздействиям по критерию сигнал/шум. Было предложено использовать зависимость в качестве оценки эффективности противодействия деструктивным электромагнитным воздействиям, в соответствии с которой способ противодействия считается эффективным, частично эффективным или неэффективным.

Кроме того, рассмотрен методический подход к оценке способа противодействия деструктивным электромагнитным воздействиям по информационному критерию, предложен способ противодействия деструктивным электромагнитным воздействиям в сетях связи специального назначения, основанный на дополнительной модуляции с применением вейвлет-преобразования.

В главе 5 (С. В. Канавин, Н. С. Хохлов) представлена организация проведения оценки рисков нарушения информационной безопасности в информационных, телекоммуникационных системах ОВД, которая позволяет получать обоснованные оценки рисков, уязвимостей, эффективности защиты. Для оценки эффективности разработанной системы была прове-

дена оценка безопасности для информационных, телекоммуникационных систем ОВД. В результате было подтверждено соответствие между реальной безопасностью информационной системы и назначенными оценками.

Использование алгоритма Мамдани для управления динамическими объектами позволяет исследовать риски нарушения информационной безопасности в самоорганизующихся сетях и дальнейшее управление ими. Полученная геометрическая поверхность быстро реагирует на изменение в изучаемой динамической системе и заданные новые выходные данные, это происходит из-за того, что геометрическая поверхность строится на основе нечеткой базы знаний, опираясь на информацию, полученную от исследуемой системы, что позволяет оперативно оценить полезность от введённой системы контрмер.

Глава 1.
МЕТОДОЛОГИЧЕСКИЕ ВОПРОСЫ АНАЛИЗА И СИНТЕЗА ПОСТРОЕНИЯ КОМПЛЕКСОВ СРЕДСТВ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕТЯХ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

1.1. Проблематика противодействия угрозам информационной безопасности в сетях связи специального назначения

Комплекс средств противодействия угрозам информационной безопасности в сетях связи специального назначения представляет собой сложную многофункциональную систему безопасности, состоящую из множества необходимых подсистем функционирования, объединенных единой интегрированной мультисервисной транспортной средой. Некоторые подсистемы могут отличаться своей внутренней инфраструктурой, наличием собственных систем управления базами данных, интеллектуальными средствами поддержки и принятия решений. Многие из таких комплексов являются самостоятельными информационными системами, доступ к которым осуществляется посредством удаленного подключения субъектов (пользователей или процессов подсистем обеспечения безопасности) к выделенным им информационным ресурсам.

Главным условием создания комплекса средств противодействия угрозам информационной безопасности СССН является его надежность. Но надежность может быть обеспечена лишь в том случае, если защита является комплексной и системной. Исходя из сказанного, можно дать такое определение: «Комплекс средств противодействия угрозам информационной безопасности СССН – это организованная совокупность органов и объектов (компонентов) защиты информации, использование методов и средств защиты, а также осуществление защитных мероприятий».

При создании комплекса средств противодействия угрозам информационной безопасности в СССН необходимо использовать принцип глубоко эшелонированной обороны от внешних и внутренних угроз. Многоуровневая система защиты с централизованным управлением исключает возможность эффективной реализации атаки при прорыве одного из уровней, в этом случае функцию защиты обеспечат другие. Применение блочной архитектуры дает возможность быстрой модернизации систем при использовании унифицированных стандартных блоков. Комплексный подход к построению системы защиты информации позволяет организовать структурированную многокомпонентную целостную систему противодействия угрозам информационной безопасности.

В настоящее время классическая модель информационного конфликта претерпевает изменения, связанные с повышением количества уровней противодействия, в соответствии с семиуровневой моделью взаимодей-

ствия OSI [2]. Такая модель получила свое название – эталонная модель взаимодействия конфликтующих систем CSI (Conflict System Interconnection Reference Model). Модель делает свой акцент на формализацию информационных конфликтов на каждом уровне модели OSI. С учетом этого особое внимание уделяется вопросам вскрытия, мониторинга СССН и наблюдения за протоколами управления и взаимодействия таких систем.

Информационное противоборство – это совокупность систематизированных, согласованных мероприятий, направленных на достижение информационного превосходства над противником [6]. Информационное противоборство включает в себя два сценария: информационное противодействие и информационную защиту.

Информационное противодействие осуществляется путем проведения комплекса мероприятий, включающих техническую разведку систем связи и управления, перехват передаваемой по каналам связи оперативной информации, мероприятия по дезинформации, радиоэлектронному подавлению и выведению из строя информационно-телекоммуникационных систем противника.

Информационная защита рассматривает вопросы разведки информационно-телекоммуникационных систем противника, проверки полученной информации, защиты от поражения элементов информационных систем. В настоящее время информационная защита и информационное противодействие – процессы, автоматизированные с возможностью применения технологии искусственного интеллекта и не требующие постоянного наблюдения и контроля со стороны человека. Комплекс информационной безопасности в сфере цифровой индустрии может быть дополнен следующими решениями: доверенная операционная среда, средства обнаружения информационно-технических атак, система управления инцидентами безопасности, средства тестирования защищенности [20].

С учетом вышеизложенного вопросы формирования комплекса средств противодействия угрозам информационной безопасности в сетях связи специального назначения являются актуальными и требуют проведения дальнейших исследований в этой области.

Для раскрытия заявленной темы рассмотрим основные термины с соответствующими определениями, опираясь на положения национального стандарта Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения».

Угроза (безопасности информации) – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. По природе возникновения угрозы подразделяются на естественные и искусственные. По источнику воздействия их принято делить на внешние и внутренние.

В качестве основных угроз информации, на предотвращение которых направлена защита информации, обычно выделяют следующие:

– нарушение конфиденциальности (секретности) – потеря ценности информации при ее раскрытии;

– нарушение целостности – потеря ценности информации при ее модификации (изменении) или уничтожении;

– нарушение доступности – потеря ценности информации при невозможности ее оперативного использования.

В соответствии с Доктриной информационной безопасности Российской Федерации угроза информационной безопасности Российской Федерации (далее – информационная угроза) – совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере.

Угрозы информационной безопасности по способам их возможного негативного воздействия подразделяются на информационные, программные, программно-математические, физические, организационные [7, 17].

Информационные угрозы реализуются в виде:

– нарушения адресности и своевременности информационного обмена, противозаконного сбора и использования информации;

– осуществления несанкционированного доступа к информационным ресурсам и их противоправного использования;

– манипулирования информацией (дезинформации, сокрытия или искажения информации);

– хищения информационных ресурсов из библиотек, архивов, банков и баз данных;

– нарушения технологии обработки информации.

Программно-математические угрозы реализуются в виде:

– внедрения в аппаратные и программные изделия компонентов, реализующих функции, не описанные в документации на эти изделия;

– разработки и распространения программ, нарушающих нормальное функционирование информационных систем или их систем защиты информации.

Физические угрозы реализуются в виде:

– уничтожения, повреждения, радиоэлектронного подавления или разрушения средств и систем обработки информации, телекоммуникации и связи;

– хищения программных или аппаратных ключей и мер криптографической защиты информации;

– перехвата информации в технических каналах связи инфокоммуникационных систем;

– внедрения электронных устройств перехвата информации в технические средства связи инфокоммуникационных систем, а также в слу-

жебные помещения органов государственной власти и других силовых ведомств;

– перехвата, дешифрования и навязывания ложной информации в сетях передачи данных и линиях связи;

– воздействия на парольно-ключевые системы защиты систем обработки и передачи информации.

Организационные угрозы реализуются в виде:

– невыполнения требований законодательства в информационной сфере;

– неправомерного ограничения конституционных прав граждан на информационную деятельность и доступ к открытой информации;

– противоправной закупки за рубежом несовершенных или устаревших информационных технологий, средств информатизации, телекоммуникаций и связи.

Рассмотрим возможные виды угроз безопасности информации в рамках какого-либо объекта [21–24].

Пассивные угрозы направлены, в основном, на несанкционированное использование информационных ресурсов объекта, не оказывая при этом влияния на его функционирование. Например, несанкционированный доступ к базам данных, прослушивание каналов связи и т.д.

Активные угрозы имеют целью нарушение нормального функционирования объекта путем целенаправленного воздействия на его информационные ресурсы. К активным угрозам относятся, например, вывод из строя компьютера или его операционной системы, искажение сведений в базах данных, разрушение программного обеспечения, нарушение работы линий связи и т.д.

Источником активных угроз могут быть действия взломщиков, вредоносные программы и т.п.

Умышленные угрозы подразделяются также на внутренние (возникающие внутри управляемой организации) и внешние.

Внутренние угрозы чаще всего определяются социальной напряженностью и тяжелым моральным климатом.

Внешние угрозы могут определяться злонамеренными действиями конкурентов, экономическими условиями и другими причинами (например, стихийными бедствиями). По данным зарубежных источников, получил широкое распространение промышленный шпионаж – наносящие ущерб владельцу коммерческой тайны незаконные сбор, присвоение и передача сведений, составляющих коммерческую тайну, лицом, не уполномоченным на это ее владельцем.

К основным угрозам безопасности информации и нормального функционирования объекта относятся:

– утечка конфиденциальной информации;

– компрометация информации;

– несанкционированное использование информационных ресурсов;
– ошибочное использование информационных ресурсов;
– несанкционированный обмен информацией между абонентами;
– отказ от информации;
– нарушение информационного обслуживания;
– незаконное использование привилегий.

В модели выделяются внутренние (предотвращение угроз, исходящих из внутренних источников) и внешние (предотвращение угроз, исходящих извне) мера противодействия. Потенциальные угрозы для СССН выявляются в процессе создания и исследования модели угроз. В качестве угроз безопасности СССН рассматриваются потенциально или реально существующие воздействия, которые могут привести (приводят) к некоторому «ущербу».

Учитывая комплексность применения технических решений, особую актуальность приобретает задача обеспечения централизованного управления комплексными системами обеспечения информационной безопасности СССН [11, 13, 18].

Классический подход к созданию комплексных систем обеспечения информационной безопасности для СССН заключается в том, что механизмы противодействия, которые используются при построении защищённых СССН, должны быть взаимоувязаны по месту, времени и характеру действия.

Обобщенная модель реализации воздействий на информацию, функционирующую в СССН, и реакции систем противодействия представлены на рис. 1.1.

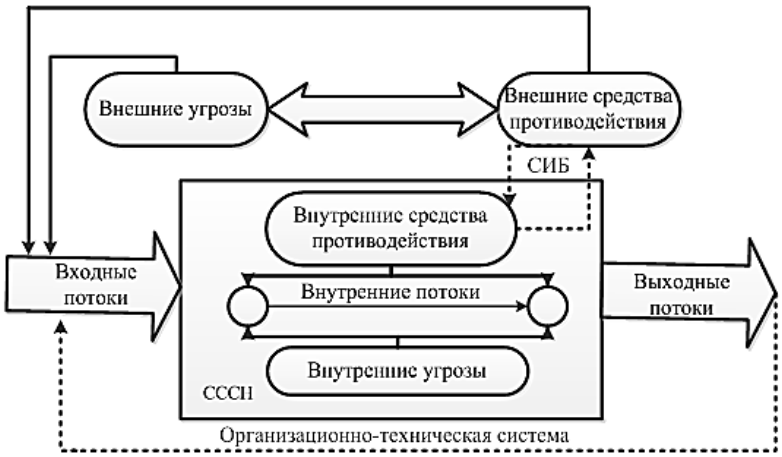


Рис. 1.1. Обобщенная модель реализации воздействий на информацию, функционирующую в СССН, и реакции систем противодействия

За основу берется формализованная модель угроз информационной безопасности с позиции теории множеств с учетом сложности, неодно-

значности (нечеткости), неопределенности оценки событий информационной безопасности в условиях информационного противоборства, рассмотренная в работе [14].

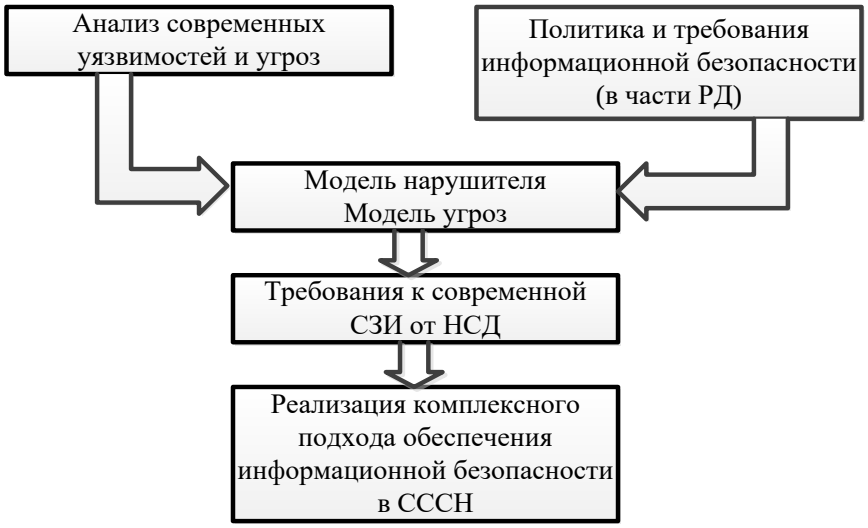


Рис. 1.2. Классический подход к созданию комплексных систем обеспечения информационной безопасности в СССН

Комплексность предполагает также использование в оптимальном сочетании различных методов и средств защиты информации: технических, программных, криптографических, организационных и правовых.

Среди отечественных разработчиков комплексных решений обеспечения информационной безопасности в СССН можно отметить решения компаний: Код Безопасности − «Secret Net Studio», АО «Концерн «Автоматика» − «Центр мониторинга «СОПКА»», ПАО «Ростелеком» − «Единая платформа сервисов кибербезопасности».

В настоящее время при построении цифровых экосистем такие комплексы рассматриваются как интегрированные платформы кибербезопасности. Обеспечение информационной безопасности в условиях динамического развития цифровых технологий и роста киберугроз невозможно без внедрения современных технологий информационной безопасности:

– анализ и интеграция BigData;

– поведенческий анализ (UBA);

– искусственный интеллект и Deep Lerning;

– максимальная интеграция различных элементов безопасности;

– использование мультиагентного подхода;

– использование технологий виртуализации и программно-конфигурируемых гибридных систем с гибкой архитектурой.

Рассмотренные комплексы имеют модульную структуру и позволяют обеспечить защиту от внешних и внутренних угроз. Кроме этого

функционал комплексов включает в себя: централизованное управление защитными механизмами, мониторинг событий безопасности и присвоение им категорий на основе риск-ориентированного подхода.

Интересным решением может являться информационно-аналитическая система – ситуационный центр, реализованнй на интеграционной платформе цифрового управления. Опираясь на возможности ситуационного центра в сфере комплексной безопасности можно решать следующие задачи: мониторинг основных показателей и потенциальных объектов, определение интегральных показателей по отдельным подсистемам комплексной безопасности и потенциала угроз в целом, анализ и прогнозирование, планирование, регулирование и контроль мероприятий по противодействию угрозам информационной безопасности. Интеллектуализация ситуационных центров одно из приоритетных направлений, которое позволит эффективно решать вопросы информационной безопасности. Необходимо учитывать, что для специалиста по информационной безопасности немаловажным фактором является визуализация сигналов тревоги при обнаружении внешних воздействий на СССН. В этом случае мы можем рассматривать визуальную защиту как один из элементов комплексной информационной защиты.

Применение комплексного подхода позволяет идентифицировать и устранить уязвимости в сетевом периметре, обеспечить круглосуточное реагирование на инциденты безопасности, а также привести процессы защиты информации в соответствие с требованиями регуляторов и законодательства Российской Федерации.

Данные примеры показывают перспективность работ, направленных на создание отечественных инновационных комплексов средств противодействия угрозам информационной безопасности в сетях связи специального назначения.

В рамках работы над задачей противодействия угрозам информационной безопасности в СССН коллективом авторов разработаны и зарегистрированы программы: ЭВМ «Методы формирования элементов комплекса противодействия разрушению информации в системах связи специального назначения при деструктивных широкополосных воздействиях»; «Программа выбора способов противодействия деструктивным электромагнитным воздействиям на основе нейронных сетей» [10, 15].

Интегрированный подход состоит в использовании для решения задачи обеспечения информационной безопасности специальных программно-аппаратных комплексов обеспечения безопасности, позволяющих на базе единого персонального компьютера (интегральной системы) обеспечить безопасность всех видов информации (голосовой, визуальной, буквенно-цифровой и т.п.) при её обработке, хранении и передаче по каналам связи. Причем интегральная защита обеспечивается не только использованием криптографии, но и блокированием как несанкционированного до-

ступа, так и технических каналов утечки информации. Несмотря на то, что интегрированный подход требует использования наиболее сложных информационных технологий и является в настоящее время более дорогим, чем традиционные, он является более эффективным и перспективным.

Интегрально оценивая методы и средства получения и защиты информации в типовых ситуациях, можно сделать вывод, что в настоящее время основным направлением противодействия угрозам информационной безопасности СССН является комплексное обеспечение физической (технические средства, линии связи, персонал) и логической (операционная система, прикладные программы и данные) защиты информационных ресурсов. При этом безопасность достигается применением аппаратных, программных и криптографических методов и средств защиты, а также комплексом организационных мероприятий.

Информационная безопасность в рамках комплексной системы безопасности основывается на решении следующих вопросов:

– правовые вопросы обеспечения информационной безопасности;

– организационные вопросы обеспечения информационной безопасности;

– инженерно-техническая защита информации;

Рассмотрим более подробно именно инженерно-техническую защиту информации [25].

Инженерно-техническая защита информации – одна из основных составляющих комплекса мер по защите информации, составляющей государственную, коммерческую и личную тайну. Этот комплекс включает нормативно-правовые документы, организационные и технические меры, направленные на обеспечение безопасности секретной и конфиденциальной информации.

В условиях рынка проблему защиты информации нельзя решить тотальным закрытием информации, потому что без информации о новой продукции, которая распространяется прежде всего через рекламу, невозможно завоевать рынок. Более того, задачи по защите информации в условиях рынка усложняются, так как информация интересует не только разведку других государств, но и многочисленных конкурентов, а также криминальные элементы. Если ранее о специальной технике добывания информации знал узкий круг сотрудников спецслужб, то в условиях рынка любой гражданин может без особых усилий купить практически любое из выпускаемых за рубежом или в России средство для скрытого добывания информации. И хотя условия свободной продажи технических средств добывания информации ужесточаются, пока существует спрос на них, будет и предложение. Учитывая тенденцию к росту цены информации, потребность в технических средствах её добывания не уменьшается.

В нашей стране проблемы защиты информации усугубляются ещё и несовершенством законодательной базы по сохранению государственной и коммерческой тайны.

Инженерно-техническая защита информации включает комплекс организационных и технических мер по обеспечению информационной безопасности техническими средствами и решает следующие задачи:

1. Предотвращение проникновения злоумышленника к источникам информации с целью её уничтожения, хищения или изменения.

2. Защита носителей информации от уничтожения в результате воздействия стихийных сил и, прежде всего, пожара и воды (пены) при его тушении.

3. Предотвращение утечки информации по различным техническим каналам.

Способы и средства решения первых двух задач не отличаются от способов и средств защиты любых материальных ценностей, третья задача решается исключительно способами и средствами инженерно-технической защиты информации.

Инженерно-техническая защита информации представляет собой достаточно быстро развивающуюся область науки и техники на стыке теории систем, физики, оптики, акустики, радиоэлектроники, радиотехники, электро- и радиоизмерений и других дисциплин. Круг вопросов, которыми вынуждена заниматься инженерно-техническая защита, широк и обусловлен многообразием источников и носителей информации, способов и средств её добывания, а следовательно, и защиты. Для обеспечения эффективной инженерно-технической защиты информации необходимо определить:

– что защищать техническими средствами в данной организации, здании, помещении;

– каким угрозам подвергается защищаемая информация со стороны злоумышленников и их технических средств;

– какие способы и средства целесообразно применять для обеспечения информационной безопасности с учётом как величины угрозы, так и затрат на её предотвращение;

– как организовать и реализовать техническую защиту информации в организации.

Без этих знаний защита информации может проводиться в форме круговой обороны (при неограниченных ресурсах) или «латания дыр» в более реальном варианте ограниченности средств.

При организации защиты информации, как и других видов защиты, необходимо также знать и учитывать психологические факторы, влияющие на принятие решения руководителем или любым другим ответственным лицом. Это обусловлено тем, что меры по защите имеют превентивную направленность без достаточно достоверных данных о потенциальных

угрозах не вообще, а применительно к конкретной организации. Кроме того, последствия скрытого хищения информации проявляются спустя некоторое время, когда порой бывает трудно выявить истинную причину ухудшения финансового положения фирмы или появления у конкурента идентичной продукции. Эти факторы не способствуют психологической готовности руководителя на большие затраты на защиту информации. Тем не менее мировой опыт организации защиты информации подтверждает, что на информационную безопасность СССН организации вынуждены выделять порядка 10–20% от общих затрат. Поскольку значительную часть расходов на защиту информации составляют затраты на покупку и эксплуатацию средств защиты, то методология инженерно-технической защиты информации должна обеспечивать возможность рационального выбора средств защиты информации.

Однако выбор средств защиты информации с ориентацией на рекламные данные чреват крупными ошибками, так как в рекламе фирмы-производители не указывают недостатки и преувеличивают достоинства своей продукции. Нужны более глубокие знания о принципах работы и возможностях тех или иных технических средств защиты информации.

Таким образом, при решении задач защиты информации объективно существует необходимость учёта большого числа различных факторов, что не удаётся, как правило, сделать на основе здравого смысла. Поэтому основы инженерно-технической защиты информации должны содержать как теоретические знания, так и методические рекомендации, обеспечивающие решение этих задач.

Так как органам безопасности, занимающимся защитой информации, противостоит разведка с мощным аппаратом и средствами, находящимися на острие научно-технического прогресса, то возможности способов и средств защиты не должны, по крайней мере, уступать возможностям разведки. Исходя из этих исходных положений, основу защиты информации должны составлять принципы, аналогичные принципам добывания информации, а именно:

– непрерывность защиты информации, характеризующаяся постоянной готовностью системы защиты в любое время к отражению угроз информационной безопасности

– активность, предусматривающая прогнозирование действий злоумышленника, разработку и реализацию опережающих мер по защите;

– скрытность, исключающая ознакомление посторонних лиц со средствами и технологией защиты информации;

– целеустремлённость, предполагающая сосредоточение усилий по предотвращению угроз наиболее ценной информации;

– комплексное использование различных способов и средств защиты информации, позволяющее компенсировать недостатки одних достоинствами других.

Эти принципы хотя и не содержат конкретных рекомендаций, однако определяют общие требования к способам и средствам защиты информации.

Следующая группа принципов характеризует основные профессиональные подходы к организации защиты информации, обеспечивает рациональный уровень её защиты и позволяет сократить затраты. Эта группа включает следующие принципы:

– соответствие уровня защиты ценности информации;

– гибкость защиты;

– многозональность защиты, предусматривающая размещение источников информации в зонах с контролируемым уровнем её безопасности;

– многорубежность защиты информации на пути движения злоумышленника или распространения носителя.

Первый принцип определяет экономическую целесообразность применения тех или иных средств и мер защиты. Он заключается в том, что затраты на защиту информации не должны превышать цену защищаемой информации.

Так как цена информации – величина переменная, зависящая как от источника информации, так и от времени, то во избежание неоправданных расходов защита информации должна быть гибкой. Гибкость защиты проявляется в возможности изменения степени защищённости в соответствии с изменившимися требованиями к информационной безопасности.

Требуемый уровень информационной безопасности достигается многозональностью и многорубежностью защиты.

Многозональность обеспечивает дифференцированный санкционированный доступ различных категорий сотрудников и посетителей к источникам информации и реализуется путём разделения пространства, занимаемого объектом защиты (организацией, предприятием, фирмой или любой другой государственной или коммерческой структурой) на так называемые контролируемые зоны.

Типовыми зонами являются:

– территория, занимаемая объектом защиты и ограниченная забором или условной внешней границей;

– здание на территории;

– коридор или его часть;

– помещение.

Зоны могут быть независимыми (здания, помещения), пересекающимися и вложенными (сейф в комнате, комната в здании, здание на территории).

С целью воспрепятствования проникновению злоумышленника в зону на её границе создаются, как правило, один или несколько рубежей защиты.

Рубежи защиты создаются и внутри зоны на пути возможного движения злоумышленника или распространения иных носителей, прежде всего электромагнитных и акустических полей. Например, для защиты акустической информации от прослушивания в помещении может быть установлен рубеж защиты в виде акустического экрана.

Каждая зона характеризуется уровнем безопасности находящейся в ней информации. Информационная безопасность в зоне зависит от:

– расстояния от источника информации (сигнала) до злоумышленника или его средств добывания информации;

– количества и уровня защиты рубежей на пути движения злоумышленника или распространения иного носителя информации (например, поля);

– эффективности способов и средств управления допуском людей и автотранспорта в зону;

– мер по защите информации внутри зоны.

Чем больше удалённость источника информации от места нахождения злоумышленника или его средства добывания информации и чем больше рубежей защиты, тем больше время движения злоумышленника к источнику и ослабление энергии носителя в виде поля или электрического тока. Количество и пространственное расположение зон и рубежей выбирается таким образом, чтобы обеспечить требуемый уровень информационной безопасности как от внешних (вне территории организации), так и внутренних (проникших на территорию злоумышленников или сотрудников) факторов атаки на защищаемый объект. Чем более ценной является информация, тем большим количеством рубежей и зон целесообразно окружить её источник и тогда тем сложнее злоумышленнику обеспечить разведывательный контакт с её носителями.

Рассмотренные выше принципы относятся к защите информации в целом. При построении системы защиты информации нужно учитывать также следующие принципы:

– минимизация дополнительных задач и требований к сотрудникам организации, вызванных мерами по защите информации;

– надёжность в работе технических средств системы, исключающая как нереагирование на угрозы (пропуски угроз) информационной безопасности, так и ложные реакции при их отсутствии;

– ограниченный и контролируемый доступ к элементам системы обеспечения информационной безопасности;

– непрерывность работы системы в любых условиях функционирования объекта защиты, в том числе, например, кратковременном отключении электроэнергии;

– адаптируемость (приспособляемость) системы к изменениям окружающей среды.

Смысл указанных принципов очевиден, дело в том, что закрытая информация о способах и средствах защиты информации в конкретной организации со временем становится известной всё большему числу людей, в результате чего увеличивается вероятность попадания этой информации к злоумышленнику. Поэтому целесообразно производить изменения в структуре системы защиты информации периодически или при появлении достаточно реальной возможности утечки информации о системе защиты, например при внезапном увольнении информированного сотрудника службы безопасности.

1.2. Особенности функционирования базовой инфраструктуры сетей связи специального назначения, а также классификация информационных атак и методы их обнаружения

Федеральный закон № 126 – ФЗ «О связи» [1] регулирует отношения, связанные с созданием и эксплуатацией всех сетей связи и сооружений связи, использованием радиочастотного спектра, оказанием услуг электросвязи и почтовой связи на территории Российской Федерации и на находящихся под юрисдикцией Российской Федерации территориях.

В Федеральном законе № 126 – ФЗ «О связи» электросвязь определяется как «любые излучения, передача или прием знаков, сигналов, голосовой информации, письменного текста, изображений, звуков или сообщений любого рода по радиосистеме, проводной, оптической и другим электромагнитным системам».

В законе, под сетью связи понимается технологическая система, включающая в себя средства и линии связи и предназначенная для электросвязи или почтовой связи. В научных исследованиях посвященных СССН, в этой интерпретации встречается термин «инфокоммуникационная система и сеть специального назначения», который обозначает сеть обмена разнородными сообщениями (различные виды трафика: голос, данные, мультимедиа и др.), интегрирующую в себе информационную вычислительную сеть ведомственных или корпоративных органов управления и телекоммуникационную сеть. Элементами инфокоммуникационных систем специального назначения являются специализированная защищенная инфокоммуникационная сеть и система управления ею. Данная система управления построена на принципах создания автоматизированных систем управления сложными системами [2, 3].

В соответствии со статьей 12 Федерального закона № 126 – ФЗ «О связи» Единая сеть электросвязи Российской Федерации состоит из расположенных на территории Российской Федерации сетей электросвязи следующих категорий:

– сеть связи общего пользования;

– выделенные сети связи;

– технологические сети связи, присоединенные к сети связи общего пользования;

– сети связи специального назначения и другие сети связи для передачи информации при помощи электромагнитных систем.

Статья 16 закона «О связи» дает следующее определение сетей связи специального назначения.

1. Сети связи специального назначения предназначены для нужд органов государственной власти, нужд обороны страны, безопасности государства и обеспечения правопорядка. Эти сети не могут использоваться для возмездного оказания услуг связи, услуг присоединения и услуг по пропуску трафика, если иное не предусмотрено законодательством Российской Федерации.

2. Связь для нужд государственного управления, в том числе президентская связь, правительственная связь, связь для нужд обороны страны, безопасности государства и обеспечения правопорядка, осуществляется в порядке, определенном законодательством Российской Федерации. Расходы на финансирование обеспечения связи для нужд государственного управления, обороны страны, безопасности государства и обеспечения правопорядка предусматриваются федеральным законом о федеральном бюджете на соответствующий год в составе соответствующих расходов.

3. Подготовка и использование ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования сетей связи специального назначения осуществляются в порядке, установленном Правительством Российской Федерации.

4. Центры управления сетями связи специального назначения обеспечивают их взаимодействие с другими сетями единой сети электросвязи Российской Федерации в порядке, установленном федеральным органом исполнительной власти в области связи.

По видам обеспечиваемого для абонентов сервиса и услуг связи выделяют первичные и вторичные сети электросвязи. В составе первичных и вторичных сетей СССН могут быть организованы выделенные сети.

Основой построения первичных (транспортных) сетей в составе СССН являются:

– линии и сети радиосвязи;

– линии и сети спутниковой связи;

– волоконно-оптические линии связи;

– линии радиорелейной и тропосферной связи;

– кабельные линии электрической связи.

Существует деление вторичных сетей по следующим типам:

– локальные сети;

– сети коллективного доступа;

– цифровые линии абонентского доступа;

– сети мобильной и транкинговой связи;

– сети радиодоступа.

Под системой передачи понимается комплекс технических средств, обеспечивающий образование линейного тракта, типовых групповых трактов и каналов передачи. При этом применяются средства связи – технические и программные средства, используемые для формирования, приема, обработки, хранения, передачи, доставки сообщений электросвязи или почтовых отправлений, а также иные технические и программные средства, используемые при оказании услуг связи или обеспечении функционирования сетей связи.

Такой элемент электросвязи, как радиосвязь, является основным видом связи со стационарными и подвижными объектами, а в ряде случаев единственным видом связи, обеспечивающим управление для нужд обороны страны, безопасности государства и обеспечения правопорядка при осложнении оперативной обстановки и ликвидации последствий чрезвычайных ситуаций. Использование радиосвязи позволяет в короткие сроки сконцентрировать в нужном месте необходимое количество оперативных сил и средств для проведения мероприятий, согласовать по месту и времени их действия и осуществлять единое руководство ими.

В настоящее время в интересах министерств и ведомств, обеспечивающих функции обороны страны, безопасности государства и обеспечения правопорядка, реализованы защищенные интегрированные мультисервисные телекоммуникационные системы, основанные на интегрированной транспортной среде и обеспечивающие взаимодействие с телекоммуникационными системами органов государственной власти, включая правоохранительные органы, а также доступ к услугам публичных и специальных федеральных информационно-телекоммуникационных систем и состоящих из автоматизированных банков данных общего пользования на базе унифицированных программно-технических комплексов информационно-аналитических и экспертно-криминалистических центров органов внутренних дел [5, 6].

Кроме того, необходимо обеспечить защиту служебной информации ограниченного распространения для системы передачи данных и цифровой радиосвязи стандартов APCO 25 и DMR с учетом возможной территориальной миграции абонентов. Предполагается до 2024 года реализовать создание и внедрение:

– цифровых решений, обеспечивающих полноценное взаимодействие абонентов цифровых сетей радиосвязи стандартов APCO 25 и DMR и защиту передаваемой служебной информации ограниченного распространения;

– технических решений, обеспечивающих ведомственный защищенный мобильный широкополосный радиодоступ к сервисам ИСОД МВД России;

– комбинированных устройств, включающих в себя системы цифровой радиосвязи и устройства защищенного мобильного широкополосного радиодоступа к сервисам ИСОД МВД России.

Реализация защищенной ведомственной системы мобильного широкополосного беспроводного радиодоступа, должна выступать как виртуальная частная сеть (VPN) по отношению к сетям связи общего пользования. Для доступа к сервисам ИСОД МВД России предполагается использование планшетного компьютера с возможностью работы в сетях мобильного широкополосного радиодоступа.

Для обеспечения функционирования базовой инфраструктуры ведомственной системы радиосвязи, а также передачи речевого трафика и данных на мобильные объекты органов внутренних дел в перспективных сетях радиосвязи специального назначения наиболее предпочтительным вариантом является использование существующих ресурсов интегрированной мультисервисной телекоммуникационной системы, которая предоставляет:

– единую сквозную транспортную среду для сигналов управления и информационных сигналов (речь, данные) на базе стека протоколов TCP/IP (Transmission Control Protocol/Internet Protocol – Протокол управления передачей/Протокол Internet), в том числе по потоку E1;

– IP-каналы связи ИМТС (интегрированные мультисервисные телекоммуникационные системы), построенные на базе Ethernet-сетей с использованием протоколов TCP/IP, для передачи абонентского трафика и служебной информации между базовыми станциями, АРМ диспетчера, администратора и центра управления и коммутации в любом цифровом режиме.

Интегрированная мультисервисная телекоммуникационная система (ИМТС) на уровне городских и районных центров субъектов Российской Федерации создаётся для обеспечения технической возможности подключения пользователей. ИМТС соединяются друг с другом и включаются в транспортную среду по протоколу TCP/IP по собственным или арендованным каналам связи.

Для примера на рис. 1.3 и 1.4 показаны обобщённые варианты использования сетей МВД России для организации внутрисистемных линий связи в сетях радиосвязи цифрового стандарта DMR (конвенциальная и транкинговая сети) [26].

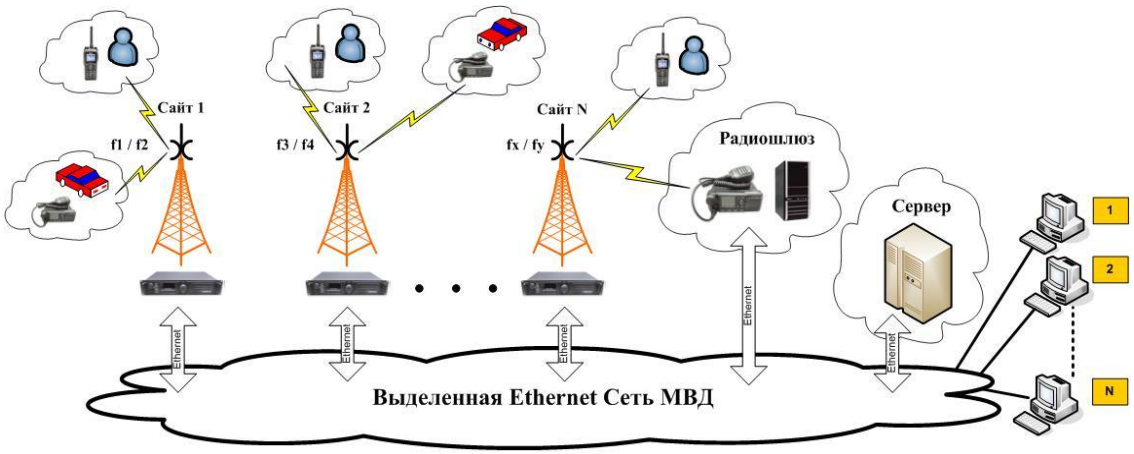


Рис. 1.3. Вариант использования сетей МВД России для организации внутрисистемных линий связи в сетях цифровой радиосвязи (стандарт DMR, конвенциальная связь)

Варианты реализации опорной транспортной сети ИМТС для каждой конкретной сети цифровой радиосвязи ОВД определяются на этапе предварительной проработки и проектирования с учётом конфигурации сети, требуемой пропускной способности каналов связи.

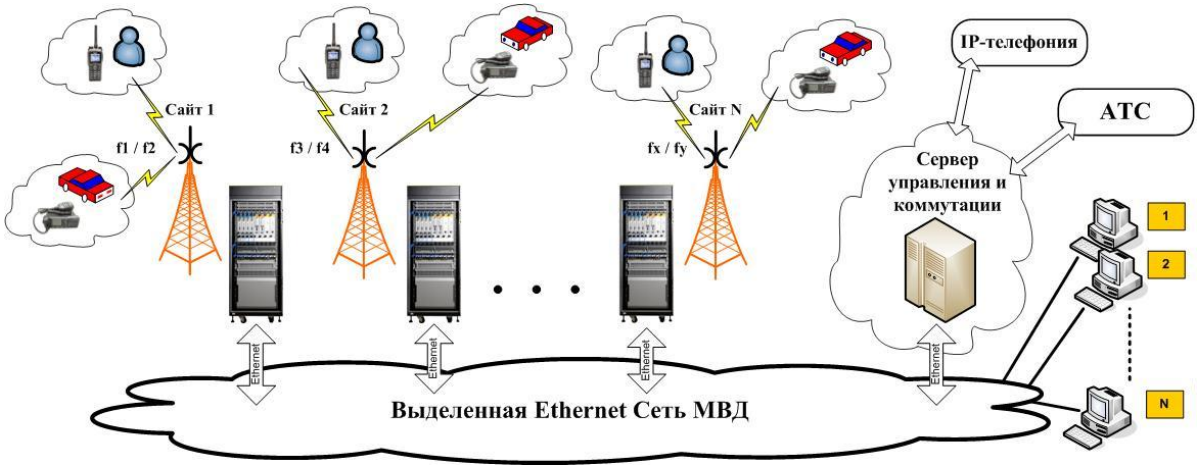


Рис. 1.4. Вариант использования сетей МВД России для организации внутрисистемных линий связи в сетях цифровой радиосвязи (стандарт DMR, транкинговая система)

Для обеспечения подключения коммутационного оборудования радиоцентров при необходимости следует предусмотреть необходимое количество портов с интерфейсом E1 G703 или IP-каналами.

Другим возможным вариантом для обеспечения функционирования базовой инфраструктуры ведомственной системы радиосвязи, а также передачи речевого трафика и данных на мобильные объекты органов внутренних дел в перспективных сетях радиосвязи МВД России является ис-

пользование ресурсов единой системы электросвязи (ЕСЭ) Российской Федерации (аренда цифровых каналов связи E1 или IP-каналов у операторов связи), а также обеспечение межведомственного информационного взаимодействия с федеральными органами государственной власти.

В соответствии со ст. 16 Федерального закона № 126-ФЗ «О связи» подготовка и использование ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования сетей связи специального назначения осуществляются в порядке, установленном Правительством Российской Федерации.

При организации коммуникаций в неоднородной среде применяется набор протоколов TCP/IP. Исторически вопросы безопасности сетей, строящихся на его основе, отходили на второй план, что привело к уязвимости реализации этого протокола.

С понятием угрозы безопасности связано понятие уязвимости сети. Уязвимость – параметр, характеризующий возможность нанесения системе повреждений любой природы теми или иными внешними средствами или факторами. Другим словами, для СССН это неудачное свойство или набор параметров или характеристик, которые могут привести к угрозе.

Атака на СССН – это поиск и/или использование злоумышленником той или иной уязвимости системы, реализация угрозы безопасности.

Сетевые атаки столь же разнообразны, как и системы, против которых они направлены. По способу реализации некоторые отличаются большой сложностью, другие может реализовать обычный пользователь, совсем не задумываясь о последствиях [27].

Нарушитель, осуществляя атаку, обычно ставит следующие цели:

– нарушение конфиденциальности передаваемой информации;

– нарушение целостности и достоверности передаваемой информации;

– нарушение системы в целом или отдельных ее частей.

С учетом этого выделяют четыре основных категории сетевых атак:

– атаки доступа;

– атаки модификации;

– атаки типа «отказ в обслуживании»;

– комбинированные атаки.

Атаки доступа – это получение злоумышленником информации, на ознакомление с которой у него нет разрешения. Атака доступа направлена на нарушение конфиденциальности информации. К атакам доступа можно отнести: подслушивание (Sniffing), перехват (Hacking), перехват сеанса (Session Hacking).

Атаки модификации – это попытка неправомочного изменения информации. Такая атака направлена на нарушение целостности и возможна везде где передается информация. К атакам модификации относятся: изменение данных, добавление данных, удаление данных.

Атаки типа «отказ в обслуживании» (Denial-of-Servise, DoS) нацелены на получение доступа к сети или на извлечение из нее какой-либо информации. В ходе таких атак могут использоваться такие протоколы, как TCP и ICMP. Если атака проводится одновременно через множество устройств, можно говорить о DDoS (Distributed DoS). К атакам типа «отказ в обслуживании» относятся: отказ в доступе к информации, отказ в доступе к приложениям, отказ в доступе к системе, отказ в доступе к средствам связи.

Комбинированные атаки заключается в применении злоумышленником нескольких взаимосвязанных действий для реализации поставленной цели. К комбинированным атакам можно отнести: подмену доверенного субъекта, посредничество, атаку эксплойта, парольные атаки, угадывание ключа, атаки на уровне приложений, анализ сетевого трафика, сетевую разведку, злоупотребление доверием, псевдоантивирусы, фишиг, фарминг, применение ботнетов, рассылку спама, анонимный доступ в сеть, кражу конфиденциальных данных.

1.3. Модель угроз информационной безопасности сети связи специального назначения

Комплекс мер противодействия угрозам информационной безопасности в сетях связи специального назначения представляет собой сложную многофункциональную систему безопасности, состоящую из множества необходимых подсистем функционирования, объединенных единой интегрированной мультисервисной транспортной средой. Некоторые подсистемы могут отличаться своей внутренней инфраструктурой, наличием собственных СУБД, интеллектуальными средствами поддержки и принятия решений. Многие из таких комплексов являются самостоятельными информационными системами, доступ к которым осуществляется посредством удаленного подключения субъектов (пользователей или процессов подсистем обеспечения безопасности) к выделенным им информационным ресурсам.

Разнородность программно-аппаратного обеспечения подсистем комплекса мер противодействия угрозам информационной безопасности, огромное количество неоднозначно классифицируемых данных (признаков атак), получаемых от сетевых и хостовых сенсоров, сложность оценки событий информационной безопасности, возможные реализаций угроз безопасности информации через обнаруживаемые злоумышленником уязвимости указывают на необходимость создания требуемой системы защиты информации.

Описание угроз безопасности, построение их модели позволяют адекватно оценить уровень опасности и предложить необходимую архитектуру подсистемы защиты сети связи специального назначения. Одним

из обязательных этапов формирования требований к защите информации в сети СССН является определение актуальных угроз. Сведения об угрозах и известных уязвимостях могут быть получены из Банка данных угроз безопасности информации (БДУ) ФСТЭК России.

В монографии для построения такой модели проведем анализ угроз, направленных на информационные ресурсы сети связи специального назначения, учитывая данные, получаемые сенсорами маршрутизаторов, коммутаторов, межсетевых экранов (МСЭ), систем обнаружения аномалий (СОА) и вторжений (СОВ). Для решения задачи определения актуальных угроз используются методические документы ФСТЭК России и, кроме того, может быть применен ряд зарубежных методик, позволяющих получить оценку защищенности для СССН (FRAAP, COBRA, OCTAVE, RiskWatch и др.).

В настоящее время подавляющее число угроз информационной безопасности принципиально могут быть реализованы только в процессе функционирования информационных систем [30], при этом логическое вторжение является наиболее результативным для злоумышленника. Логическое вторжение обычно делится на внутрисистемное и удаленное. При внутрисистемном вторжении предполагается, что нарушитель уже имеет учетную запись в системе как пользователь с невысокими привилегиями и совершает атаку на систему для получения дополнительных привилегий. Удаленное вторжение заключается в попытке проникновения в систему с удаленной машины (хоста) участников информационного обмена сети связи специального назначения. Это атаки, выполняемые при постоянном участии человека, и атаки, выполняемые специальными программами: атаки на информацию, хранящуюся на внешних запоминающих устройствах, атаки на информацию, передаваемую по линиям связи, атаки на информацию, обрабатываемую в памяти компьютера [31].

Основная цель практически любой атаки при реализации угрозы – получение несанкционированного доступа к информации.

Для описания угрозы, представляющей собой канал несанкционированного доступа (реализация сетевой атаки, деструктивные воздействия вредоносных программ, инсайдерские атаки), необходимо указать субъект доступа, путь распространения угрозы и информационный объект, к которому осуществляется несанкционированный доступ, нарушающий правила разграничения. Такая угроза может быть описана кортежем [14, 31]:

$$U = \langle S, K, Б_c, Б_x, П, ИО(C) \rangle, \qquad (1.1)$$

где S – источник угрозы, т.е. субъект доступа (пользователь (инсайдер), внешний злоумышленник или запущенные ими процессы); K – оборудование в канале связи (коммутаторы, маршрутизаторы и др.); $Б_c$, $Б_x$ – сервисы безопасности на пути распространения угрозы, соответственно сетевые и хостовые (МСЭ, СОА, журналы регистрации аномальных сетевых соединений, журналы регистрации операционных систем и др.); $П$ – протоколы

и пакеты; *ИО* – информационный объект доступа (в конкретном сетевом сегменте ограничения *С*).

В соответствии с рекомендуемыми в [32] основными принципами построения архитектуры безопасности сети зададим три категории ограничения информации: открытая, конфиденциальная и секретная. Тогда множество информационных объектов *ИО* (информационные ресурсы конфиденциального, секретного и открытого контуров) в сети связи специального назначения представляет собой объединение множеств:

$$ИО = ИО^{o} \cup ИО^{к} \cup ИО^{c}, \quad (1.2)$$

где $ИО^{o}$ – множество информационных объектов категории «открыто»; $ИО^{к}$ – множество информационных объектов категории «конфиденциально»; $ИО^{c}$ – множество информационных объектов категории «секретно».

Множество сегментов сети *С* также представляет собой объединение множеств:

$$C = C^{o} \cup C^{к} \cup C^{c}, \quad (1.3)$$

где $C^{o}, C^{к}, C^{c}$ – подмножества сегментов, в которых хранится и обрабатывается информация соответственно с открытым, конфиденциальным и секретным уровнем ограничения;

$$C^{o} = \{c_k^{o}, k \in [1, K]\}, \quad (1.4)$$

где *K* – число сегментов, в которых хранится и обрабатывается информация категории «открыто»;

$$C^{к} = \{c_l^{к}, l \in [1, L]\}, \quad (1.5)$$

где *L* – число сегментов, в которых хранится и обрабатывается информация категории «конфиденциально»;

$$C^{c} = \{c_m^{c}, m \in [1, M]\}, \quad (1.6)$$

где *M* – число сегментов, в которых хранится и обрабатывается информация категории «секретно».

На хостах хранится и обрабатывается информация с определенным для сегмента уровнем ограничения. Зададим множество хостов в каждом сегменте через характеристические предикаты [6]:

$$X_k^{o} = \{x_{k_i}^{o} : x_{k_i}^{o} \text{ - узел в сегменте } C_k^{o}\}, i \in [1, I_k]; \quad (1.7)$$

$$X_l^{k} = \{x_{l_j}^{k} : x_{l_j}^{k} \text{ - узел в сегменте } C_l^{k}\}, j \in [1, J_l]; \quad (1.8)$$

$$X_m^{c} = \{x_{m_k}^{c} : x_{m_k}^{c} \text{ - узел в сегменте } C_m^{c}\}, k \in [1, K_m]. \quad (1.9)$$

Множество субъектов доступа, внешних или внутренних, можно рассматривать как источники угроз, под которыми понимается атакующая программа или пользователь, непосредственно осуществляющий воздействие на сетевой сегмент информационной инфраструктуры сети связи специального назначения.

По расположению субъекта доступа относительно атакуемого объекта угрозы подразделяются на внешние и внутренние (внутрисегментные и межсегментные) [31].

Внешние угрозы – это потенциально возможные действия, заключающиеся в поиске и использовании той или иной уязвимости, предпринимаемые: злоумышленником в целях проникновения с удаленного хоста в защищаемую систему, получения прав на удаленный доступ к ресурсам подсистем сети связи специального назначения и хищения данных; удаленным пользователем, имеющим легальные права, пытающимся превысить уровень своих полномочий.

Внутренние угрозы связаны с нарушением принятой политики безопасности: нелегальным поведением пользователя на хосте (ПК или сервере), попытками доступа пользователя к информационным ресурсам, уровень ограничения которых превышает его уровень доступа (попытки сетевых соединений, запуска приложений, реализации запросов к СУБД).

Множество угроз включает в себя подмножества внешних и внутренних угроз:

$$U = U^{вн} и U^{внш}. \qquad (1.10)$$

В свою очередь, подмножество внутренних угроз включает в себя подмножества $U_{m(l)}{}^{вн}$ и $U_{ml(k)}{}^{вн}$, где

$$U_{m(l)}{}^{вн} = \left\langle S^k, К, Б_c, Б_x, П, ИО^c\left(C^c\right)\right\rangle . \qquad (1.11)$$

Здесь $U_{m(l)}{}^{вн}$ – угроза информационным объектам категории ограничения «секретно» ($ИО^c$) в случае, когда нарушитель имеет учетную запись в системе как пользователь с правами доступа к информации с уровнем ограничения «конфиденциально» (S^k), обрабатываемой в сегментах с ограничением «конфиденциально» или «открыто», и пытается превысить свои привилегии;

$$U_{ml(k)}{}^{вн} = \left\langle S^o, К, Б_c, Б_x, П, ИО^k\left(C^k\right) \square\ ИО^c\left(C^c\right)\right\rangle - \qquad (1.12)$$

угроза информационным объектам категории ограничения «секретно» ($ИО^c$) и «конфиденциально» ($ИО^k$) в случае, когда нарушитель имеет учетную запись в системе как пользователь с правами доступа к «открытой» информации (S^o), обрабатываемой в сегментах сети с «открытым» доступом, и пытается превысить свои привилегии.

Внешняя угроза связана с внешним субъектом доступа и описывается кортежем

$$U^{внш} = \left\langle S^{внш}, К, Б_c, Б_x, П, ИО(C)\right\rangle . \qquad (1.13)$$

Таким образом, получено описание угроз безопасности исследуемого объекта, при этом источниками внутренних угроз являются субъекты и процессы, описываемые множествами S^k, S^o, источниками внешних угроз – субъекты и процессы, описываемые множеством $S^{внш}$.

Множество внешних субъектов доступа – это объединение множеств

$$S^{внш} = S_r^{п.внш} \square\ S_r^{внш}, r \square\ [1, R], \qquad (1.14)$$

где $S_r^{п.внш}$ – внешние пользователи, обладающие правами доступа (авторизованные удаленные участники информационного обмена); $S_r^{внш}$ – внешние пользователи, обладающие возможностью несанкционированного доступа (неавторизованные участники информационного обмена других сегментов сети связи специального назначения); R – число точек доступа через периметр сети связи специального назначения (совокупность инфокоммуникационного оборудования, заключенная в единое кольцо информационного обмена локальной сети и имеющая доступ во внешние сети – к другим контурам).

Введем множество функциональных индикаторов $И$ – значений контролируемых параметров, с помощью которых фиксируются отдельные события информационной безопасности. Функциональные индикаторы отражают результаты контроля: изменений правил МСЭ; соответствия настроек других сервисов безопасности политике безопасности; изменений привилегий пользователей; системных вызовов; попыток доступа; состояния соединений.

Поскольку одним из эффективных способов идентифицировать угрозу (атаку) является анализ комбинаций поведений, предлагается сопоставить множеству возможных путей распространения атаки множество индикаторов. Тогда признак того, что подозрительная активность является угрозой, может быть оценен числом индикаторов на пути распространения атаки. Для идентификации внутренних атак предлагается использовать два типа индикаторов: системные и сетевые (хостовые), для идентификации внешних вторжений дополнительно использовать индикаторы, отображающие аномальные события на периметре инфокоммуникационной сети.

Зададим множество путей распространения атак с помощью характеристического предиката [33]:

$$P = \{p_i : p_i \text{ - путь распространения атаки }\}, i \in [1, I_p]; \quad (1.15)$$

$$I_p = Q^o + Q^к + Q^c, \quad (1.16)$$

где $Q^o, Q^к, Q^c$ – число путей распространения атак к узлам в сегментах, в которых хранится и обрабатывается информация с уровнем ограничения, соответственно «открытая», «конфиденциальная», «секретная».

Множество индикаторов является объединением подмножеств:

$$И = И_o^к \cup И_o^c \cup И_к^c \cup И_{пер}, \quad (1.17)$$

где $И_o^к$ – подмножество индикаторов, фиксирующих попытки доступа субъекта с «открытым» уровнем доступа к объекту с уровнем ограничения «конфиденциально»; $И_o^c$ – подмножество индикаторов, фиксирующих попытку доступа субъекта с «открытым» уровнем доступа к объекту с уровнем ограничения «секретно»; $И_{пер}$ – подмножество индикаторов, фиксирующих попытки проникновения на периметре.

Заданное множество индикаторов и путей распространения атак позволяет внести дополнительные экспертные знания о количестве событий информационной безопасности в систему построения нечетких продукционных правил [14, 34].

Предложенное описание модели угроз показывает основные элементы канала несанкционированного доступа (субъект доступа, путь распространения атаки и информационный объект) к информации, циркулирующей на разных уровнях сетевого инфокоммуникационного взаимодействия (контуры безопасности, хосты сегмента, периметр сети) сети связи специального назначения, учитывающего показания индикаторов событий информационной безопасности от маршрутизаторов, межсетевых экранов, систем обнаружения аномалий и вторжений. Обозначается подход для создания модели комплексов средств противодействия угрозам информационной безопасности в сети связи специального назначения.

Таким образом, приведено формализованное построение угроз безопасности сети связи специального назначения с позиции теории множеств с учетом сложности, неоднозначности (нечеткости), неопределенности оценки событий информационной безопасности в условиях информационного противоборства. Такое описание является математической основой построения моделей трудно формализуемых процессов информационного противоборства. Сама модель строится на основе использования интеллектуальных методов, учитывающих суждения специалистов и предоставляющих окончательный результат в виде простых операций над неопределенностью, неточностью и размытостью событий информационной безопасности (теория нечетких множеств, лингвистическая неопределенность, нечеткая логика).

1.4. Принципы оптимального интегрирования разнородных информационных процессов в интересах противодействия угрозам информационной безопасности в сетях связи специального назначения

Основополагающими принципами при организации противодействия угрозам разрушения информации в сетях связи специального назначения (СССН) на основе оптимального интегрирования разнородных информационных процессов СССН являются [7] **принцип допустимости таких угроз и принцип согласованности разнородных информационных процессов, одновременно обеспечивающих целевые функции СССН и функции противодействия разрушению информации в этих системах.**

В соответствии с первым принципом СССН должна рассматриваться как система, обладающая некоторой гарантированной эффективностью при воздействии угроз разрушения информации. Это достигается тем, что наличие таких угроз является следствием реальных условий функционирования СССН, приводящих к особым состояниям ее информационных про-

цессов. Такие состояния должны быть допустимыми и содержать информационные процедуры воздействия на информационный процесс, противодействующий подобного рода угрозам.

Реализация второго принципа приводит к необходимости перераспределения информационных ресурсов СССН в интересах одновременной реализации информационного процесса, обеспечивающего целевые функции СССН, и информационных процессов противодействия угрозам разрушения информации. Это, в общем случае, ведет к некоторому снижению эффективности СССН в условиях отсутствия воздействия угроз разрушения информации, но позволяет сохранять ее приемлемые значения при наличии таких воздействий.

Это позволяет рассматривать проблему повышения эффективности противодействия угрозам разрушения информации в СССН на основе оптимального интегрирования разнородных информационных процессов как согласованную последовательность задач оптимального информационного резервирования.

Для решения этих задач формальными методами сформулируем ряд принципов [7, 35].

Принцип интегрирования форм информационного резервирования предполагает необходимость использования двух различных подходов к резервированию информационных процессов в СССН [7, 35]. В соответствии с первым подходом осуществляется постоянное насыщение избыточностью передаваемой информации с целью идентификации признаков ее разрушения. При втором подходе информационные процессы резервируются лишь в случае идентификации таких признаков с целью восстановления информации, подвергнувшейся разрушению.

Принцип покрытия информационного пространства при одновременной реализации двух разнородных информационных процессов предполагает внедрение в базовый информационный процесс процедур другого информационного процесса, который обеспечивает требуемый уровень характеристик базового процесса. При этом в процессе нормального режима обмена информацией в СССН (без разрушения информации) базовым информационным процессом является процесс передачи информации, а дополнительным – информационный процесс идентификации признаков разрушения информации. С момента идентификации разрушения информации до момента восстановления нормального режима работы СССН базовым является процесс идентификации признаков разрушения, а дополнительным – информационный процесс восстановления нормального режима обмена информацией в СССН. Принцип информационного покрытия является одним из основных условий оптимизации функционирования СССН в условиях противодействия разрушению информации.

Принцип баланса эффективности СССН предполагает нахождение компромисса между снижением, с одной стороны, эффективности

СССН вследствие воздействия угроз разрушения информации и постоянной избыточности информационного процесса и ее повышением, с другой стороны, за счет резервирования при воздействии угроз разрушения информации.

Принцип оптимального распределения информационной избыточности резерва утверждает, что при обеспечении требуемого уровня защищенности информационного процесса в СССН информационная избыточность должна распределяться путем согласования потребностей информационных процедур в избыточности с возможностями по ее внесению. При реализации этого принципа предполагается, что воздействию угроз разрушения будут подвержены чаще выполняемые информационные процедуры СССН, а возможности по внесению избыточности – с учетом ее влияния на характеристики СССН.

Принцип показателей эффективности резервирования СССН предполагает оценку характеристик информационных процедур, реализующих процессы резервирования. Этот принцип основан на том, что частные процессы идентификации источника угроз, анализа последствий воздействия угроз и восстановления корректности информационных процессов в СССН являются по содержанию независимыми друг от друга. Вместе с тем в соответствии с алгоритмами противодействия перечисленные частные процессы должны выполняться строго последовательно, в том порядке, в котором они перечислены, т.е. являются функционально зависимыми. Однако данный принцип не противоречит определению информационного процесса, так как в условиях рассмотренного выше принципа информационного покрытия сохраняется основное условие интегрируемости разнородных информационных процессов – наличие базового и дополнительного информационных процессов.

В соответствии с **принципом дифференциации в реализации информационной избыточности СССН** информационный объем, выделяемый для идентификации признаков разрушения информации, может быть реализован двумя способами: путем анализа смысловых характеристик передаваемых данных и путем анализа параметрических характеристик.

Для обеспечения возможности выявления ресурса информационной избыточности СССН, его распределения и реализации при организации противодействия разрушению информации на основе оптимального интегрирования разнородных информационных процессов в условиях подобного рода угроз информационной безопасности с учетом изложенных принципов перейдем к обоснованию и формализации показателей для оценки эффективности противодействия разрушению информации в СССН и эффективности функционирования таких систем в данных условиях [35].

1.5. Методы теории эффективности, декомпозиции и оптимизации показателей качества функционирования сетей связи специального назначения при условии защиты от разрушающих информационных воздействий

Современная система управления деятельностью органов внутренних дел относится к классу организационно-технических (человеко-машинных) систем и представляет собой совокупность взаимосвязанных технических средств и организационно взаимодействующих между собой должностных лиц, совершающих согласованные действия. При этом эффективность управления в органах государственной власти, органах, осуществляющих функции обороны страны, безопасности государства и обеспечения правопорядка, в значительной степени определяется достоверностью, полнотой и своевременностью информации, необходимой для оценки обстановки и принятия обоснованных решений, а также надежностью управления системой связи. Под эффективностью системы понимается ее соответствие своему целевому предназначению. Целевое же предназначение системы определяет выполнение требуемых показателей качества. Применительно к системам связи к таким требованиям можно отнести пропускную способность, достоверность, задержки в доставке сообщения и др. Тогда требуемое качество системы можно описать вектором $Q = (q_1, q_2, \ldots q_n)$, где q_i – показатель качества для i-го частного требования к системе. Заметим, что в силу случайного характера внешних воздействий на систему связи, а также присущей самой системе неопределенности описания ее внутреннего состояния текущее качество выходного информационного процесса является случайной функцией времени [49].

Одной из трудностей формирования вектора показателей качества системы связи является несоответствие между реальным составом информации о характеристиках сети связи и требуемым ее объемом. Такая неполнота данных приводит к трудности формирования обобщенного критерия эффективности функционирования и, как итог, критерия оптимальности управления. Иначе говоря, появляется необходимость описания управления в условиях целевой неопределенности. В силу динамического характера задач управления в мобильных системах связи возникают сложности формирования полной системы показателей эффективности системы управления. Присущие мобильным сетям неполнота и противоречивость контрольной информации обуславливают возможность использования нечеткой системы управления (НСУ), которая использует нечеткое описание процесса и системы управления им в виде нечеткой базы знаний. Такая НСУ затем преобразует нечеткое описание системы в последовательность команд управления на основе использования логико-лингвистического моделирования. При этом в НСУ реализуется ряд функций, ранее бывших

прерогативой ЛПР: восприятие информации в словесной форме, структурирование, логический анализ, формулирование выводов.

Процесс управления описывается совокупностью функций управления, а конкретные задачи оперативного управления будут определяться условиями функционирования сети. Выработка решений осуществляется по функциям управления с учетом целевых функций. При этом осуществляется декомпозиция основной цели функционирования управления системы, как это описано ранее. Так, на канальном уровне реализуется управление ресурсами: пространством, частотой, временем и кодом. Решение о методе доступа и об эффективном использовании ресурсов сети принимается интеллектуальной НСУ.

Нечеткая система управления должна опираться на знания об объекте управления, включающие в себя состав и структуру сети связи, правила и закономерности управления ею.

База знаний НСУ также включает в себя знания как о целях функционирования системы и управления в целом, так и способах достижения целей, то есть логических правилах вывода решений о достижимости целей управления с учетом ресурсных или других ограничений в процессе управления.

Выработка решений на основе НСУ будет осуществляться по функциям управления с реализацией заявленных целей управления. При этом цель достигается при использовании определенных ресурсов системы и применении управляемых параметров, например определенной мощности, скорости передачи, вида модуляции, метода маршрутизации и т.д.

В условиях существующей неопределенности знаний о состоянии внешней среды, внутреннем состоянии системы связи возможно использование алгоритмов, основанных на понятиях нечеткой логики. Так, например, если задача многокритериальной оптимизации допускает формулировку в лингвистических переменных, то становится возможным использовать расстояние Хемминга как оцениваемое расстояние до эталона. При этом понятие эталона задается принятием всех показателей на «высоком» уровне, что и определяет нечеткое множество – эталон, от которого и отсчитывается расстояние Хемминга.

Оценка эффективности системы управления позволяет также найти показатели эффективности всей сети [36].

При решении проблемы противодействия разрушению информации в СССН на основе оптимального интегрирования информационных процессов с учетом рассмотренных принципов интерес представляет пропускная способность каналов обмена информации [7].

В качестве основы для конструирования показателя эффективности функционирования СССН в условиях противодействия разрушению информации будем использовать объем информации, передаваемый в единицу времени C, гарантированно обеспечивающий противодействие [35].

Информационные процессы в СССН считаются реализованными корректно, если величина C не выше пропускной способности канала $C^{(к)}$, т.е. при выполнении неравенства:

$$C \le C^{(k)}. \qquad (1.18)$$

Обозначим формально вектором $\vec{X}$ условия функционирования СССН, вектором $\vec{S}$ – функциональную структуру информационных процессов в СССН, а вектором $\vec{Y}$ – характеристики угроз разрушения информации. Тогда величину C можно представить в виде $C = C\left(\vec{X}, \vec{Y}, \vec{S}\right)$. Случайный характер условий функционирования СССН, описываемых вектором $\vec{X}$, и воздействий угроз разрушения информации, описываемых вектором $\vec{Y}$, позволяет сделать вывод о том, что правая часть неравенства (1.18) является случайной величиной, поэтому его выполнение является случайным событием. Вероятность этого события $P\left(C \le C^{(k)}\right)$ представляет собой среднее количество ситуаций, когда СССН корректно реализует свои функции по передаче информации в течение исследуемого интервала времени $[t_н, t_к]$ ее функционирования относительно общего числа таких ситуаций, т.е. имеет место соотношение:

$$P(C \le C^{(k)}) = \frac{1}{L}\sum_{l=1}^{L}\delta_l, \text{ где } \quad \delta_l = \begin{cases} 1, \textit{ при } C_l \le C^{(к)} \\ \\ 0, \textit{ при } C_l \ge C^{(к)} \end{cases};$$

C_l – объем информации, передаваемый в единицу времени при l – ой, $l = 1, 2, \ldots, L$, попытке ее разрушения [82];

L – общее число попыток разрушения информации в СССН в течение исследуемого интервала $[t_н, t_к]$ времени ее функционирования;

$t_н$ – начало временного интервала исследования процесса функционирования СССН;

$t_к$ – конец этого интервала.

Пропускная способность канала $C^{(к)}$ зависит от технических характеристик СССН и является величиной детерминированной.

Значение величины C зависит от способа противодействия разрушению информации: традиционного, при котором осуществляется обеспечение помехоустойчивости; и рассматриваемого в работе способа противодействия разрушению информации на основе оптимального интегрирования разнородных информационных процессов.

При использовании традиционного способа осуществляется противодействие лишь угрозам, обусловленным условиями штатного функционирования СССН. В рамках данного способа противодействие осуществляется за счет помехоустойчивого кодирования [27, 109], при этом кодирующую часть передаваемых сообщений, несмотря на ее избыточность, не

принято отделять от информационной. В этом случае величину C можно записать в виде

$$C^{(mp)} = C^{(ц)},$$

где $C^{(ц)}$ – объем информации, передаваемый в единицу времени в соответствии с целевым назначением СССН.

В условиях противодействия разрушению информации на основе оптимального интегрирования разнородных информационных процессов величина C представляет собой комбинацию трех случайных величин: $C^{(ц)}$ – объем информации, передаваемый в единицу времени в соответствии с целевым назначением СССН; $C^{(ин)}$ – объем передаваемой в единицу времени информации, идентифицирующей признаки искажения и $C^{(вк)}$ – объем передаваемой в единицу времени информации, обеспечивающей восстановление информации, подвергшейся разрушению. В этом случае имеет место выражение

$$C^{(ои)} = C^{(ц)} + C^{(ин)} + C^{(вк)}. \qquad (1.19)$$

С учетом изложенного можно сделать вывод о том, что вероятность $P\left(C \le C^{(к)}\right)$ достаточно полно характеризует особенности функционирования СССН в условиях противодействия разрушению информации, что позволяет использовать ее в качестве обобщенного показателя Э эффективности функционирования СССН в данных условиях, т. е.

$$Э = P(C \le C^{(к)}). \qquad (1.20)$$

При этом в зависимости от способа противодействия разрушению информации выражение (1.20) будет иметь вид:

$$Э^{(mp)} = P(C^{(mp)} \le C^{(к)}) = P(C^{(ц)} \le C^{(к)}) - \qquad (1.21)$$

при традиционном способе противодействия;

$$Э^{(ou)} = P(C^{(ou)} \le C^{(к)}) = P(C^{(ц)} + C^{(ин)} + C^{(вк)} \le C^{(к)}) - \qquad (1.22)$$

в условиях оптимального интегрирования разнородных информационных процессов.

Как следует из выражений (1.19) и (1.22), показатель $Э$ функционирования СССН в условиях противодействия разрушению информации является интегрированным показателем, характеризующим поведение СССН в результате реализации трех разнородных информационных процессов – процесса функционирования по целевому назначению, процесса идентификации признаков разрушения информации и процесса восстановления корректности информации, подвергшейся разрушению.

Обоснованный показатель используются далее при решении проблемы оптимального интегрирования разнородных информационных процессов в СССН в интересах противодействия разрушению информации. Содержательная и формализованная формулировка этой проблемы, а также общая схема ее решения приводятся в следующем разделе монографии.

1.6. Типовая модель сети связи специального назначения в условиях информационного конфликта

В настоящее время правоохранительные и военные системы управления наполнены элементами критической инфраструктуры и сложными аппаратно-техническими и электронными компонентами, что с одной стороны, повышает их эффективность, с другой – увеличивает их уязвимость. Для решения задач проектирования конфликто-устойчивых СССН необходимо применение математических моделей конфликта, учитывающих его динамику и целенаправленность действий каждой из сторон.

Конфликт – специфический процесс взаимодействия двух или большего количества компонентов системы (или систем в целом), преследующих разные интересы. Если интересы взаимодействующих систем (сторон) противоположны, то говорят об антагонистическом конфликте, а само взаимодействие сторон трансформируется в столкновение интересов [39]. В антагонистическом конфликте предельно высока степень противодействия, при которой достижение цели одной стороной исключает достижение цели другой стороной (компромисс невозможен).

Динамическая структура конфликта представляет собой чрезвычайно многообразный и сложный процесс. Макродинамическая модель описывает развитие конфликта в пространстве укрупненных состояний, в качестве которых выделяют противодействие, содействие, эксплуатацию и нейтралитет. Помимо этого существует конечное состояние, которое принято называть гибелью системы. Также принято полагать, что функционирование каждой из конфликтующих систем характеризуется эффективностью $E \geq 0$ (минимально возможное значение эффективности положим равным нулю), а их цель заключается в максимизации эффективности, что обозначим записью $E \rightarrow \max E$ [40].

Задачу можно представить как задачу формирования зависимости выходных показателей качества функционирования СССН от совокупности исходных данных *I*, включающей параметры СССН и обстановки. Эта зависимость строится на основании композиции известных моделей Ω_f отдельных процессов в конфликте:

$$W = f(I),\ f = f_1 \cdot f_2 \cdot \ldots \cdot f_M,\ f_i \in \Omega_f,\ i = 1,2,\ldots,M.$$

Поскольку СССН и ее элементы, участвующие в информационном конфликте, являются сложными техническими системами, функционирующими под воздействием условий внешней среды, комплекса технических средств противоборствующей стороны и системы управления комплексом противодействия, структура модели основана на декомпозиции структуры СССН и динамики конфликта.

Эталонная модель взаимодействия конфликтующих систем CSI (Conflict System Interconnection Reference Model) формализует объекты и общие подходы к описанию локальных информационных конфликтов в СССН на каждом из уровней OSI [41, 42]. В модели CSI подразумевается, что средствами вскрытия и наблюдения протоколов, используемых в системах связи, являются как средства подавления, так и новые виды информационно-технических воздействий. В модели CSI семь уровней: физический (Physical – 1), канальный (DataLink – 2), сетевой (Network – 3), транспортный (Transport – 4), сеансовый (Session – 5), представительный (Presentation – 6) и приложений (Application – 7).

Реализации модели OSI протоколами называются стеками (наборами) протоколов. В рамках одного конкретного протокола невозможно реализовать все функции модели OSI. Обычно задачи конкретного уровня реализуются одним или несколькими протоколами. На одном компьютере должны работать протоколы из одного стека. При этом компьютер одновременно может использовать несколько стеков протоколов. Модель OSI систематизирует представление об организации сетей и разбивает задачи коммуникаций на более мелкие фрагменты (подзадачи), реализуемые протоколами различных уровней. Конкретные протоколы и стеки протоколов выполняют подзадачи определенных уровней модели OSI.

Модель CSI базируется на обобщении известных моделей программно-технических и радиоэлектронных воздействий на различные элементы СССН.

В СССН, выступающей в роли объекта воздействия, необходимо рассматривать следующие составные части:

– подсистему взаимодействия элементов СССН, построенную на некотором стеке протоколов и в достаточно общем виде представляемую моделью OSI;

– подсистему защиты информации;

– подсистему управления и решения целевых задач СССН.

Фактическая работа объекта воздействия осуществляется априорно неизвестным для нарушителя программным и аппаратным обеспечением.

При этом основные протоколы обмена информацией в сетях достаточно полно описаны. Поэтому в процессе подготовки воздействия нарушителю достаточно решать задачи идентификации реализованных в СССН на основе стека протоколов. Соответственно, система создания дестабилизирующих воздействий СССН, формирующая воздействия и выступающая в роли нарушителя, должна содержать:

– подсистему управления воздействиями;

– подсистему взаимодействия с объектом воздействий;

– подсистему моделей объекта воздействий, включающую подмодели подсистем взаимодействия и защиты информации.

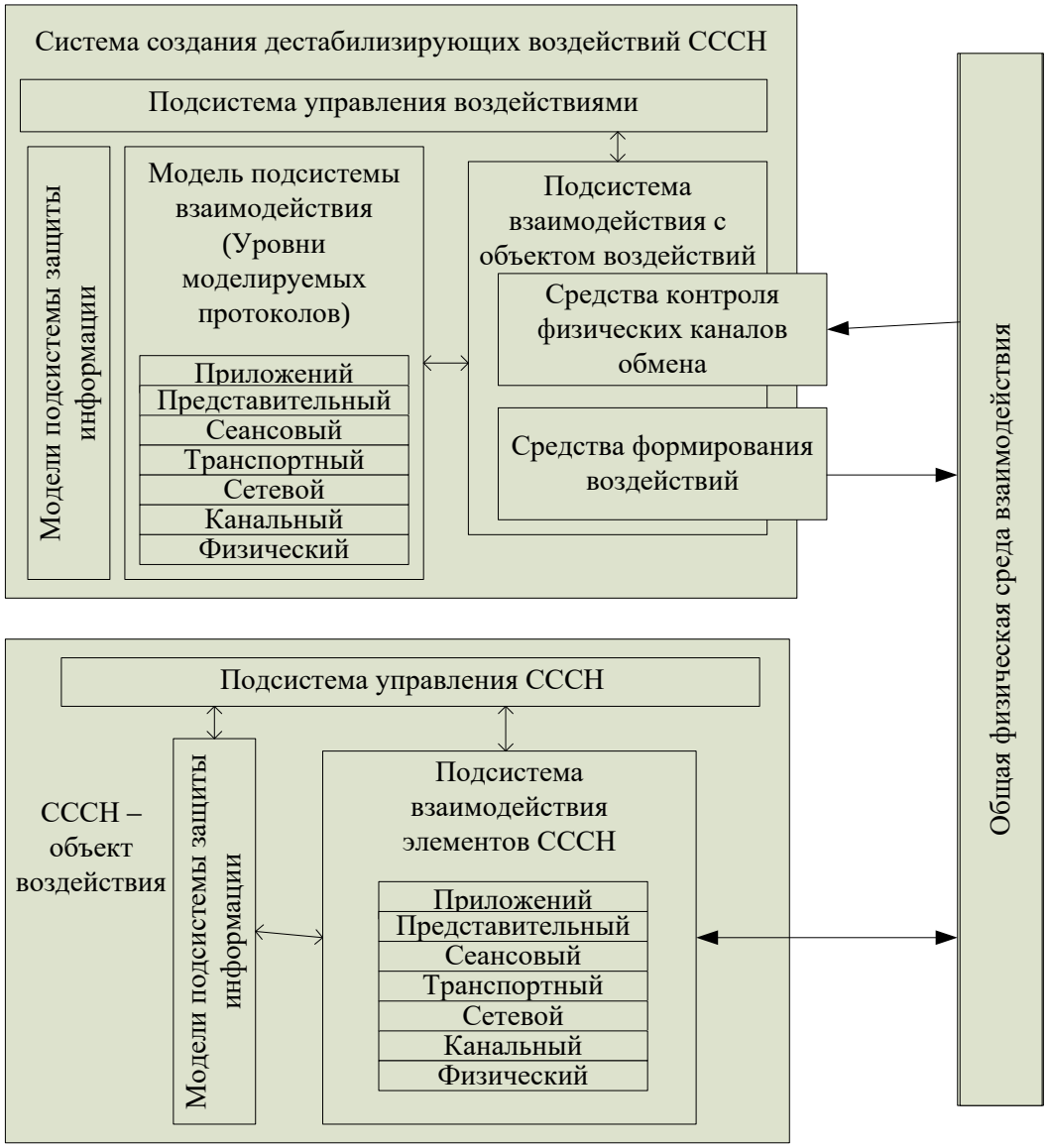


Рис. 1.5. Обобщенная модель взаимодействия конфликтующих систем CSI

Специфика данной модели заключается в том, что чем более высокого уровня протоколы удается идентифицировать или смоделировать нарушителю, тем более опасные виды воздействий могут создаваться. В самом опасном случае нарушитель может вскрыть все уровни протоколов обмена информацией и конфигурацию системы защиты информации в объекте воздействия. При этом нарушитель может создать виртуальный элемент сети, имитирующий работу легитимного пользователя или узла сети, и получить полный доступ к защищаемой системе.

1.7. Перспективные цифровые информационные технологии как техническая основа повышения эффективности и защищенности функционирования сетей связи специального назначения

Научно-технический прогресс в области системы связи МВД России проявляется в развитии инфокоммуникационной инфраструктуры, замене устаревших технических средств новыми. Основой развития системы связи являются достижения фундаментальных наук, открывающие новые физические принципы и способы функционирования устройств и систем. В современной системе радиосвязи МВД России можно выделить следующие важные направления: интеллектуализация систем радиосвязи на основе компьютерных средств и технологий; освоение в практике ОВД новых диапазонов частот; повышение роли устройств обработки информации. Усложнение функций, связанных с передачей, накоплением и обработкой информации, решается за счет устройств цифровой техники. Так, важное место в оперативной деятельности ОВД играют дежурные части. Именно в их компетенции находится получение требуемой информации о совершенных преступлениях, наличии рядом сил и средств полиции, привлекаемых для участия в расследовании. Для передачи оперативной информации от вышестоящей дежурной части к подчиненным частям в системе МВД России создана система громкоговорящего оповещения дежурных частей на базе аппаратно-программного комплекса «Мегафон-Р» с возможностью принятия информации в автоматическом режиме и дальнейшим подтверждением на интерфейсе АРМ оперативного дежурного. Оповещение реализуется через телекоммуникационные каналы МВД России. Один из важнейших этапов развития системы радиосвязи – организация устойчивых каналов передачи данных и доступа к информационным ресурсам и ведомственным информационным системам. Это возможно, например, за счет внедрения новых диапазонов частот, например при использовании спутниковых каналов передачи. Пример: в МВД Республики Татарстан реализован авторизованный доступ участковых из отдаленных сельских поселений к ресурсам ИМТС МВД России. Это обеспечено использованием спутниковых терминалов со спутниковым модемом SkyEdge 2.

Спутниковые технологии связи существенно продвинули развитие инфраструктуры связи во многих подразделениях ОВД страны. Развитие навигационной спутниковой системы ГЛОНАСС позволило внедрить в деятельность ОВД во всех регионах новые технологии, в частности автоматизировать процесс управления силами и средствами подразделений ОВД, упростить контроль за несением службы и нахождением нарядов на постах и маршрутах патрулирования. В дежурных частях появились АРМ системы управления мобильными нарядами и автотранспортными средствами. С их помощью возможно определить состав наряда, скорость, направление

движения, осуществлять контроль за ходом дежурства, архивировать историю дежурства.

Для обеспечения большой площади радиопокрытия и повышения надежности передачи данных в состав системы входит цифровая радиосеть, формирующая цифровую ретрансляцию данных от мобильных, пеших нарядов к диспетчерским центрам системы. Каждый ретранслятор принимает данные на навигационных частотах и передает данные на частоте радиосети. Радиосеть синхронизируется по принципу передачи маркера. В том случае, когда каждое устройство радиосвязи помимо функций приема и передачи сможет выполнять функции ретранслятора, появляется возможность реализации интеллектуальной самоорганизующейся радиосети. Такая сеть представляет собой структуру из многих абонентов и нескольких точек доступа к внешним сетям. Структура такой сети обладает возможностью к самостоятельному конфигурированию, в зависимости от нахождения радиосредств в зоне взаимной видимости. Информационный пакет проходит через все устройства на пути прохождения информации по маршруту. Таким образом, за счет ресурсов каждого абонента увеличивается радиус действия сети, надежность и оперативность связи. Пример: комплекс средств цифровой радиосвязи «Гранит Р-86АЦ». В основе комплекса лежит протокол «Волновая сеть» на основе множественного случайного доступа к каналу передачи данных с контролем несущей. Радиосредства самоорганизующейся сети работают в широкополосном канале и позволяют передавать информацию и речь [43].

Большинство радиосетей МВД представляют собой конвенциональные системы радиосвязи, общим недостатком которых является неэффективное использование радиочастот. В настоящее время основные производители оборудования радиосвязи предлагают новые цифровые решения для конвенциональных радиосетей. Это, прежде всего, система MOTOTRBO (европейский открытый стандарт DMR) от компании Motorola, оборудование этого же стандарта от компании Hytera, а также системы IDAS (производства Icom) и NEXEDGE (производства Kenwood). Важным отличием систем связи стандарта DMR (Motorola, Hytera) от протоколов от компаний Icom и Kenwood является принцип разделения каналов – 2-слотовый TDMA с шириной канала 12,5 кГц в стандарте DMR и FDMA с шириной канала 6,25 кГц для IDAS/NEXEDGE. Эти системы, несмотря на разный подход к реализации, предусматривают возможность системной интеграции посредством среды TCP/IP, взаимодействуют с системой спутниковой навигации и обеспечивают повышенную функциональность, недостижимую для аналоговых систем радиосвязи.

Активно внедряемые в практику МВД системы транкинговой связи предназначены для построения локальных и многозоновых сетей, предоставляющих различные виды услуг при высоком качестве связи. В частности, поддерживаются речевая связь между абонентами и группами абонен-

тов, доступ к ведомственным телефонным сетям, телефонным сетям общего пользования и сетям передачи данных (телеметрия, аварийная сигнализация, цифровые данные). Для построения системы цифро-аналоговой радиосвязи с передачей данных и голоса между абонентами по связанным зонам радиосети и диспетчеризации требуется наличие транспортной сети широкополосной передачи данных (ШПД), организованной по беспроводной, оптической или проводной технологии. Для организации внутрисистемных линий связи (межсайтовые соединения, удалённые объекты связи и прочее) в сетях УКВ-радиосвязи цифровых стандартов радиосвязи (APCO 25, DMR, IDAS) используются общепринятые, широко применяемые в органах внутренних дел интерфейсы (E1 G703, IP). Наиболее часто используются цифровые каналы, образованные с помощью волоконно-оптических линий связи (ВОЛС) или радиорелейных линий (РРЛ), реже – медные линии связи. IP-соединение ретрансляторов также может применяться для увеличения географической зоны покрытия радиосвязью.

Для подключения по IP также могут быть использованы ретрансляторы разных диапазонов. Преимуществом IP-соединения является возможность использования глобальной сети Интернет. При этом рекомендуется использовать роутеры или другие устройства, способные обеспечить функцию VPN. IP-сети находят применение не только для соединения компонентов цифровых сетей радиосвязи, но и для их интеграции с аналоговыми сетями. Например, система «Радиокупол» представляет собой специализированную RoIP-систему, разворачиваемую на базе RoIP-шлюзов, подключаемых к имеющемуся телекоммуникационному оборудованию и обеспечивающих коммутацию и диспетчеризацию аналоговой и цифровой радиосвязи [26, 47]. Для объединения зон действия разных ретрансляторов в общую зону радиопокрытия и подключения станций удалённого доступа используется опорная IP-сеть.

Инфраструктура МВД России предоставляет IP-каналы связи ИМТС (интегрированные мультисервисные телекоммуникационные системы) ОВД, построенные на базе Ethernet-сетей с использованием протоколов TCP/IP, для передачи абонентского трафика и служебной информации между базовыми станциями, АРМ диспетчера, администратора и центра управления и коммутации в любом цифровом режиме. Системы связи RoIP – это новый сегмент радиосвязи, разрабатываемый в России. RoIP является универсальной коммуникационной системой, которая преобразовывает радиосигнал в цифровые данные, подходящие для передачи по IP-сети, и наоборот. Эта система предназначена для передачи речи по локальной сети в реальном времени между компьютером и удаленными радиостанциями. Система состоит из рабочего места диспетчера и удаленных радиостанций. Радиостанция подключается к IP-сети посредством шлюза RoIP.

Основное назначение системы – обеспечение устойчивой радиосвязью объектов со сложной инфраструктурой и топологией, объединение в

одну сеть нескольких групп пользователей, использующих различный частотный ресурс; обеспечение возможности перехода на цифровые системы передачи голоса без замены и модернизации абонентского парка радиостанций. Устройство RoIP-шлюзов строится с учетом последних тенденций по созданию комплексных систем радиосвязи на основе IP-сетей для управления и информационного обеспечения различных служб общественной безопасности. Использование в системах радиосвязи ПК дает возможность без применения специальных пультов программно изменять настройки ретрансляторов и базовых станций и осуществлять по IP-сети прямой контроль над состоянием систем связи. Система RoIP связи позволяет создать единый диспетчерский центр управления подразделениями (нарядами) различных служб (с возможностью организации конференцсвязи между диспетчерами), реализовывать удаленное управление и настройку базовых станций многозоновых радиосетей. С помощью данной схемы пользователи радиостанций получают доступ к тем сервисным возможностям, которые традиционно могли использовать только абоненты сотовых сетей связи или телефонных сетей общего пользования, включая прямой вызов телефонных номеров, переадресацию вызовов, конференцсвязь, а также запись переговоров в эфире [43].

Сложность создания сетей связи нового поколения заключается в том, что сети фиксированной и мобильной связи построены по разным стандартам и используют разное программное обеспечение. В этих условиях важно, чтобы программное обеспечение предоставления сервисов не зависело от архитектуры сети и технологии доставки информации. Для построения мультисервисной сети необходимы транспортные каналы и протоколы, способные поддерживать доставку информации различного вида (речь, данные, видео) [44]. Это реализуется объединением сетей мобильной связи, IP-сетей, сетей общего пользования в единую сеть, которая интегрирует различные технологии. Для передачи данных, в том числе фото и видеотрафика, в интересах ОВД используются системы технологии широкополосного радиодоступа. Такие технологии позволяют реализовать требования системы управления ОВД и значительно увеличить ёмкость сетей за счёт использования спектрально-эффективных методов передачи данных.

В настоящее время сети МШПД в системе связи органов внутренних дел Российской Федерации предназначены для формирования гибкой транспортной инфраструктуры, позволяющей подключить как фиксированных, так и мобильных пользователей и передавать данные, телефонию, видеоинформацию в недоступных для организации проводных каналов местах, организовать подключение к ведомственным информационным ресурсам пользователей структурных подразделений МВД России (районные отделы полиции, подразделения полиции на транспорте, патрульные наряды ДПС). Указанные технологии полностью реализованы в оборудовании

радиодоступа, базирующемся на мобильных технологиях IEEE 802.16-2005 («мобильный» WiMAX) и LTE [45].

Система радиосвязи специального назначения, являясь составной частью системы связи в целом, обеспечивает перенос информации между источниками и получателями информации. В то же время современная система радиосвязи начинает включать в себя информационные устройства для поиска, хранения и сжатия, преобразования и организации доступа к источникам информации, в том числе сетевые узлы – серверы, шлюзы, терминалы. Учитывая, что источники и получатели информации также являются элементами системы радиосвязи, можно сделать вывод о конвергенции сетей радиосвязи и информационных сетей, а также взаимном влиянии технологий, то есть возникновении и реализации инфокоммуникационных систем.

Развитие инфокоммуникационных сервисов осуществляется в рамках IP-сетей, с одновременным расширением функций самих сетей связи. Важнейшими из них представляются: мультисервисность, предоставление услуг независимо от транспортных технологий; широкополосность, для гибкого изменения скорости передачи информации; мультимедийность, для передачи многокомпонентной информации. Такие требования предполагают наличие некоторой интеллектуальной надстройки, управляющей вызовами и предоставлением услуг, то есть системы радиосвязи становятся интеллектуальными. Подобная интеллектуальность реализуется в общей инфраструктуре программными средствами для управления радиосредствами.

Это позволяет определять перспективные радиосредства как программно-определяемое радио, характеристики радиосистем в этом случае не только обусловлены программным обеспечением (ПО), но и используют инфраструктуру, обычно присущую только сетям. В программно-определяемом радио программное обеспечение определяет службы и интерфейсы, которые согласуют сигнальные приложения с аппаратными средствами. Структура такого радио определяется программным обеспечением цифровой обработки сигналов. ПО характеризует функции системы и интерфейсы управления, конфигурирование приложений, формирование сигнала и его обработки. Концепция программно-определяемого радио основана на использовании объектно-ориентированных языков (C++, Java и др.). Программно-реализуемая архитектура имеет ряд преимуществ по сравнению с традиционными радиосредствами. Их применение с учетом возможностей современных цифровых сигнальных процессоров позволяет обеспечивать надежную связь и высокий уровень совместимости радиосистем. Расширяются возможности перенастройки системы, совместимость с разными аппаратными платформами. Разработка концепции программно-определяемого радио базируется на разработке инфраструктуры операционной среды. Такая среда используется для управления, настройки и регу-

лирования радиосистем, используемых в них приложений. Это позволяет модернизировать системы, то есть внедрять новые технологии и улучшать характеристики.

Стремительный прогресс в области телекоммуникационных и информационных технологий привел к возможности конвергенции разнородных сетей в единую мультисервисную сеть. Данная сеть позволит предоставлять пользователям разнородные телекоммуникационные услуги – передачу голоса, мультимедийные услуги, передачу данных и многое другое. Мультисервисные сети связи могут быть созданы непосредственно на основе как существующих цифровых, так и виртуальных сетей.

Ядром мультисервисных сетей связи (NGN, Next Generation Networks – сетей следующего поколения) являются опорные IP-сети, поддерживающие полную или частичную интеграцию услуг передачи речи, данных и мультимедиа. NGN реализует принцип конвергенции услуг электросвязи.

Пакетная коммутация, основанная на IP-технологии, реализуется в NGN, которые предназначены для предоставления услуг электросвязи и для использования нескольких широкополосных технологий транспортировки с включенной функцией QoS.

Основу сетей NGN, изначально сложившихся как NGN IPCC (International Packet Communication Consortium), составляют гибкие коммутаторы Soft switch и IP-АТС. NGN представляет собой модернизированную TDM-сеть с возможностью передачи IP-трафика, а также с дополнительными возможностями предоставления услуг для конечного пользователя. В настоящий момент в NGN на смену архитектуре IPCC приходит TISPAN, ключевым элементом которой является IMS (IP Multimedia Subsystem). Основное отличие NGN TISPAN (IMS) от NGN IPCC заключается в гибкости и масштабируемости таких сетей. В них функции управления сеансами и маршрутизацией выполняет CSCF (Call Session Control Function), пришедший на смену Soft switch. С одной стороны, сети NGN IPCC/TISPAN (IMS) предоставляют широкий набор дополнительных услуг (т.н. ДВО – дополнительные виды обслуживания), которые предоставляют возможности более эффективного управления сетью по сравнению с TDM-архитектурой. С другой стороны, такой спектр функциональных возможностей увеличивает число уязвимостей и порождает источники угроз информационной безопасности**.**

Сложность создания сетей нового поколения заключается в том, что сети фиксированной и мобильной связи построены по разным стандартам и используют разное программное обеспечение.

В этих условиях важно, чтобы программное обеспечение предоставления сервисов не зависело от архитектуры сети и технологии доставки информации.

Для построения мультисервисной сети необходимы транспортные каналы и протоколы, способные поддерживать доставку информации раз-

личного вида (речь, данные, видео). Это реализуется объединением сетей мобильной связи, IP-сетей, сетей общего пользования в единую сеть, которая интегрирует различные технологии. Функциональная модель такой сети может быть представлена транспортным уровнем, уровнем управления коммутацией и передачей информации, а также управления услугами.

Собственная мультисервисная сеть связи позволит:

– создать высокопроизводительную и помехоустойчивую технологическую основу для внедрения новых приложений, направленных на повышение уровня общественной безопасности;

– расширить возможности существующих ведомственных систем связи за счет добавления функций мобильности и мультимедийности;

– обеспечить дистанционное управление экипажами ведомственных автомобилей и двухсторонний мультимедийный цифровой радиообмен;

– организовать постоянное видеонаблюдение на территории города, в том числе с использованием мобильных объектов;

– обеспечить доступ мобильных и стационарных пользователей к информационным ресурсам и ведомственным базам данных;

– осуществить передачу телеметрической информации с мобильных и стационарных объектов;

– существенно снизить накладные расходы на аренду внешних каналов связи и телефонии.

Мультисервисная сеть связи – основа современной информационной системы связи специального назначения.

Широкие функциональные возможности NGN в сравнении с традиционными сетями, включающие открытость архитектуры; конвергентность услуг (голос, данные, видео) и сетей (ТфОП, интернета, мобильной связи); мультистандартный доступ к услугам (xDSL, Wi-Fi, WiMAX, 3G/4G/5 G); создают новые угрозы информационной безопасности или открывают более широкие возможности реализации известных угроз. Данные факторы требуют комплексного решения проблемы на основе разработки соответствующих политик безопасности и методов защиты информации, а также построения системы обеспечения информационной безопасности.

Общая архитектура информационной безопасности NGN, согласно рекомендациям МСЭ X.805, Y.2701, определяется понятиями слой и плоскость. Слои безопасности связаны с выполнением требований к сетевым элементам, образующим сквозную сеть [46]. При распределении данных требований по слоям применяется иерархический подход для достижения межконцевой безопасности за счет обеспечения безопасности каждого слоя. Архитектура информационной безопасности в этом случае включает 3 слоя (рис. 1.6):

– слой инфраструктуры – совокупность сетевых элементов (шлюзы, гибкие коммутаторы, маршрутизаторы, серверы и др.) и каналов передачи информации;

– слой услуг – совокупность сетевых услуг (услуги IP-транспорта, услуги VPN, VoIP, QoS, услуги определения местонахождения и др.);

– слой приложений – совокупность основных приложений пользователей.

Рис. 1.6. Архитектура информационной безопасности NGN

Одним из преимуществ данного подхода является возможность его многократного применения для обеспечения межконцевой безопасности различных приложений. Степень уязвимости каждого слоя различна, и, следовательно, меры противодействия определяются из задач, выполняемых каждым слоем.

Плоскости безопасности связаны с безопасностью деятельности в сетевой среде. В рамках архитектуры безопасности, по аналогии с архитектурой NGN, определяются три плоскости:

– плоскость административного управления (менеджмента) – совокупность функций эксплуатации, администрирования, технического обслуживания;

– плоскость оперативного управления – совокупность функций сигнализации для установления/разъединения соединений в сети независимо от среды передачи и телекоммуникационных технологий;

– плоскость конечного пользователя – совокупность функций доступа и использования ресурсов сети пользователями.

В соответствии с представленной архитектурой для каждого слоя и плоскости вводятся:

– функции безопасности: контроль доступа, аутентификация, конфиденциальность данных, целостность данных, неотказуемость, приватность (защищенность частной информации);

– механизмы безопасности: шифрование, цифровая подпись, управление доступом, контроль целостности данных, аутентификация, защита трафика, управление маршрутизацией, арбитраж, реализуемые соответствующими средствами информационной безопасности.

Важным требованием к архитектуре информационной безопасности NGN является соблюдение логического и физического (определяемого маршрутизацией) разделения трафика пользователей, сигнализации, управления, а также обеспечения безопасности во всех плоскостях [4].

Выводы

В главе представлены методологические вопросы анализа и синтеза построения комплексов средств противодействия угрозам информационной безопасности в сетях связи специального назначения. Систематизирован материал по проблематике противодействия сетей связи специального назначения угрозам информационной безопасности.

Представлены особенности функционирования базовой инфраструктуры сетей связи специального назначения, а также классификация информационных атак и методы их обнаружения.

Приведена модель угроз информационной безопасности сети связи специального назначения на основе формализованного построения угроз безопасности сети связи специального назначения с позиции теории множеств, с учетом сложности, неоднозначности (нечеткости), неопределенности оценки событий информационной безопасности в условиях информационного противоборства. Математическая основа построения моделей процессов информационного противоборства трудно формализуема. Сама модель строится на основе использования интеллектуальных методов, учитывающих суждения специалистов и предоставляющие окончательный результат в виде простых операций над неопределенностью, неточностью и размытостью событий информационной безопасности (теория нечетких множеств, лингвистическая неопределенность, нечеткая логика).

Изложены принципы оптимального интегрирования разнородных информационных процессов в интересах противодействия угрозам информационной безопасности в сетях связи специального назначения.

Разработан метод теории эффективности, декомпозиции и оптимизации показателей качества функционирования сетей связи специального назначения при условии защиты от разрушающих информационных воздействий.

Предложена типовая модель сети связи специального назначения в условиях информационного конфликта на основе эталонной модели взаимодействия конфликтующих систем CSI (Conflict System Interconnection Reference Model). Она формализует объекты и общие подходы к описанию

локальных информационных конфликтов в СССН на каждом из уровней OSI.

Рассмотрены особенности представления широкоплосных и сверхширокополосных импульсных сигналов с различными видами модуляции в сигнальном пространстве, применяемых в современных цифровых сетях специального назначения.

Предложены перспективные цифровые информационные технологии как техническая основа повышения эффективности и защищенности функционирования сетей связи специального назначения. Важным требованием к архитектуре информационной безопасности NGN является соблюдение логического и физического (определяемого маршрутизацией) разделения трафика пользователей, сигнализации, управления, а также обеспечения безопасности во всех плоскостях.

Глава 2.
ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ОПТИМАЛЬНОГО УПРАВЛЕНИЯ КОМПЛЕКСОМ СРЕДСТВ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕТЯХ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

2.1. Основные положения оптимального управления функционально ориентированными информационными процессами при обеспечении безопасности территориальных сегментов сети связи специального назначения

В условиях выбранного множества показателей эффективности СССН справедливы следующие утверждения:

Утверждение 1. Показатель своевременности обработки информации в компьютерной системе будет представлять собой монотонно убывающую в интервале [0, 1] функцию объема информационного пространства, реализующего процессы обработки накопления и выдачи данных.

Утверждение 2. Показатель защищенности СССН будет представлять собой монотонно убывающую в интервале [0, 1] функцию объемов информационного пространства, реализующих процессы обнаружения и парирования воздействий угроз информационной безопасности.

С целью формальной формулировки данной теоремы введем следующие обозначения:

$I^{(обр)}$ – информационное пространство, реализующее процесс обработки информации в СССН;

$I^{(н)}$ – информационное пространство, реализующее процесс накопления информации в СССН;

$I^{(обн)}$ – информационное пространство, реализующее процесс обнаружения воздействий угроз информационной безопасности в СССН;

$I^{(п)}$ – информационное пространство, реализующее процесс парирования воздействий угроз информационной безопасности в СССН;

$V^{(обр)} = V(I^{(обр)})$ – объем информационного пространства $I^{(обр)}$;

$V^{(н)} = V(I^{(н)})$ – объем информационного пространства $I^{(н)}$;

$V^{(обн)} = V(I^{(обн)})$ – объем информационного пространства $I^{(обн)}$;

$V^{(п)} = V(I^{(п)})$ – объем информационного пространства $I^{(п)}$.

В этом случае, теорему формально можно сформулировать следующим образом:

Для произвольных $V^{(обр)}_1 < V^{(обр)}_2$ ($V^{(н)}_1 < V^{(н)}_2$) будет справедливо:

$$П^{(с)}(V^{(обр)}_1) > П^{(с)}(V^{(обр)}_2),$$

а для произвольных $V^{(обн)}_1 < V^{(обн)}_2$ ($V^{(п)}_1 < V^{(п)}_2$) будет справедливо:

$$П^{(з)}(V^{(п)}_1) > П^{(з)}(V^{(п)}_2) \; (П^{(з)}(V^{(п)}_1) > П^{(з)}(V^{(п)}_2)).$$

С целью доказательства первой части сформулированной теоремы обратимся к выражению (2.1), в соответствии с которым

$$П^{(сб)}=P(\tau_{(о)} \le \tau_{(тр)}).$$

Поставим в соответствие времени $\tau_{(о)}$ обработки информации в СССН объем $V^{(онв)}$ информационного пространства, реализующего процессы обработки, накопления и выдачи данных в ней:

$$V^{(онв)} = V^{(о)} + V^{(н)}$$

т.е.

$$\tau_{(о)}(V^{(о)}, V^{(н)}) = \rho^{(о)} \cdot V^{(о)} + \rho^{(в)} \cdot V^{(н)}, \qquad (2.1)$$

где $\rho^{(о)}$ – быстродействие средств обработки информации;

$\rho^{(в)}$ – быстродействие средств выдачи данных.

Воспользуемся подобием с классическим определением функции распределения вероятностей $P(x<y)$, как вероятности того, что случайная величина $\boldsymbol{x}$ не превысит величину y. Очевидно, что для двух случайных величин x_1 и x_2, из которых $x_1 > x_2$, вероятность выполнения события $x_2<y$, при фиксированном y, больше вероятность выполнения события $x_1<y$, т.е.

$$P(x_1<y) < P(x_2<y) \text{ при } x_1 > x_2 \text{ и } y = Const. \qquad (2.2)$$

С учетом (3.1.1) и (2.2.3) условие (2.2) можно записать как

$$P(\tau_{(о)}(V^{(о)}{}_1, V^{(н)}) \le \tau_{(тр)}) < P(\tau_{(о)}(V^{(о)}{}_2, V^{(н)}) < \tau_{(тр)})$$

при $V^{(о)}{}_1 > V^{(о)}{}_2$ и $\tau_{(тр)} = Const$

и

$$P(\tau_{(о)}(V^{(о)}, V^{(н)}{}_1) \le \tau_{(тр)}) < P(\tau_{(о)}(V^{(о)}, V^{(н)}{}_2) < \tau_{(тр)})$$

при $V^{(н)}{}_1 > V^{(н)}{}_2$ и $\tau_{(тр)} = Const$,

что и требовалось доказать.

С целью доказательства второй части сформулированной теоремы обратимся к выражению, в соответствии с которым

$$П^{(з)} = P(\tau_{(п)} \le \tau_{(с)}).$$

Поставим в соответствие времени $\tau_{(п)}$ реализации функций противодействия угрозам информационной безопасности СССН объемы $V^{(обн)}$ и $\boldsymbol{V^{(п)}}$ информационных пространств, реализующих процессы обнаружения и парирования воздействий угроз информационной безопасности, соответственно, т.е.

$$\tau_{(п)}(V^{(обн)}, V^{(п)}) = \rho^{(обн)} \cdot V^{(обн)} + \rho^{(п)} \cdot V^{(п)},$$

где $\rho^{(обн)}$ – быстродействие средств обнаружения воздействий угроз информационной безопасности;

$\rho^{(п)}$ – быстродействие средств парирования воздействий угроз информационной безопасности.

Логика доказательства этой части теоремы аналогична логике доказательства первой ее части.

Теорема об экстремуме функции эффективности (теорема 2)

В условиях синтеза функционально ориентированных информационных процессов в СССН справедливо следующее утверждение:

Существует экстремум эффективности СССН как функции объема информационного пространства, реализующего процесс обнаружения воздействий угроз ее информационной безопасности.

С целью формальной формулировки данной теоремы обозначим:

$$I^{(кс)} = \mathcal{B}(I^{(обр)}, I^{(н)}, I^{(обн)}, I^{(п)}) -$$

синтезированное информационное пространство СССН.

Формально теорема формулируется следующим образом:

$$\text{при } I^{(кс)} = \mathcal{B}(I^{(обр)}, I^{(н)}, I^{(обн)}, I^{(п)}) \ \exists \operatorname{extr}[П^{(с)}(V^{(обн)})].$$

С целью доказательства теоремы воспользуемся представлением $П^{(с)}$ в виде выражения, которое, с учетом введенных в данном параграфе обозначений, имеет вид:

$$П^{(с)}{}_{(син)}(V^{(обн)}) = P\{(1-P_{(у)})\cdot(\rho^{(о)}\cdot V^{(о)} + \rho^{(в)}\cdot V^{(н)}) + \rho^{(обн)}\cdot V^{(обн)} + P_{(у)}[(1- П^{(з)}{}_{(син)})\cdot \tau_{(у)}] \le \tau_{(тр)}\}. \quad (2.3)$$

Воспользовавшись некоторыми результатами интегрирования разнородных информационных процессов [53] представим $П^{(з)}{}_{(син)}$ в виде:

$$\Pi^{(з)}_{(син)} = 1 - \left(1 - \frac{\omega\cdot\log_2\Omega\left(I^{(обн)}\right)}{\omega\cdot\log_2\left(\Omega\left(I^{(обр)}\right)+\Omega\left(I^{(н)}\right)\right)+\omega\cdot\log_2\Omega\left(I^{(обн)}\right)}\right)^{\frac{V^{(обр)}+V^{(н)}}{V^{(обн)}}},$$

где ω – количество уникальных терминов (словарь) информационного пространства $I^{(кс)}$;

$\Omega(I)$ – общее число терминов информационного пространства $\boldsymbol{I}$.

Тогда выражение (2.3) можно представить в виде

$$П^{(с)}{}_{(син)}(V^{(обн)}) = P\{(1 - P_{(у)})\cdot(\rho^{(о)}\cdot V^{(о)} + \rho^{(в)}\cdot V^{(н)}) + \rho^{(обн)}\cdot V^{(обн)} + P_{(у)}\cdot\left(1 - \frac{\omega\cdot\log_2\Omega\left(I^{(обн)}\right)}{\omega\cdot\log_2\left(\Omega\left(I^{(обр)}\right)+\Omega\left(I^{(н)}\right)\right)+\omega\cdot\log_2\Omega\left(I^{(обн)}\right)}\right)^{\frac{V^{(обр)}+V^{(н)}}{V^{(обн)}}}\cdot\tau_{(у)}] \le \tau_{(тр)}\}. \quad (2.4)$$

Введем следующие обозначения:

$$a = (1-P_{(у)})\cdot(\rho^{(о)}\cdot V^{(о)} + \rho^{(в)}\cdot V^{(н)}),$$

$$b = \rho^{(обн)},$$

$$x = V^{(обн)},$$

$$c = P_{(у)}\ \tau_{(у)},$$

$$d = \left(1 - \frac{\omega\cdot\log_2\Omega\left(I^{(обн)}\right)}{\omega\cdot\log_2\left(\Omega\left(I^{(обр)}\right)+\Omega\left(I^{(н)}\right)\right)+\omega\cdot\log_2\Omega\left(I^{(обн)}\right)}\right),$$

$$e = V^{(обр)} + V^{(н)}$$

и представим (2.4) в виде:

$$П^{(с)}{}_{(син)}(V^{(обн)}) = P\{y \le \tau_{(тр)}\}, \quad (2.5)$$

где $y=a+b\cdot x+c\cdot d^{\frac{e}{x}}$.

Продифференцируем y по x и определим соответствующие производные. В результате получим выражение:

$$y'=(a+b\cdot x)'+(c\cdot d^{\frac{e}{x}})'=b-c\cdot e\cdot ln(d)\cdot d^{\frac{e}{x}}\cdot\frac{1}{x^2}. \qquad (2.6)$$

Приравняв правую часть (2.6) нулю, получим

$$bx^2-c\cdot e\cdot ln(d)\cdot d^{\frac{e}{x}}=0. \qquad (2.7)$$

Обозначив $B=l\cdot ln(d)$, $A=\frac{c}{b}\cdot B$,

представим (2.7) в виде $x^2-A\cdot e^{\frac{B}{x}}=0$.

Введя обозначения $z=\frac{B}{x}$ и представив x в виде $x=\frac{B}{z}$,

окончательно получим $\frac{B^2}{z^2}=A\cdot e^z$.

Полученное уравнение является трансцендентным и решается известными численными методами [7]. При этом, исходя из физического смысла величины $x=V^{(обн)}$, из двух возможных корней уравнения (2.7) выбирается не равный нулю или неотрицательный (рис. 2.1).

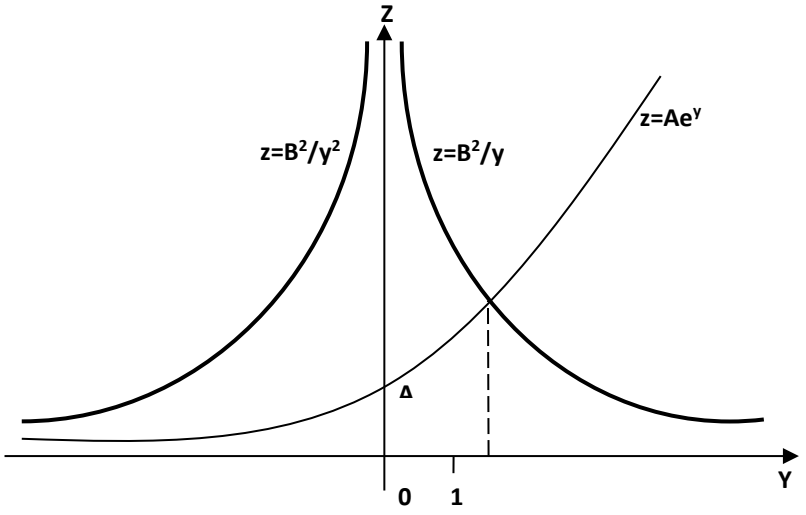


Рис. 2.1. Корни исследуемого уравнения

Из этого следует, что экстремум зависимости времени обработки информации в СССН органа государственной власти, органа, осуществляющего функции обороны страны, безопасности государства и обеспечения правопорядка, как функции объема информационного пространства, реали-

зующего процесс обнаружения воздействий угроз ее информационной безопасности, существует, т.е.

$$x_{(ext)} = \arg\{\mathrm{extr}[П^{(с)}(V^{(обн)})]\}. \qquad (2.8)$$

Тогда, на основании теоремы 1 о монотонности функции (2.5) будет существовать и экстремум зависимости эффективности СССН как функции объема информационного пространства, реализующего процесс обнаружения воздействий угроз ее информационной безопасности, что и требовалось доказать.

2.2. Метод оценки ресурса безопасности территориальных сегментов сети связи специального назначения

Методической основой для определения оптимального информационного объема СССН, за счет которого реализуется обнаружение воздействий угроз информационной безопасности, является сформулированная в п. 2.1 теорема 2. Определим этот объем как ресурс безопасности СССН. В соответствии с положениями теоремы 2 оптимальным объемом $V_{(opt)}^{(обн)}$ считается объем, полученный на основе (2.5), соответствующий экстремуму (максимуму) функции эффективности СССН, т.е.

$$V_{(opt)}^{(обн)} = x_{(ext)},$$

где $x_{(ext)}$ соответствует (2.8).

Ресурс безопасности СССН в этом случае определяется согласно выражению

$$\Delta = П^{(с)}(V_{(opt)}^{(обн)}) - П^{(с)}(0). \qquad (2.9)$$

Графическая иллюстрация рассмотренного метода приведена на рис. 2.2.

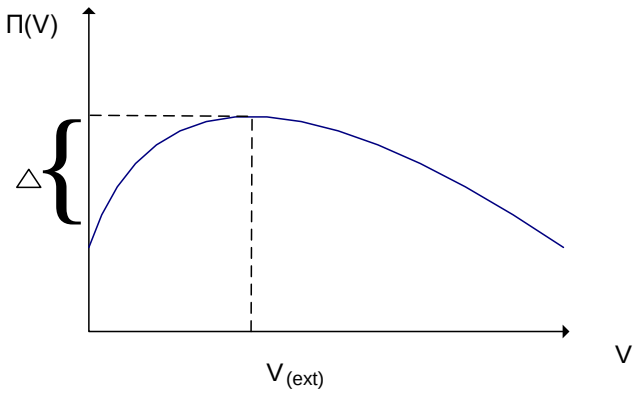


Рис. 2.2. Определение ресурса безопасности СССН

Метод оптимального распределения ресурса безопасности СССН с целью реализации в виде средств обнаружения воздействий угроз ее информационной безопасности рассматривается в следующем разделе.

2.3. Метод оптимального распределения ресурса безопасности территориальных сегментов сети связи специального назначения

Известно, что решение любой оптимизационной задачи сопряжено с необходимостью определения целевой функции и функции ограничений. В рассматриваемом случае в качестве таких функций выступают показатель эффективности функционирования СССН территориального органа государственной власти (органов, осуществляющих функции обороны страны, безопасности государства и обеспечения правопорядка) и показатель ее защищенности [50, 35].

С целью решения поставленной задачи определим соответствующий ресурсу безопасности СССН временной ресурс [50]:

$$\Delta\tau_{(o)} = \psi(\Delta), \qquad (2.10)$$

который в дальнейшем будем называть отвлекаемым.

Необходимым и достаточным условием решения поставленной задачи оптимального распределения ресурса безопасности СССН является соблюдение условия:

$$\Delta\tau_{(o)} > 0.$$

С целью формализации этой задачи под j – ым вариантом использования вычислительного ресурса СССН формально условимся понимать определенную совокупность B_j данных, характеризующих его распределение между функциями защиты информации с целью использования разнотипными подходами к организации защиты информации. Обозначив множество возможных вариантов использования временного ресурса СССН через

$$B = \{B_j \mid B_j \in B,\ j = \overline{1,|B|}\},$$

где $|B|$ – число вариантов во множестве B, а значение показателя (2.11) используемого временного ресурса при варианте B_j через $\tau_{(o)}(B_j)$, формально решаемую задачу представим в виде

$$\Delta\tau_{(ou)}(B_j) \to \min, B_j \in B,\ j = \overline{1,|B|},$$

при $\overline{E}^{(p)}_{(зи)} \geq \overline{E}^{(m)}_{(зи)}$, где $\overline{E}^{(p)}_{(зи)}$ – достигаемое значение показателя эффективности защиты информации, а $\overline{E}^{(m)}_{(зи)}$ – его требуемое значение.

Сформулированную задачу целесообразно решать путём декомпозиции и представления в виде следующих основных последовательно решаемых частных задач:

– определение ограничений при распределении временного ресурса между разнотипными подходами к организации защиты информации;

– разработка алгоритма определения минимального уровня отвлечения временного ресурса при использовании этих подходов.

В основу способа определения ограничений положена гипотеза о

том, что возможности средств защиты информации того или иного типа определяются исходя из частоты их использования и значимости.

Это приводит к необходимости оценки соответствующих возможностей средств защиты информации того или иного типа. В качестве такой оценки предлагается использовать частотную характеристику процесса защиты информации в СССН. В дальнейшем в качестве такой характеристики условимся использовать вектор $\vec{W}$ вероятностей выполнения задач защиты информации средствами защиты информации придаваемого и встраиваемого типа, формально представляемый в виде

$$\vec{W} = (w_1, w_2),$$

где w_1 и w_2 – вероятности выполнения задач защиты информации средствами защиты информации придаваемого и встраиваемого типа соответственно.

С учетом того, что данные вероятности описывают полную группу событий, будет справедливым условие:

$$w_1 + w_2 = 1.$$

Наиболее удобной формой получения этих вероятностей является имитационное моделирование процессов обработки информации в СССН в условиях противодействия угрозам информационной безопасности.

Соответствующая схема моделирования предполагает имитацию рассмотренных выше процессов на заданном интервале. В результате формируется множество

$$Q^{(y)} = \left\{ q_s^{(y)}, s = 1, 2, \ldots, S \right\}$$

инициированных воздействий угроз информационной безопасности.

Обозначив через $Q'^{(y)}$ подмножество элементов $Q^{(y)}$, обслуживание которых производилось средствами защиты информации придаваемого типа, а через $Q''^{(y)}$ подмножество элементов $Q^{(y)}$, обслуживание которых производилось средствами защиты информации встраиваемого типа, частотную характеристику процесса защиты информации в СССН запишем в виде частоты появления соответствующих угроз, что при $S \to \infty$ можно интерпретировать соответствующими вероятностями:

$$w_1 = \frac{\left|Q'^{(y)}\right|}{\left|Q^{(y)}\right|}, \; w_2 = \frac{\left|Q''^{(y)}\right|}{\left|Q^{(y)}\right|}.$$

С учетом изложенного требуемая вероятность реализации задач защиты информации средствами придаваемого типа определяется в соответствии с выражением

$$E_{(тр)}^{(пр)} = w_1 \cdot \xi_1,$$

где ξ_1 – важность (значимость) задач защиты информации СЗИ придаваемого типа, определяемая методом непосредственной оценки.

Требуемая вероятность реализации функций защиты информации средствами встраиваемого типа определяется в соответствии с выражением

$$E_{(тр)}^{(вс)} = w_2 \cdot \xi_2,$$

где ξ_2 – важность задач защиты информации решаемых средствами встраиваемого типа.

Обобщенная требуемая вероятность защиты информации в СССН определяется в соответствии с выражением:

$$E_{(зи)}^{(тр)} = E_{(тр)}^{(пр)} \cdot E_{(тр)}^{(вс)}.$$

С целью определения текущих значений ограничений на решение оптимизационной задачи формально представим механизм организации защиты информации разнотипными средствами следующим образом.

На рис. 2.3. формально представлен механизм организации защиты информации средствами придаваемого типа.

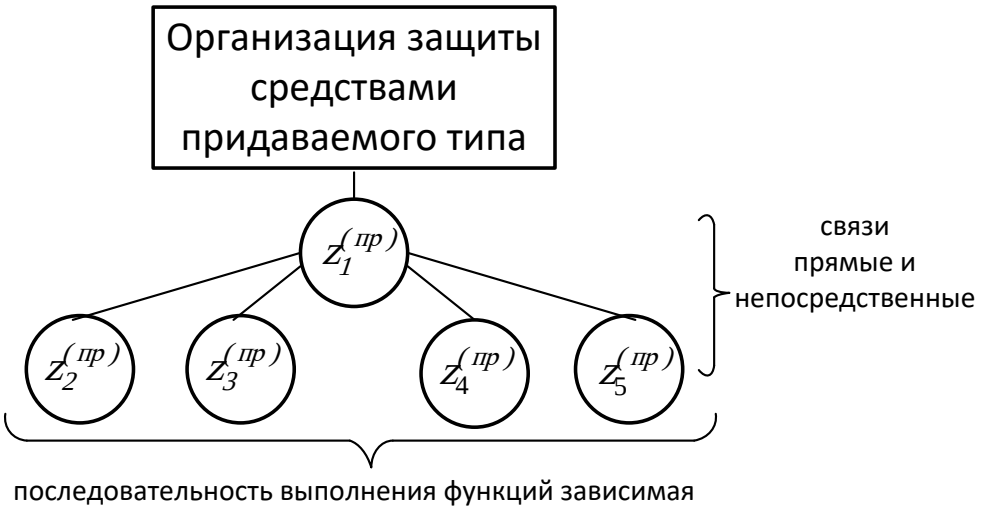


Рис. 2.3. Структурная схема механизма организации защиты средствами придаваемого типа

Как следует из рисунка совокупность элементарных событий при реализации данного механизма защиты информации является зависимой. Это дает основание полагать, что обобщенный показатель эффективности защиты информации в СССН средствами придаваемого типа определяется в соответствии с выражением:

$$E_{(зи)}^{(пр)} = 1 - (1 - E_{(зи)1}^{(пр)} E_{(зи)2}^{(пр)})^{\lambda_2} \cdot (1 - E_{(зи)1}^{(пр)} E_{(зи)3}^{(пр)})^{\lambda_3} \times$$

$$\times (1 - E_{(зи)1}^{(пр)} E_{(зи)5}^{(пр)})^{\lambda_5} = 1 - \prod_{i=2}^{5} (1 - E_{(зи)1}^{(пр)} E_{(зи)i}^{(пр)})^{\lambda_i}, \qquad (2.12)$$

где $E^{(пр)}_{(зи)\,i}$ – эффективность соответствующей функции защиты.

λ_i – индикатор отвлечения вычислительного ресурса за счет использования i – й задачи, определяемое для $i = 2,3,4,5$ согласно выражению:

$$\lambda_i = \begin{cases} 1, & \textit{если } i-\textit{я задача защиты информаци используется}, \\ 0, & \textit{в противном случае}, \end{cases}$$

в то время как λ_1 всегда равен 1.

На рисунке 2.4. формально представлен механизм организации защиты информации средствами встраиваемого типа.

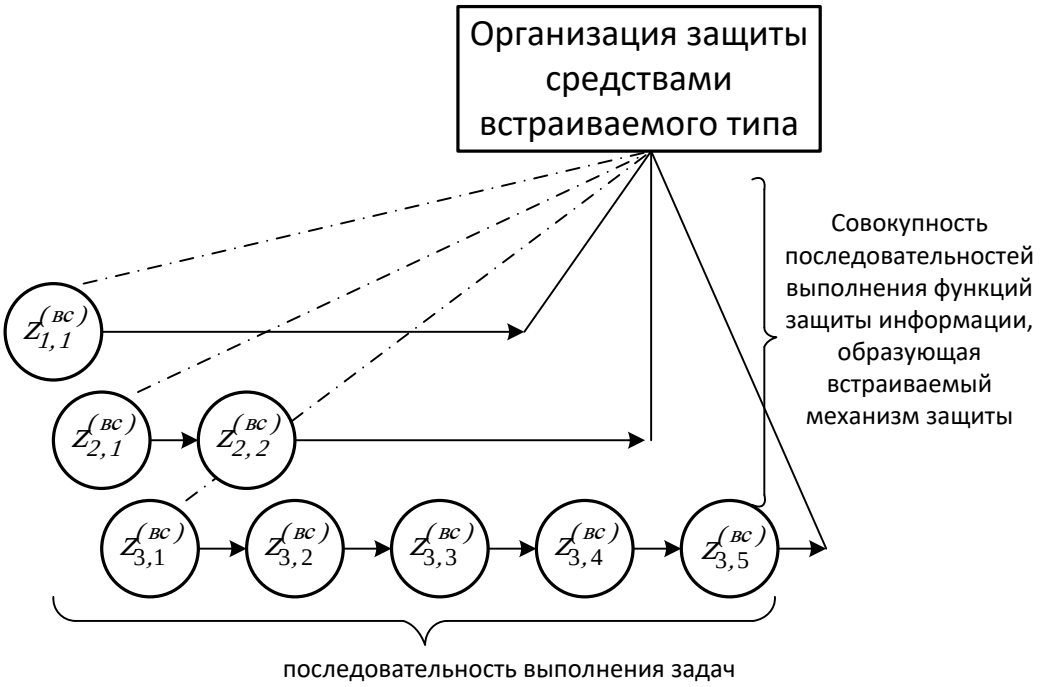


Рис. 2.4. Структурная схема механизма организации защиты средствами встраиваемого типа

Как видно из рисунка, схема организации защиты средствами встраиваемого типа может быть реализована путем выполнения одной или нескольких последовательностей функций защиты информации, обеспечивающих механизм данного типа защиты. Совокупность элементарных событий по реализации таких последовательностей является независимой. В этом случае эффективность противодействия защиты информации при реализации j-й, $j = 1,2,3$, последовательности функций защиты средствами данного типа определяется в соответствии с выражением

$$E^{(вс)}_{(зи)} = 1-(1-E^{(вс)}_{(зи)1})^{\mu_1}\cdot(1-E^{(вс)}_{(зи)1}\cdot E^{(вс)}_{(зи)2})^{\mu_2}\cdot \\ \cdot(1-E^{(вс)}_{(зи)1}E^{(вс)}_{(зи)2}E^{(вс)}_{(зи)3}E^{(вс)}_{(зи)4}E^{(вс)}_{(зи)5})^{\mu_3}, \qquad (2.13)$$

в котором μ_1 – индикатор отвлечения вычислительного ресурса за счет использования функции контроля процесса обработки информации;

μ_2, μ_3 – индикаторы отвлечения вычислительного ресурса за счет использования задач выявления и подавления угроз информационной безопасности, определяемые по формуле

$$\mu_{2(3)} = \begin{cases} 1, & \textit{если задача используется}; \\ 0, & \textit{в противном случае}, \end{cases}$$

в то время как μ_1 всегда равен 1.

Рассмотренные ограничения используются при решении оптимизационной задачи по минимизации отвлечения вычислительного ресурса компьютерной системы в условиях противодействия угрозам информационной безопасности разнотипными средствами защиты информации.

Наиболее приемлемыми в этом плане являются задачи математического программирования [35], ввиду следующих условий:

– показатель эффективности представляет собой функцию от элементов решения;

– ограничительные условия, налагаемые на возможные решения, имеют вид равенств или неравенств.

Рассмотрим в этом контексте данную оптимизационную задачу.

Имеется пять функций $z_i^{(пр)}$, $i = 1, 2, \ldots, 5$ защиты информации, реализуемых придаваемыми средствами защиты информации, и пять функций $z_j^{(вс)}$, $j = 1, 2, \ldots, 5$ защиты информации, реализуемых встраиваемыми средствами:

$z_1^{(пр)}$ – разграничение доступа к вычислительным ресурсам СССН;

$z_2^{(пр)}$ – разграничение полномочий пользователей;

$z_3^{(пр)}$ – преобразование данных;

$z_4^{(пр)}$ – контроль последствий влияния угроз информационной безопасности в СССН;

$z_5^{(пр)}$ – поддержание целостности вычислительной среды;

$z_1^{(вс)}$ – контроль процесса обработки информации на предмет его подверженности угрозам информационной безопасности;

$z_2^{(вс)}$ – выявление угроз информационной безопасности;

$z_3^{(вс)}$ – подавление угроз информационной безопасности;

$z_4^{(вс)}$ – идентификация последствий воздействия угроз информационной безопасности в СССН;

$z_5^{(вс)}$ – оперативное восстановление информационных процессов, подвергнутых воздействию угроз информационной безопасности.

Требуется таким образом распределить вычислительный ресурс СССН между функциями защиты информации, выполняемыми разнотипными средствами, чтобы достичь его минимального отвлечения, обеспечив требуемый уровень ее защиты $E_{(зи)}^{(тр)}$.

Обозначим через $\lambda_i, i=1,2,\ldots,5$ коэффициенты отвлечения вычислительного ресурса компьютерной системы средствами защиты информации придаваемого типа при реализации ими соответствующих функций защиты информации.

Соответствующий i – й функции защиты информации объем вычислительного ресурса обозначим через $x_i, i=1,2,\ldots,5$.

Обозначим через μ_2 и μ_3 коэффициенты отвлечения вычислительного ресурса компьютерной системы средствами встраиваемого типа при решении ими функций выявления и подавления угроз информационной безопасности СССН соответственно.

Обозначим через y_1 объем вычислительного ресурса, отвлекаемый для реализации функции $z_1^{(вс)}$, через y_j, $j=1,2$, отвлекаемый для реализации цепочки функций защиты $z_1^{(вс)}$, $z_2^{(вс)}$, а через y_l, $l=1,2,\ldots,5$, объем вычислительного ресурса, отвлекаемый для реализации цепочки функций в виде последовательности всех функций средствами встраиваемого типа.

Объем отвлекаемого при этом вычислительного ресурса составит

$$\tau_{(р)} = \sum_{i=1}^{5} \lambda_i \cdot x_i + \mu_1 \cdot y_1 + \mu_2 \sum_{j=1}^{2} y_j + \mu_3 \sum_{l=1}^{5} y_l \,. \qquad (2.14)$$

В свою очередь, уровень эффективности защиты информации в СССН, обеспечиваемый при реализации задач средствами обоих типов, не должен быть меньше $E_{(зи)}^{(тр)}$, откуда получаем условие-неравенство

$$\Delta \geq E_{(зи)}^{(mp)}, \qquad (2.15)$$

в котором Δ определяется согласно (2.9).

Входящие в выражения (2.14) и (2.15) коэффициенты λ_i, μ_1, μ_2 и μ_3 характеризуют степень влияния вычислительного ресурса, отвлекаемого при реализации соответствующих функций защиты информации на эффективность защиты.

Эти условия представляют собой ограничения, накладываемые на решение оптимизационной задачи.

Таким образом, решаемая задача имеет следующую формулировку:

Выбрать такие неотрицательные значения переменных $\lambda_i, i=1,2,\ldots,5$, μ_1, μ_2 и μ_3, удовлетворяющие неравенству (2.15), при которых функция этих переменных (2.14) обращалась бы в минимум.

Поставленная задача представляет собой задачу математического программирования и решается известными методами.

2.4. Реализация ресурса безопасности территориальных сегментов системы связи специального назначения

В соответствии с существующими способами обнаружения воздействий угроз информационной безопасности на СССН временной резерв дифференцируется по типам: функциональный (Ф), алгоритмический (А) и технический (Т). При этом Ф-резерв обеспечивает возможность контроля информации в СССН за счет введения соответствующих функций в процедуры информационного процесса, А-резерв обеспечивает возможность контроля отдельных функций информационного процесса путем проверки логики их выполнения, Т-резерв обеспечивает возможность контроля временных, структурных и информационных параметров вычислительной среды СССН.

Обозначим через $\Delta\tau^{(\phi)}$, $\Delta\tau^{(a)}$, $\Delta\tau^{(m)}$ соответствующие перечисленным выше типам ресурса СССН его части, для которых выполняется условие:

$$\Delta\tau = \Delta\tau^{(\phi)} + \Delta\tau^{(a)} + \Delta\tau^{(m)},$$

и запишем их в виде выражений

$$\Delta\tau^{(\phi)} = d^{(\phi)} \cdot \Delta\tau, \quad \Delta\tau^{(a)} = d^{(a)} \cdot \Delta\tau, \quad \Delta\tau^{(m)} = d^{(m)} \cdot \Delta\tau, \qquad (2.16)$$

в которых $d^{(\phi)}$, $d^{(a)}$ и $d^{(m)}$ – соответствующие доли уровня R временного ресурса.

Распределение ресурса по типам предлагается осуществлять на основе разработанного алгоритма лингвистической идентификации Ф-, А- и Т-ресурса, основанного на понятии лингвистической переменной [51]. Для описания этого алгоритма определим лингвистическую переменную РЕСУРС. Ее количественной мерой служат значения базовой переменной [52] d, определяющие доли типов резерва. Областью изменения d является универсальное множество $D = [0,1]$. На этом множестве определим терм-множество:

$$L = \left\{ l^{(\phi)}, l^{(a)}, l^{(m)} \right\},$$

в котором нечеткие переменные термы $l^{(\phi)}$, $l^{(a)}$ и $l^{(m)}$ описываются кортежем

$$l^{(q)} = \left\langle \mathrm{N}^{(q)}, D^{(q)}, \mathrm{M}^{(q)} \right\rangle.$$

Его элементами являются:

$\mathrm{N}^{(q)}$ – наименование q-го терма (ФУНКЦИОНАЛЬНЫЙ, АЛГОРИТМИЧЕСКИЙ, ТЕХНИЧЕСКИЙ);

$D^{(q)} = \left[d_1^{(q)}, d_2^{(q)} \right]$ – область определения нечеткой переменной $d^{(q)}$ $D^{(q)} \subset D$; ограниченная слева и справа значениями $d_1^{(q)}$ и $d_2^{(q)}$ соответственно;

$\mathrm{M}^{(q)}$ – нечеткое множество на $D^{(q)}$, описывающее ограничения на смысл нечеткой переменной в соответствии с выражением

$$\mathrm{M}^{(q)} = \bigcup_{d \subset D} \mu^{(q)}(d)/d,$$

в котором $\mu^{(q)} : d^{(q)} \to D^{(q)}$ – функция принадлежности $d^{(q)}$ к $D^{(q)}$.

При построении $\mu^{(\phi)}$, $\mu^{(a)}$ и $\mu^{(m)}$ воспользуемся алгоритмом, модифицировав его следующим образом:

1) при построении функции принадлежности $\mu^{(\phi)}$ терма $l^{(\phi)}$ значения d изменяются от нуля вправо, вследствие чего $d_1^{(\phi)}$ всегда равно нулю;

2) при построении функции принадлежности $\mu^{(m)}$ терма $l^{(m)}$ значения d изменяются от единицы влево, вследствие чего $d_2^{(m)}$ всегда равно единице;

3) при построении функции принадлежности $\mu^{(a)}$ терма $l^{(a)}$ значения d изменяются симметрично влево и вправо относительно значения $\left(d_2^{(\phi)} - d_1^{(m)}\right)/2$.

Получаемые с помощью такого подхода функции принадлежности $\mu^{(\phi)}$, $\mu^{(a)}$ и $\mu^{(m)}$ лингвистической переменной РЕСУРС имеют вид, показанный на рис. 2.5, на котором представлен и один из возможных вариантов определения значений $d^{(\phi)}$, $d^{(a)}$ и $d^{(m)}$ для идентификации типа ресурса согласно соотношением (2.16).

При построении функций принадлежности лингвистической переменной РЕСУРС для произвольных значений уровня резерва R необходимо учитывать ряд соотношений между размерами областей определения $D^{(q)} = \left[d_1^{(q)}, d_2^{(q)}\right]$ нечеткой переменной $l^{(q)}$ и значениями R. Основные из них заключаются в следующем. При малых значениях должна преобладать область $D^{(m)}$ определения терма $l^{(m)}$. Увеличение значений R должно сопровождаться расширением областей $D^{(\phi)}$и $D^{(a)}$ определения термов $l^{(\phi)}$, $l^{(a)}$ и уменьшением области $D^{(m)}$ определения терма $l^{(m)}$.

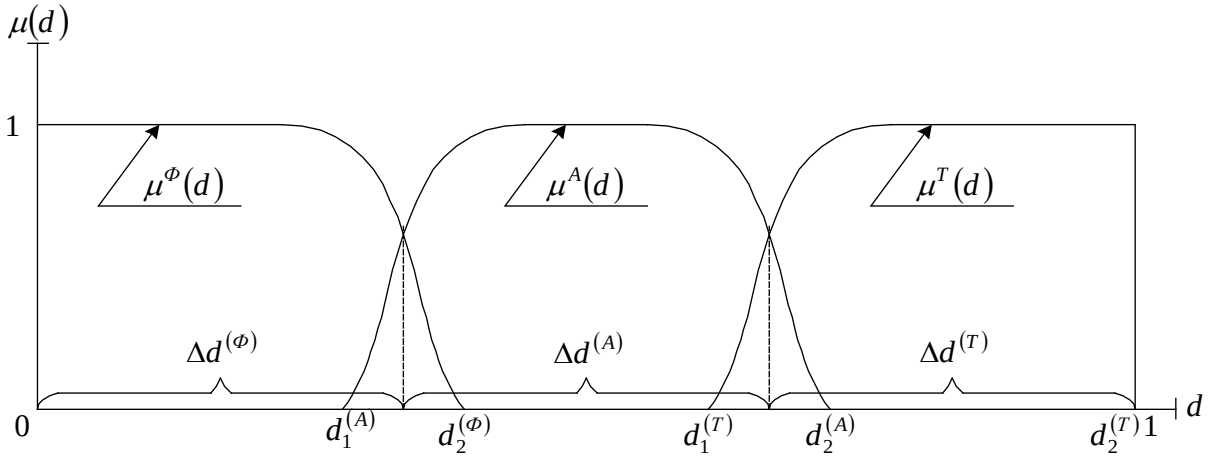


Рис. 2.5. Типовые функции принадлежности $\mu^{(\phi)}$, $\mu^{(a)}$ и $\mu^{(m)}$ лингвистической переменной РЕСУРС

С учетом изложенного для идентификации типов временного резерва предлагается строить функцию принадлежности $\mu^{(\phi am)}$ от двух переменных R и d, т.е. в виде

$$\mu^{(\phi am)} = \mu^{(\phi am)}(R, d), \tag{2.17}$$

описывающем некоторую поверхность принадлежности в системе координат $\mu^{(\phi am)}$, R, d. С этой целью область определения значений уровней резерва R обозначим через $R = \lfloor 0, R_{(\max)} \rfloor$, где $R_{(\max)}$ – максимально возможное значение R, и определим прямоугольник $\Omega = R \times D$. С помощью одномерных сеток

$$\eta_n^{(1)}: \quad 0 = R_0 < R_1 < R_2 < \cdots < R_n = R_{(\max)},$$

$$\eta_m^{(2)}: \quad 0 = d_0 < d_1 < d_2 < \cdots < d_m = 1$$

разобьем прямоугольник Ω на частные прямоугольники:

$$\omega_{kj} = [R_k, R_{k+1}] \times \lfloor d_j, d_{j+1} \rfloor, \; k = 0, 1, 2, \ldots, n-1; \quad j = 0, 1, 2, \ldots, m-1.$$

Для каждого узла сетки в соответствии с рассмотренным выше подходом построим функцию принадлежности $\mu^{(\Phi)}(R_k, d)$ терма $l^{(\phi)}(R_k)$ и определим ее значения $\mu_{kj}^{(\phi)}$ в узлах сетки $\eta_m^{(2)}$, т.е.

$$\mu_{kj}^{(\phi)} = \mu^{(\phi)}(R_k, d_j), \; j = 0, 1, 2, \ldots, m.$$

Применительно к полученному таким образом набору значений $\mu_{kj}^{(\phi)}(R_k, d_j), l = 0, 1, 2, \ldots, n, \quad j = 0, 1, 2, \ldots, m$, далее решается задача сглаживания функций двух переменных. Формально эта задача ставится как задача отыскания функции $\mu^{(\phi)} = \mu^{(\phi)}(R, d)$, обеспечивающей минимум функционала

$$\Psi\left(\mu^{(\phi)}(R,d)\right)=\sum_{k=0}^{n}\sum_{j=0}^{m}\psi_{kj}\left(\mu_{kj}^{(\phi)}-\mu^{(\phi)}\left(R\ ,d\ \right)\right)^2+\psi\int_0^{R(\max)}\int_0^1\left(\frac{\partial\mu^{(\phi)}(R,d)}{\partial R}\right)^2+\left(\frac{\partial\mu^{(\phi)}(R,d)}{\partial d}\right)^2 \mathrm{d}R\mathrm{d}d\,,$$

в котором $\psi_{kj}>0$ и $\psi\geq 0$ – заданные числа, и решается известным методом.

Получаемая таким образом функция принадлежности $\mu^{(\phi)}=\mu^{(\phi)}(R,d)$ терма $l^{(\phi)}$ лингвистической переменной РЕСУРС описывает соответствующую ему поверхность принадлежности. Ее возможный вид показан на рис. 2.6, а.

Аналогичным образом на прямоугольнике Ω строятся функции принадлежности $\mu^{(a)}=\mu^{(a)}(R,d)$ и $\mu^{(m)}=\mu^{(m)}(R,d)$ термов $l^{(a)}$ и $l^{(m)}$. Возможный вид соответствующих им поверхностей принадлежности показан на рис. 2.6, б и рис. 2.6, в соответственно.

Принимая во внимание, что прямоугольник Ω является областью определения всех трех построенных таким образом функций принадлежности, совокупность соответствующих им поверхностей принадлежности формально условимся описывать выражением

$$\mu^{(\phi am)}=\left(\mu^{(\phi)}(R,d),\mu^{(a)}(R,d),\mu^{(m)}(R,d)\right), \qquad (2.18)$$

которое определяет вид функций принадлежности (рис. 2.7).

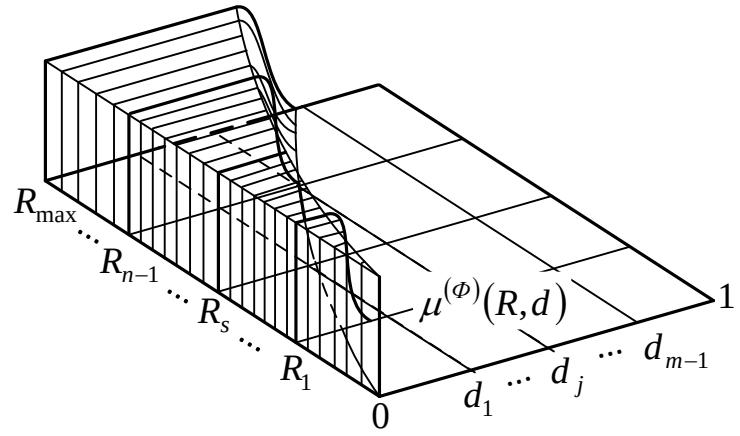
Лингвистическая идентификация типов резерва для i - ой, $i=1,2,...,|\mathrm{A}|$, процедуры информационного процесса с использованием построенной таким образом функции $\mu^{(\phi am)}$ осуществляется на основе следующего методического подхода. Вначале определяется уровень временного резерва r_i по формуле

$$r_i=\frac{\Delta\tau_i^{(opt)}}{\tau_i}$$

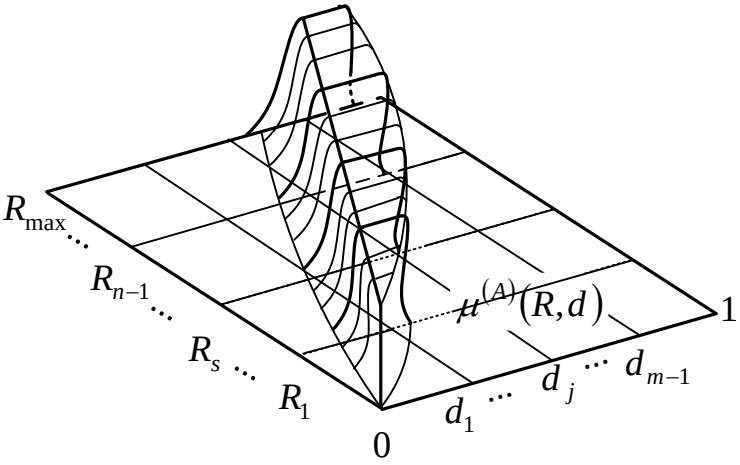
и рассматривается соответствующее ему сечение поверхности принадлежности, описываемой выражением (2.18), плоскостью $\mu^{(\phi am)}=\mu^{(\phi am)}(r_i,d)$.

Возможный вид функций принадлежности $\mu_i^{(\phi)}=\mu^{(\phi)}(r_i,d)$, $\mu_i^{(a)}=\mu^{(a)}(r_i,d)$ и $\mu_i^{(m)}=\mu^{(m)}(r_i,d)$ в плоскости $\mu^{(\phi am)}$ показан на рис. 2.7. Далее, учитывая, что области $D^{(\phi)}$, $D^{(a)}$ и $D^{(m)}$ изменения значений базовой переменной d функций принадлежности $\mu^{(\phi)}$, $\mu^{(a)}$ и $\mu^{(m)}$ термов $l^{(\phi)}$, $l^{(a)}$ и $l^{(m)}$ пересекаются, соответствующий тип $\Delta\tau_i^{(\phi)}$, $\Delta\tau_i^{(a)}$, $\Delta\tau_i^{(m)}$ временного ресурса, вносимый в процедуру, определяются согласно следующему алгоритму (рис. 2.8). Содержание блоков схемы алгоритма следующее.

а)



б)



в)

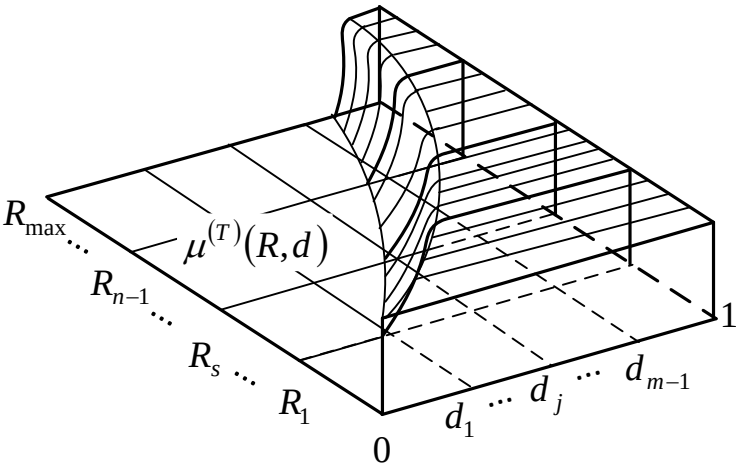


Рис. 2.6. Поверхности принадлежности соответствующие функциям принадлежности термов $l^{(\phi)}$, $l^{(a)}$ и $l^{(m)}$

Блок 1. На основе анализа содержания i - й, $i = 1, 2, ..., |\mathrm{A}|$, процедуры определяется способ ее контроля и оценивается его реализуемость с помощью известных методов. Получаемая при этом оценка временной сложности соответствующей функции контроля i - й процедуры рассматривается в качестве значения $\Delta\tau_i^{(\phi)}$.

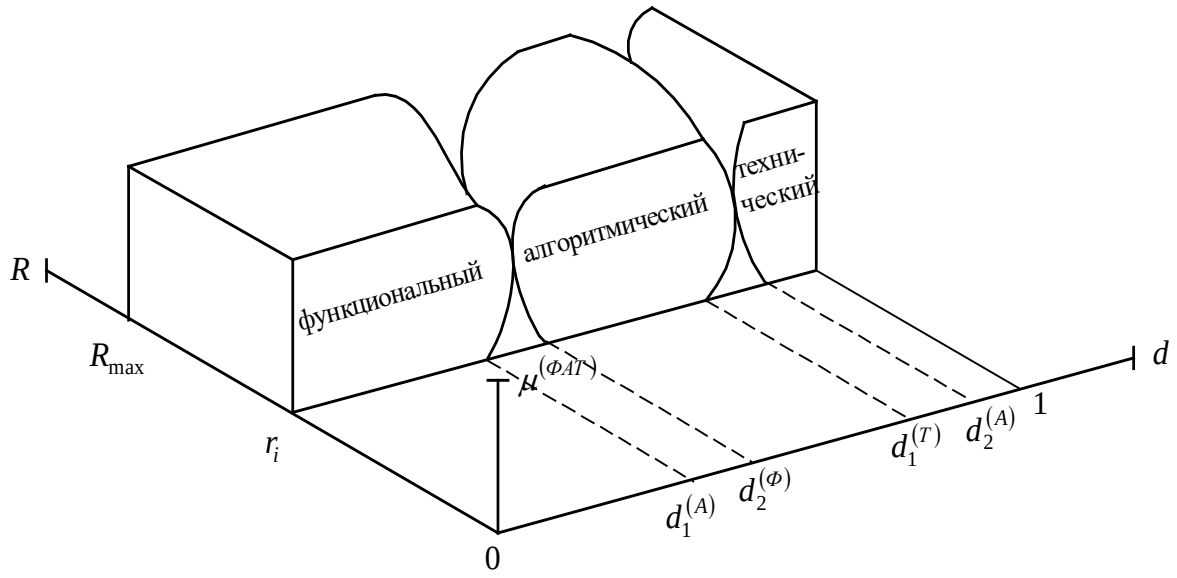


Рис. 2.7. Вид функций принадлежности $\mu^{(\phi am)} = \mu^{(\phi am)}(R, d)$

Блок 2. Определяются минимально $\Delta\tau_{(\min)i}^{(\phi)}$ и максимально $\Delta\tau_{(\max)i}^{(\phi)}$ возможные значения величины $\Delta\tau_i^{(\phi)}$:

$$\Delta\tau_{(\min)i}^{(\phi)} = d_{1i}^{(a)} \cdot \Delta\tau_i^{(opt)},$$
$$\Delta\tau_{(\max)i}^{(\phi)} = d_{2i}^{(\phi)} \cdot \Delta\tau_i^{(opt)}.$$

Блок 3. Проверка упрощенности способа контроля. При выполнении условия

$$\Delta\tau_i^{(\phi)} < \Delta\tau_{(\min)i}^{(\phi)}$$

считается, что данный способ контроля i - й процедуры является упрощенным и неприемлемым, после чего осуществляется переход на блок 4, в противном случае принимается решение о проверке усложненности способа контроля и переход на блок 5.

Блок 4. Принимается решение о необходимости усложнения рассматриваемой функции контроля.

Блок 5. Проверка усложненности способа контроля. При выполнении условия

$$\Delta\tau_i^{(\phi)} > \Delta\tau_{(\max)i}^{(\phi)}$$

считается, что данный способ контроля i - й процедуры является усложненным и неприемлемым, после чего осуществляется переход на блок 6, в противном случае принимается решение о приемлемости способа контроля и переход на блок 7.

Блок 6. Принимается решение о необходимости упрощения рассматриваемой функции контроля.

Блок 7. Значение $\Delta\tau_i^{(\phi)}$ рассматривается в качестве временной меры Ф-ресурса.

Блок 8. На основе анализа содержания отдельных функций, реализующих i - ю процедуру, определяются алгоритмы контроля соответствующих им информационных процессов и оценивается их реализуемость аналогичными применяемым в блоке 1 методами. Получаемая при этом оценка суммарной временной сложности алгоритмов контроля рассматривается в качестве значения для $\Delta\tau_i^{(a)}$.

Блок 9. Определяются минимально $\Delta\tau_{(\min)i}^{(a)}$ и максимально $\Delta\tau_{(\max)i}^{(a)}$ возможные значения величины $\Delta\tau_i^{(a)}$:

$$\Delta\tau_{(\min)i}^{(a)} = d_{1i}^{(a)} \cdot \Delta\tau_i^{(opt)} - \Delta\tau_i^{(\phi)},$$

$$\Delta\tau_{(\max)i}^{(a)} = d_{2i}^{(\phi)} \cdot \Delta\tau_i^{(opt)} - \Delta\tau_i^{(\phi)}.$$

Блок 10. Проверка упрощенности алгоритмов контроля. При выполнении условия

$$\Delta\tau_i^{(a)} < \Delta\tau_{(\min)i}^{(a)}$$

считается, что предлагаемые алгоритмы контроля функций i - й процедуры являются упрощенными и неприемлемыми, после чего осуществляется переход на блок 11, в противном случае принимается решение о проверке усложненности алгоритмов контроля и переход на блок 12.

Блок 11. Принимается решение о необходимости усложнения предлагаемых алгоритмов контроля.

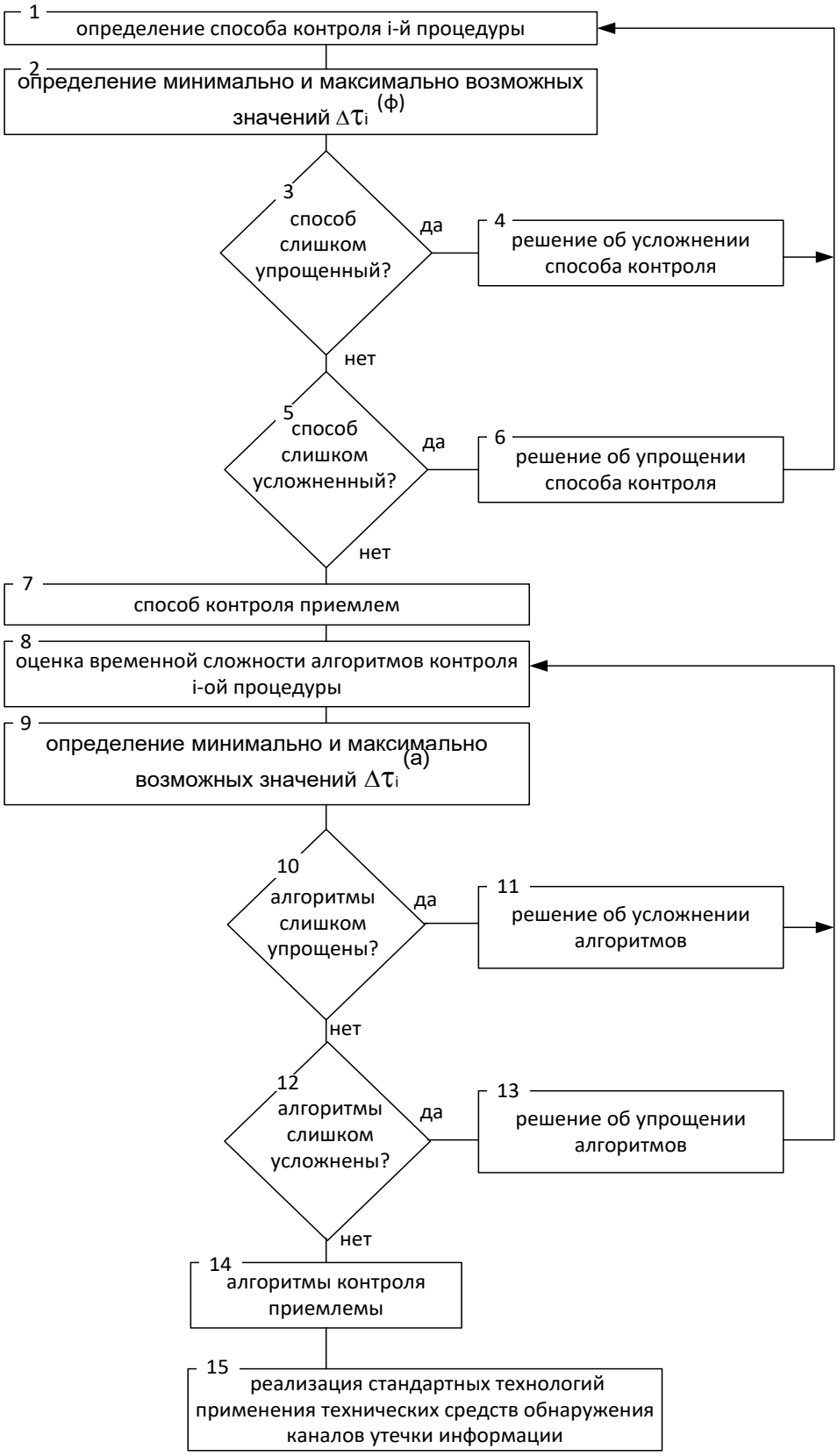


Рис. 2.8. – Схема алгоритма лингвистической идентификации временного ресурса СССН

Блок 12. Проверка усложненности алгоритмов контроля. При выполнении условия

$$\Delta\tau_i^{(a)} > \Delta\tau_{(\max)i}^{(a)}$$

считается, что предлагаемые алгоритмы контроля функций i - й процедуры являются усложненными и неприемлемыми, после чего осуществляется переход на блок 13, в противном случае принимается решение о приемлемости алгоритмов контроля и переход на блок 14.

Блок 13. Принимается решение о необходимости упрощения рассматриваемых алгоритмов контроля.

Блок 14. Значение $\Delta\tau_i^{(a)}$ рассматривается в качестве временной меры А-ресурса.

Блок 15. Оставшийся после выполнения блоков 1-15 ресурс $\Delta\tau_i^{(m)}$, определяемый согласно выражению:

$$\Delta\tau_i^{(m)} = \Delta\tau_i^{(opt)} - \left(\Delta\tau_i^{(\phi)} + \Delta\tau_i^{(a)}\right),$$

используется для реализации Т-ресурса.

Рассмотренные выше методические подходы и алгоритмы выявления, оптимального распределения и идентификации временного ресурса СССН, а также оценки их влияния на ее эффективность целесообразно решать на основе применения методов математического моделирования. В следующих разделах работы описываются разработанные для этих целей математические модели.

2.5. Средства противодействия угрозам информационной безопасности СССН и стратегии их применения

Возможный перечень средств противодействия угрозам информационной безопасности СССН определяется, прежде всего, воздействиями на дестабилизирующие факторы или влияющие на их возникновение. Причем направление воздействия должно способствовать увеличению показателя защищенности или сохранению ранее достигнутых значений.

Рассмотрим более подробно содержание представленных способов и средств противодействия угрозам информационной безопасности в сетях связи специального назначения. По способу обеспечения безопасности они могут подразделяться на пассивные и активные.

Пассивные способы заключаются в создании некоторого барьера на пути распространения дестабилизирующего фактора. Он блокирует развитие и возможности реализации конечных целей соответствующего фактора. Примерами таких способов защиты являются блокировки, не позволяющие человеку или техническому устройству выйти за опасные границы. Это может быть реализовано в виде создания физических препятствий на

пути злоумышленников, экранирования помещения и применение технических средств зашумления и т.д.

Активные способы включают в себя контур управления, который воздействует на каждом шаге функционирования СССН на ее элементы с целью решения одной или нескольких задач защиты информации.

Кроме того, различают формальные и неформальные средства. К формальным относятся средства, которые выполняют свои функции по защите информации без участия человека. К неформальным относятся средства, основу которых составляет целенаправленная деятельность людей. Формальные средства принято делить на физические, аппаратные и программные. Неформальные средства делятся на организационные, законодательные и морально-этические.

Стратегия применения средств противодействия угрозам информационной безопасности СССН определяет структуру, приоритеты, методы принятия решений при организации и обеспечении соответствующего вида деятельности, направлена на то, чтобы наиболее важные цели этой деятельности достигались при наиболее рациональном расходовании имеющихся ресурсов.

Выработка стратегии защиты информации может быть представлена как поиск оптимального компромисса между потребностями в защите и необходимыми для этих целей ресурсами. Состав и структура средства противодействия угрозам информационной безопасности СССН существенно зависят от выбранной стратегии защиты. Классификация возможных стратегий защиты приведена на рис. 2.9.

В аспекте функционирования комплекса средств противодействия угрозам информационной безопасности в СССН можно выделить три предельные стратегии, которые представлены в табл. 2.1.

Таблица 2.1. – Стратегии функционирования комплекса средств противодействия угрозам информационной безопасности в СССН

Учитываемые угрозы	Влияние на СССН		
	Отсутствует	Частичное	Полное
Наиболее опасные	Оборонительная стратегия		
Все идентифицированные угрозы		Наступательная стратегия	
Все потенциально возможные угрозы			Упреждающая стратегия

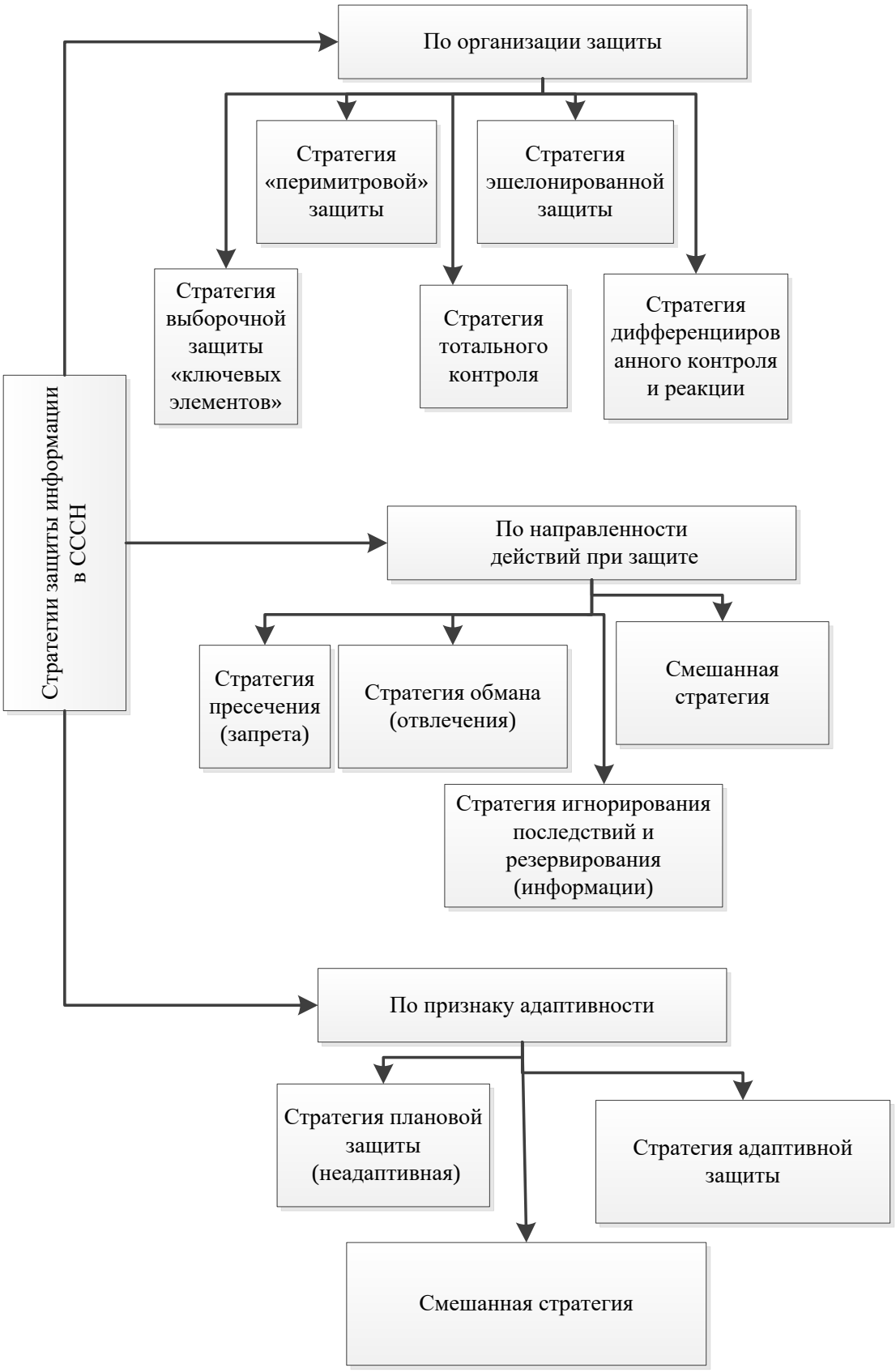


Рис. 2.9. Классификация стратегий защиты в СССН

Так, выбирая оборонительную стратегию, принято считать, что при недопущении вмешательства в процесс функционирования СССН обработки информации можно нейтрализовать лишь наиболее опасные угрозы. Данная стратегия может включать в себя разработку организационных мер, использование технических средств защиты по ограничению несанкционированного доступа к объекту защиты. Наступательная стратегия предусматривает активное противодействие известным угрозам, влияющим на функционирование СССН. Упреждающая стратегия предполагает тщательное исследование возможных угроз СССН и разработку мер по их нейтрализации еще на стадии проектирования и изготовления СССН.

В настоящее время выбор стратегии защиты не выделяется в отдельную процедуру. Это связано с непроработанностью общей методологии защиты с использованием разных стратегий.

Выводы

В главе 2 приведены теоретические основы оптимального управления комплексом средств противодействия угрозам информационной безопасности в сетях связи специального назначения.

Авторами разработаны основные положения оптимального управления функционально ориентированными информационными процессами при обеспечении безопасности территориальных сегментов сети связи специального назначения. В условиях выбранного множества показателей эффективности СССН справедливы следующие утверждения:

Утверждение 1. Показатель своевременности обработки информации в СССН будет представлять собой монотонно убывающую в интервале [0, 1] функцию объема информационного пространства, реализующего процессы обработки накопления и выдачи данных.

Утверждение 2. Показатель защищенности компьютерной системы будет представлять собой монотонно убывающую в интервале [0, 1] функцию объемов информационного пространства, реализующих процессы обнаружения и парирования воздействий угроз информационной безопасности.

Экстремум зависимости эффективности СССН является функцией объема информационного пространства, реализующего процесс обнаружения воздействий угроз ее информационной безопасности.

Метод оценки ресурса безопасности территориальных сегментов сети связи специального назначения базируется на методической основе определения оптимального информационного объема СССН, за счет которого реализуется обнаружение воздействий угроз информационной безопасности. Этот объем определяется как ресурс безопасности СССН. В соответствии с положениями теоремы 2 оптимальным объемом $V_{(opt)}^{(обн)}$ счита-

ется объем, полученный на основе объема, соответствующего экстремуму (максимуму) функции эффективности СССН.

Авторами систематизирована информация о средствах противодействия угрозам информационной безопасности СССН и классифицированы стратегии их применения.

Глава 3.
РАЗРАБОТКА И ОБОСНОВАНИЕ МЕТОДОЛОГИИ МОДЕЛИРОВАНИЯ КОМПЛЕКСА СРЕДСТВ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ИНФОРМАЦИОННОГО КОНФЛИКТА

3.1. Методология моделирования комплекса средств противодействия угрозам информационной безопасности

Главным условием создания комплекса средств противодействия угрозам информационной безопасности СССН является его надежность. Но надежность может быть обеспечена лишь в том случае, если защита является комплексной и системной. Исходя из сказанного, можно дать такое определение: «Комплекс средств противодействия угрозам информационной безопасности СССН – это организованная совокупность органов и объектов (компонентов) защиты информации, использование методов и средств защиты, а также осуществление защитных мероприятий».

Средства защиты информации, с одной стороны, являются составной частью системы, с другой стороны – они сами организуют комплекс противодействия, осуществляя защитные мероприятия. Поскольку комплекс определяется как совокупность взаимосвязанных элементов, то назначение комплекса противодействия угрозам информационной безопасности СССН состоит в том, чтобы объединить все составляющие элементы защиты в единое целое, в котором каждый компонент, выполняя свою прямую функцию, одновременно обеспечивает выполнение функций другими компонентами и связан с ними логически и технологически. При отсутствии отдельных компонентов комплекса или их несогласованности между собой неизбежно возникновение уязвимостей в технологии защиты информации. Следовательно, основным условием при разработке комплекса средств противодействия угрозам информационной безопасности СССН должна быть системность. Системный подход к задачам обеспечения ИБ включает в себя, прежде всего, оценку угроз безопасности объекта; анализ средств, которые могут использоваться при построении комплекса средств противодействия угрозам информационной безопасности СССН; оценку экономической целесообразности СЗИ и возможности увеличения её эффективности.

Реализация комплекса организационных (режимных) и технических мероприятий, направлена на обеспечение защиты информации, информационных СССН от утечки, хищения, утраты, несанкционированного доступа, уничтожения, модификации, подделки, копирования, блокирования.

К организации системы защиты информации с позиции системного подхода выдвигается ряд требований, определяющих ее целостность, адекватность и эффективность.

Комплексная система защиты информации – это система, в которой действуют в единой совокупности правовые, организационные, технические, программно-аппаратные и другие нормы, методы, способы и средства, обеспечивающие защиту информации от всех потенциально возможных и выявленных угроз и каналов утечки. Элементы КСЗИ, в свою очередь, состоят из средств, устройств и способов защиты информации, а также методов их использования [58].

Комплексность – один из основополагающих принципов защиты информации. Ее назначение состоит в объединении в одно целое локальных средств ЗИ. При этом они должны функционировать в единой «связке». В качестве локальных СЗИ могут выступать, например, правовые, организационные (режимные), инженерно-технические, программно-аппаратные механизмы защиты информации. Кроме того, комплексность должна обеспечивать безопасность всей совокупной информации, подлежащей защите, при любых обстоятельствах. Это означает, что должны защищаться все носители информации во всех компонентах ее сбора, хранения, передачи и использования, в любое время и при всех режимах функционирования системы обработки информации. В то же время комплексность не исключает, а, наоборот, предполагает дифференцированный подход к защите информации. Дифференцированность зависит от состава ее носителей, видов тайны, к которым отнесена информация, степени ее конфиденциальности, средств хранения и обработки, форм и условий проявления ее уязвимости, каналов и методов несанкционированного доступа к информации [53].

Решение задач разработки комплекса средств противодействия угрозам информационной безопасности может происходить различными способами: проведение натурных экспериментов с прототипами комплексов средств противодействия угрозам информационной безопасности в СССН, осуществление экспертного опроса по расстановке приоритетов, принимаемых архитектурных и схемных решений, непосредственное внедрение и исследование комплексов в рабочем режиме эксплуатации и т.д.

В общем виде моделирование представляет собой процесс замещения объекта исследования некоторой его моделью и проведение исследований на модели с целью получения необходимой информации об объекте [46].

В зависимости от характера изучаемых процессов модели могут быть разделены на детерминированные и стохастические; статические и динамические, дискретные и непрерывные и дискретно-непрерывные.

Предшествовать приведенным в схеме на рис. 3.1 этапам моделирования комплекса средств противодействия угрозам ИБ СССН должны процедуры, связанные с исследованием самого комплекса, выделением его элементов и отношений между ними, т.е. определение состава и структуры.

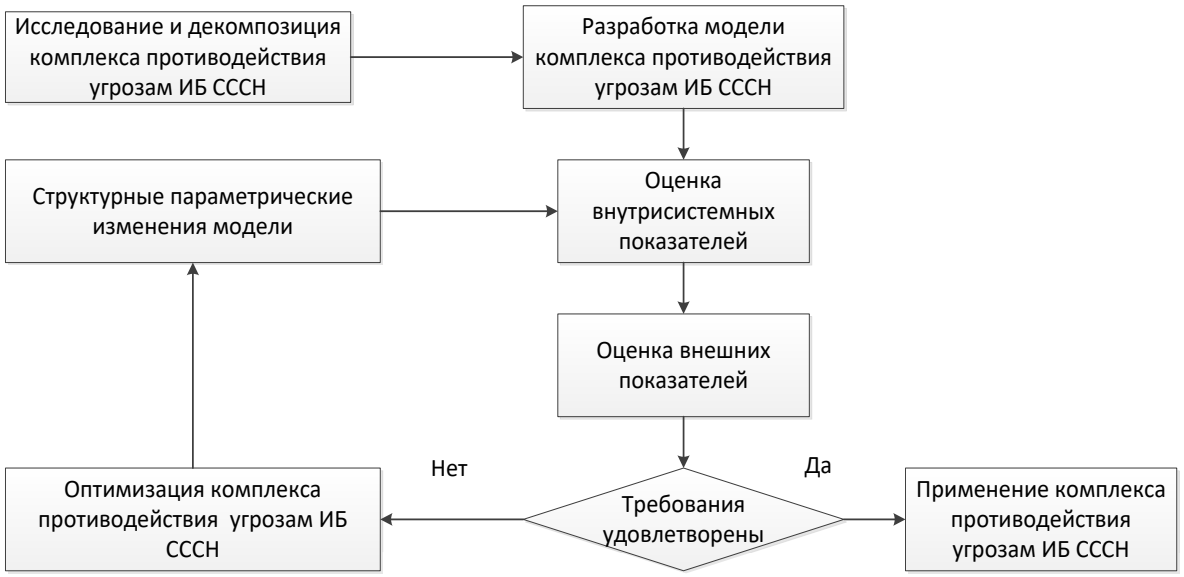


Рис. 3.1. Общая схема моделирования комплекса средств противодействия угрозам информационной безопасности в СССН

Разработка модели комплекса и проверка её адекватности также должны предшествовать выделенным этапам.

Рассмотрим содержание этапов моделирования, которые будут входить в состав предлагаемой методологии.

Исследование и декомпозиция комплекса противодействия угрозам ИБ (ПРУИБ) СССН могут быть выполнены классическими методами [54], и включать в себя исследование современных комплексов ПРУИБ СССН, выявление особенностей комплексов ПРУИБ СССН, обобщение структуры и состава комплекса ПРУИБ СССН.

Разработка модели комплекса противодействия угрозам ИБ СССН в случае рассмотрения комплекса как эргатической системы будет подразделяться на анализ и выбор методов моделирования комплекса ПРУИБ СССН, разработку обобщенной модели комплекса ПРУИБ СССН.

Оценка внутрисистемных показателей должна основываться на показателях конфликтности взаимодействия элементов комплекса ПРУИБ СССН.

Оценка внешних показателей должна основываться на обработке экспертных данных, получаемых от пользователей различных категорий.

Кроме того, наличие внешних и внутрисистемных показателей непременно ставит задачу определения связи между ними с целью экстраполяции значений показателей на различные варианты построения комплекса ПРУИБ СССН.

Оптимизация комплекса противодействия угрозам ИБ СССН заключается в выборе оптимального количества элементов комплекса, обеспечивающего эффективное функционирование условиях противодействия.

Структурные и параметрические изменения модели комплекса ПРУИБ СССН должны включать перечень допустимых модификаций, с последующей оценкой их последствий для внутриссистемных и внешних показателей.

Проведение вычислительных экспериментов и получение результатов моделирования должны подтверждаться адекватностью и целесообразностью их применения.

Итоговым результатом будет являться применение комплекса противодействия угрозам ИБ СССН и внедрение результатов исследования в практическую деятельность.

Таким образом, методология моделирования комплекса противодействия угрозам ИБ СССН как эргатической системы будет иметь следующий вид:

Рис. 3.2. Методология моделирования комплекса средств противодействия угрозам информационной безопасности СССН

Разработка модели комплекса в случае рассмотрения эргатических систем может после анализа существующих подходов моделирования осуществляться с помощью применения теории конфликтов, позволяющей на основе полученных на предыдущем этапе результатов разработать обобщенную математическую модель комплекса. Например, такая модель

может быть основана на применении лингвистических переменных и нечетких экспертных систем.

В соответствии с требованием оптимальной структурированности совокупность показателей эффективности средств интегрированной защиты информации должна представляться минимальным набором математических моделей для их оценки.

Оптимальность обусловлена согласованностью неформальных (эвристических) правил [55] структуризации показателей в соответствии с интуитивными (экспертными) оценками [25, 59] с существующими классическими подходами к решению оптимизационных задач [61].

На основе изложенных требований сформулируем постановку и порядок решения задачи разработки математических моделей для оценки эффективности средств интегрированной защиты информации комплексных систем безопасности объектов [60].

С этой целью представим множество исходных характеристик средств интегрированной защиты информации комплексных систем безопасности объектов в виде

$$X = \{x_i\},\ i = 1, 2, \ldots, |\{x_i\}|$$

и промежуточных характеристик в виде

$$Y = \{y_j\},\ j = 1, 2, \ldots, |\{y_j\}|\ .$$

Для их оценки будем использовать множество:

$$L=\{l_k\},\ k = 1, 2, \ldots, K$$

из K логико-лингвистических моделей. Множество L должно обеспечивать адекватное формирование обобщенного показателя. Адекватное в том смысле, что процедура его оптимального построения считается реализованной, если множество L логико-лингвистических моделей обеспечивает анализ влияния любого из исходных x_i и промежуточных $\boldsymbol{y_j}$ показателей на формирование обобщенного показателя Z.

Обозначим через S – правило систематизации исходных X и промежуточных $\boldsymbol{Y}$ показателей при формировании обобщенного показателя Z. Тогда задачу оптимального построения обобщенного показателя $\boldsymbol{Z}$ можно рассматривать как задачу формирования варианта $w_m \in W$ систематизации характеристик средств интегрированной защиты информации минимизирующего множество $\boldsymbol{L}$ логико-лингвистических моделей для их оценки.

$$w_{(opt)} = \underset{w_m \in W,\ m=1,\ldots,M}{\arg\min} L\left[S\left(X\right)\right]\ . \qquad (3.1)$$

Сформулированную задачу целесообразно решать в виде следующей последовательности:

– синтез показателя эффективности средств интегрированной защиты информации на основе систематизации их характеристик;

– унификация формальных методов оценки характеристик средств интегрированной защиты информации на основе минимального набора логико-

лингвистических моделей;

– проведение экспериментов по исследованию возможностей синтеза показателя эффективности средств интегрированной защиты информации.

В последующих разделах описаны методы, модели и результаты решения поставленной задачи.

3.2. Алгоритмы противодействия при воздействии сверхширокополосных помех на системы передачи видеоинформации

Актуальным вопросом настоящего времени является передача видеоинформации с помощью инфраструктуры сетей связи специального назначения. Реализация алгоритмов противодействия при воздействии сверхширокополосных помех на системы передачи видеоинформации является одним из направлений обеспечения информационной безопасности, реализуемых сотрудниками, осуществляющими обеспечение общественной безопасности.

В соответствии с ч. 1 ст. 11 Федерального закона от 7 февраля 2011 г. № 3-ФЗ «О полиции» «полиция в своей деятельности обязана использовать достижения науки и техники, информационные системы, сети связи, а также современную информационно-телекоммуникационную инфраструктуру». Указанные средства находят свое применение в сферах противодействия преступности, экстремизму и терроризму, охраны общественного порядка, а также повседневной служебной деятельности органов внутренних дел. Таким образом, автоматизированные технические средства, информационные системы и сети связи, а также информационно-телекоммуникационная инфраструктура, способствующие решению законодательно закрепленных за органами внутренних дел задач, в комплексе формируют информационную платформу «Цифровой полицейский».

Одним из элементов экипировки «Цифрового полицейского» являются персональные видеорегистраторы (ПВР). Передовой опыт в области применения ПВР накоплен в подразделениях полиции США, Великобритании, Германии, Австралии, Гонконга, Китая, России и других стран мира [75–79].

Основываясь на мировом и российском опыте, можно сделать вывод, что применение ПВР имеет следующие положительные аспекты:

– повышается дисциплина полицейских;

– снижается количество случаев коррупции и взяточничества;

– снижается количество спорных ситуаций;

– снижается количество жалоб на полицейских;

– уменьшается количество «бумажной работы» полицейских по защите правопорядка;

– освобождается время для работы полицейских по защите правопорядка;

– косвенный результат – повышается психологическая устойчивость и уверенность полицейских в своих действиях в опасных ситуациях;

– в целом повышается эффективность работы полицейских;

– сбор доказательств в случаях правонарушений становится быстрее;

– снижается количество случаев оскорблений и нападений на полицейских.

На снабжение подразделений МВД России поступают ПВР «ДОЗОР-77». Современные беспроводные технологии позволяют обеспечивать двухстороннюю аудиосвязь, возможность передавать тревожный сигнал и просмотр видео с него одновременно с позицией сотрудника на карте. Видеоданные с «ДОЗОР-4G+» могут быть по сети объединены с видеоданными со стандартных и мобильных систем видеонаблюдения для построения централизованных многоканальных систем.

В нормативно-правовых документах МВД России по обеспечению правопорядка в общественных местах установлено, что системы видеонаблюдения применяются для решения таких задач, как:

– оценка оперативной обстановки, организационное информационно-аналитическое обеспечение управленческих решений;

– своевременное выявление противоправных действий, организация их расследования, раскрытия и предотвращения;

– создание видеоархивов, позволяющих использовать их в качестве доказательств.

Особое внимание уделяется мобильным комплексам передачи видео и звука, активно используемым подразделениями быстрого реагирования. На снабжение органов внутренних дел поступают комплексы передачи видео и звука, такие как «СОВА», «ОКО-2», «Волна-М4», «ЭРИКА-ВС-С-04». Эти комплексы позволяют дистанционно осуществлять наблюдение в режиме реального времени за обстановкой и действиями личного состава в местах проведения массовых мероприятий и оперативно принимать и доносить управленческие решения до личного состава подразделения. Комбинированная передача аудиовизуальной информации может осуществляться по различным каналам связи (UHF/VHF, 3G, 4G, LTE, WiFi), что повышает стабильность и надежность ее доставки. В качестве объекта в данном разделе был выбран комплекс передачи видео- и аудиоинформации в диапазоне UHF/VHF. Необходимо отметить что данный комплекс помимо аудиосигналов передает и видеосигнал, что значительно усложняет процесс передачи, увеличивается полоса занимаемых радиочастот, а следовательно, увеличивается вероятность перекрытия частот функционирования с другими радиосистемами и появления интермодуляционных эффектов и искажений радиосигнала [80, 83]. Таким образом, можно сделать вывод, что применение комплексов передачи видео и звука для раскрытия и расследования преступлений представляет собой актуальную как в научном, так и в практическом плане задачу. В работе приведено эксперимен-

тальное исследование функционирования таких комплексов в условиях сложной помеховой обстановки и наличия взаимных помех.

Эффекты интермодуляции в РЭС.

Интермодуляция в приемнике – это возникновение помех на выходе радиоприемника при действии на его входе двух и более мешающих сигналов, частоты которых находятся вне основного и побочных каналов приема. Помехи этого вида называют интермодуляционными. Причина их появления – нелинейность амплитудной функции передачи сигнала в активных элементах ВЧ тракта, вследствие чего анализ интермодуляционных помех аналогичен анализу процессов возникновения блокирования и перекрестных искажений полезного сигнала [76]. Интермодуляция в приемнике возможна при любом виде мешающих сигналов независимо от типа их модуляции. Восприимчивость к интермодуляционным помехам – важный параметр ЭМС приемника. В службах радиосвязи с большим числом радиосредств во многих случаях интермодуляционные помехи оказываются ограничивающим фактором для повышения загрузки радиочастотного ресурса. Интермодуляция возникает в усилителях высокой частоты и преобразователе приемника при определенном превышении уровня U мешающих сигналов над уровнем U полезного сигнала, т.е. при превышении «порога интермодуляции». Эффекты интермодуляции представлены на рис. 3.3.

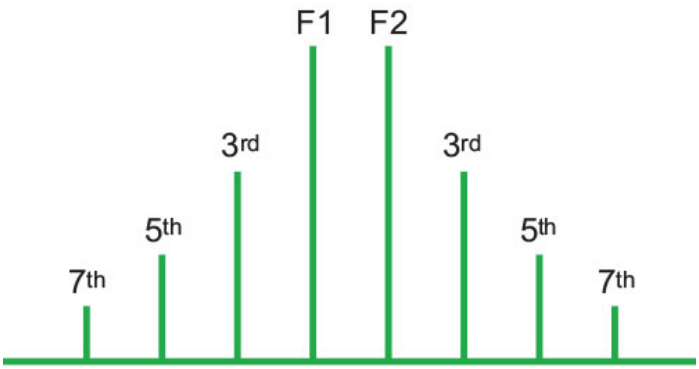


Рис. 3.3. Интермодуляционный эффект

Влияние интермодуляционной помехи на полезный сигнал характеризуется коэффициентом интермодуляции, который представляет собой отношение уровня радиопомехи, возникающей в результате интермодуляции в приемнике, к уровню сигнала, соответствующего чувствительности приемника. Коэффициент интермодуляции определяют по отношению помеха сигнал на выходе приемника. Для этого воспользуемся моделью степенного полинома:

$$i_{вых} = \sum_{k=0}^{m} b_k u^k{}_{вх} \approx b_0 + b_1 u_{вх} + b_2 u^2{}_{вх} + b_3 u^3{}_{вх},$$

где коэффициенты b полинома, с помощью которого представим амплитудную функцию передачи сигнала, определяют крутизну нелинейной функции передачи. Для анализа интермодуляции в усилителях высокой частоты можно ограничиться кубичным полиномом и в качестве мгновенного значения U принять сумму только двух мешающих сигналов в отсутствии полезного сигнала, что не нарушит результаты вычислений уровня интермодуляционной помехи. В целях упрощения считаем мешающие сигналы немодулированными и их сумму равной

$$u_{вх} = u_1 + u_2 = U_1 \cos \omega_1 t + U_2 \cos \omega_2 t \qquad (3.2)$$

Подставим в полином, чтобы выделить из него составляющие выходного тока, интермодуляции второго:

$$i_{инт} = b_2 U_1 U_2 \cos(\omega_1 \pm \omega_2) t \qquad (3.3)$$

и третьего порядка:

$$i_{инт} = b_3 U_1^2 U_2 \cos(2\omega_1 - \omega_2) t \qquad (3.4)$$

$$i_{инт} = b_3 U_2^2 U_1 \cos(2\omega_2 - \omega_1) t \, . \qquad (3.5)$$

Интермодуляционные составляющие второго порядка имеют частоты, значительно отличающиеся от частоты настройки приёмника, и они ослабляются избирательными цепями ВЧ тракта приёмника. Однако в широкополосном входном усилителе они могут проявляться как помехи. Интермодуляционные составляющие третьего порядка имеют частоты, близкие к частоте настройки приёмника, и могут не ослабляться цепями ВЧ тракта. Если же частоты этих составляющих соответствуют частоте настройки приёмника, то есть

$$2\omega_1 - \omega_2 = \omega_0 \qquad (3.6)$$

или

$$2\omega_2 - \omega_1 = \omega_0 , \qquad (3.7)$$

то интермодуляционная помеха оказывается непосредственно в полосе пропускания приёмника и от неё отстроиться невозможно. Интермодуляционная помеха может возникнуть и в первом преобразователе приёмника. Интермодуляция третьего порядка может возникать при одновременном действии не только двух, но и трёх мешающих сигналов в полосе тракта ВЧ приёмника. В службах радиосвязи с большим количеством средств вероятность возникновения интермодуляционных помех от трёх мешающих сигналов близка к вероятности таких помех от двух сигналов. Для предот-

вращения интермодуляционных помех, как и перекрестной модуляции, необходимо добиваться хорошей линейности входных каскадов приемника, а также принимать меры для защиты входов этих каскадов от сильных помех [81].

Вычисление интермодуляционных частот производится по формулам:

$$F_{интер}\ (3\ порядка) = 2f1 - f2, \quad (3.15)$$

$$F_{интер\ (}\ 3\ порядка) = 2f2 - f1, \quad (3.16)$$

$$F_{интер}\ (2\ порядка) = f1 - f2, \quad (3.17)$$

где f1, f2. — частоты взаимодействующих РЭС, МГц.

Описание комплекса передачи видео- и аудиоинформации

Мобильная цифровая система передачи видео и звука предназначена для передачи высококачественной оперативной видео- и аудиоинформации по UHF/VHF радиоканалу от одного или нескольких носимых комплектов передачи данных (НКПД) на центральный пункт управления (ЦПУ). Приемо-передающее оборудование комплекса использует в своей работе цифровую модуляцию COFDM и технологии сжатия MPEG2/MPEG4. Для подобных комплексов передачи видео и звука, функционирующих, как правило, в условиях городской застройки и сложных условиях для организации связи, характерна передача данных с помощью портативного оборудования на расстояние от нескольких сотен метров до километра и более [82].

Ортогональное частотное разделение каналов с кодированием COFDM – это разновидность технологии OFDM, сочетающая канальное кодирование и OFDM. Канальное кодирование подразумевает использование прямой коррекции ошибок (FEC), которая применяется для исправления сбоев и ошибок при передаче данных. За счет избыточной служебной информации возможно восстановление утерянных данных. Оборудование на основе технологии COFDM формирует видеоканал с полосой 2,5 МГц с количеством поднесущих около 400.

Безопасность передачи мультимедийного потока обеспечивается использованием алгоритма шифрования AES с длиной ключа 128 бит. Высокое качество передаваемого изображения 704x576 пикселей при скорости 25 кадров/с.

Система обеспечивает передачу высококачественной оперативной аудио- и видеоинформации по радиоканалу в диапазоне частот от 150,00 до 900,00 МГц НКПД на ЦПУ. Для передачи информации в аппаратуре используются широкополосные каналы связи (ШПС) с полосой частот 2,5 МГц, со скоростью передачи цифрового потока до 3,5 Мбит/с. Даль-

ность связи по ШПС УКВ радиоканалу в условиях прямой видимости не менее 20 км при использовании стационарных антенн. Система обеспечивает автоматическое восстановление соединения между НКПД и ЦПУ со временем восстановления не более 5 секунд.

В состав комплекса входят:

1. Центральный пункт управления (ЦПУ) – 1 комплект, в состав которого входят:

– четырехмониторная ЖК-панель (диагональ);

– двухканальный видеорегистратор на флешнакопителях.

2. Носимый комплект передачи данных (НКПД) – 4 комплекта, состоящий из:

– передатчика аудио- и видеоинформации;

– шлема защитного ЗШ-1 с установленной миниатюрной видеокамерой, микрофоном и гарнитурой с функцией VOX к радиостанции;

– видеокамеры переносной;

– комплекта носимой радиостанции;

ЦПУ и НКПД комплектуются комплектом приемопередающих антенн.

Схема функционирования комплекса приведена на рис 3.4.

Рис. 3.4. Схема функционирования комплекса

Видеоизображение с камер, которые могут быть размещены на штативах или на обмундировании личного состава, принимающего участие в спецоперации, транслируется на ЖК-дисплеях, а голосовые сообщения

воспроизводятся на встроенном динамике ЦПУ. Руководство спецоперацией осуществляется посредством передачи аудиосообщений от оперативного штаба во встроенную гарнитуру бойцов, выполняющих поставленные задачи.

Описание и настройка экспериментального исследования воздействия РЭС СН на комплекс передачи видео- и аудиоданных.

ШАГ 1. Для проведения экспериментального исследования настроим соединение между НКПД и ЦПУ таким образом, чтобы на мониторах ЦПУ транслировалось изображение со всех видеокамер, входящих в состав НКПД. Также проверяем работоспособность средств радиосвязи, входящих в НКПД, путем вызова ЦПУ. После проведения данных процедур комплекс находится полностью в работоспособном состоянии и готов к проведению эксперимента.

ШАГ 2. Устанавливаем соединение между анализатором спектра FSH 8 и персональным компьютером с установленным программным обеспечением при помощи Ethermet-соединения.

ШАГ 3. Производим настройку спектроанализатора, указывая следующие параметры:

– ширина полосы частот 30 МГц;
– верхняя частота 440 МГц;
– нижняя частота 470 МГц;
– ширина полосы пропускания 100 КГц.

Схема экспериментального исследования приведена на рис. 3.5.

Рис. 3.5. Схема экспериментального исследования

Этапы проведения эксперимента.

На первом этапе эксперимента изучим спектр сигнала трех включенных НКПД (рис. 3.6).

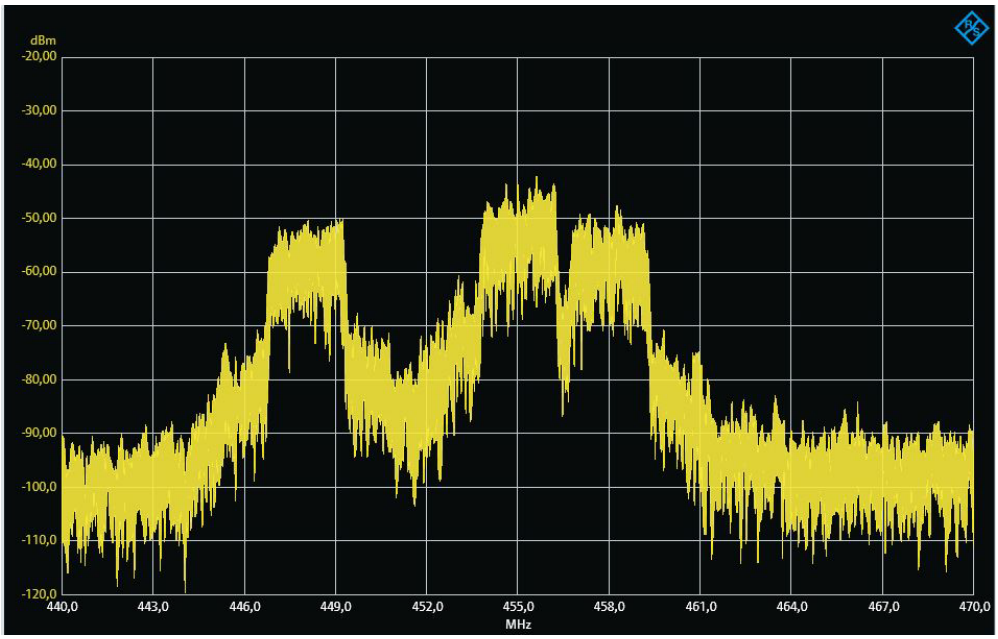


Рис. 3.6. Спектрограмма сигнала трех НКПД

На рис. 3.6 можно пронаблюдать спектр видеосигнала трех НКПД и сделать вывод, что в рамках одной системы каналы имеют частотный разнос и не оказывают влияния друг на друга, изображение на ЦПУ четкое и не прерывается.

Вторым этапом эксперимента является изучение спектра 3 НКПД и аналогового радиосредства, входящего в их состав. Спектр приведен на рис. 3.7.

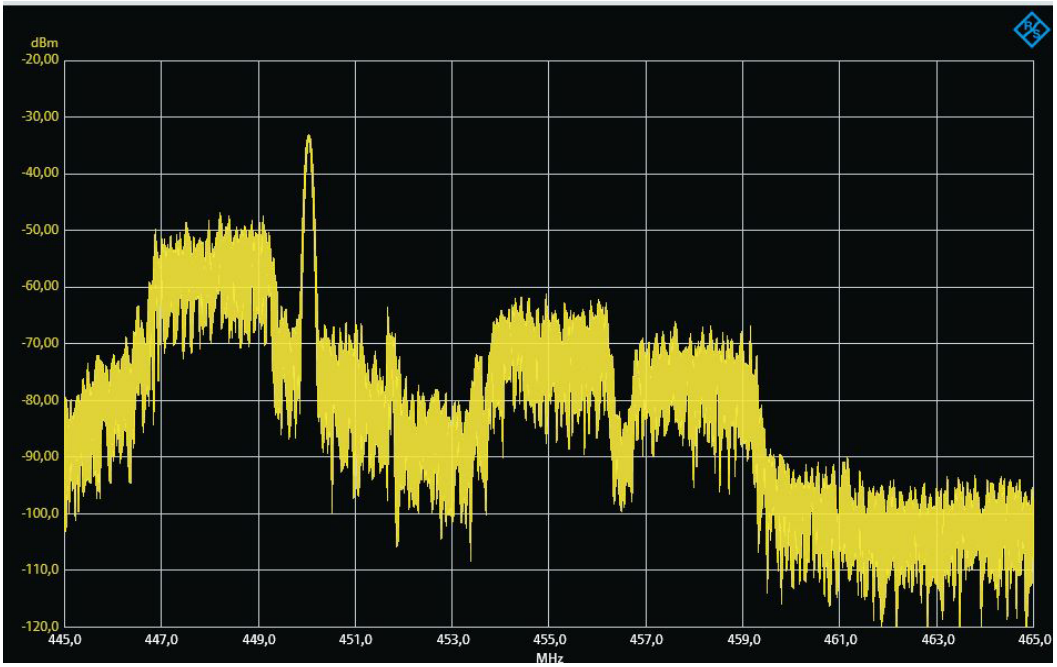


Рис. 3.7. Спектрограмма сигнала трех НКПД и аналогового радиосредства, входящего в их состав

Из спектрограммы можно сделать вывод, что речевой сигнал и видеосигнал не оказывают влияния друг на друга из-за наличия частотного разноса и разности ширины спектра. На ЦПУ отчетливо наблюдается изображение с видеокамер и слышится речь, передаваемая с помощью радиосредства.

Третьим этапом эксперимента является изучение спектра 3 НКПД и стороннего аналогового радиосредства, настроенного на тот же частотный диапазон работы. Спектр приведен на рис. 3.8.

Из спектра видно, что спектр канала, на частоту работы которого настроено стороннее радиосредство, кардинально изменился. В нем появились интермодуляционные составляющие, оказывающие негативное влияние на передаваемый видеосигнал. На ЦПУ наблюдается искажение видеосигнала и передаваемой речи, которые происходят, пока не прекратится работа стороннего аналогового радиосредства.

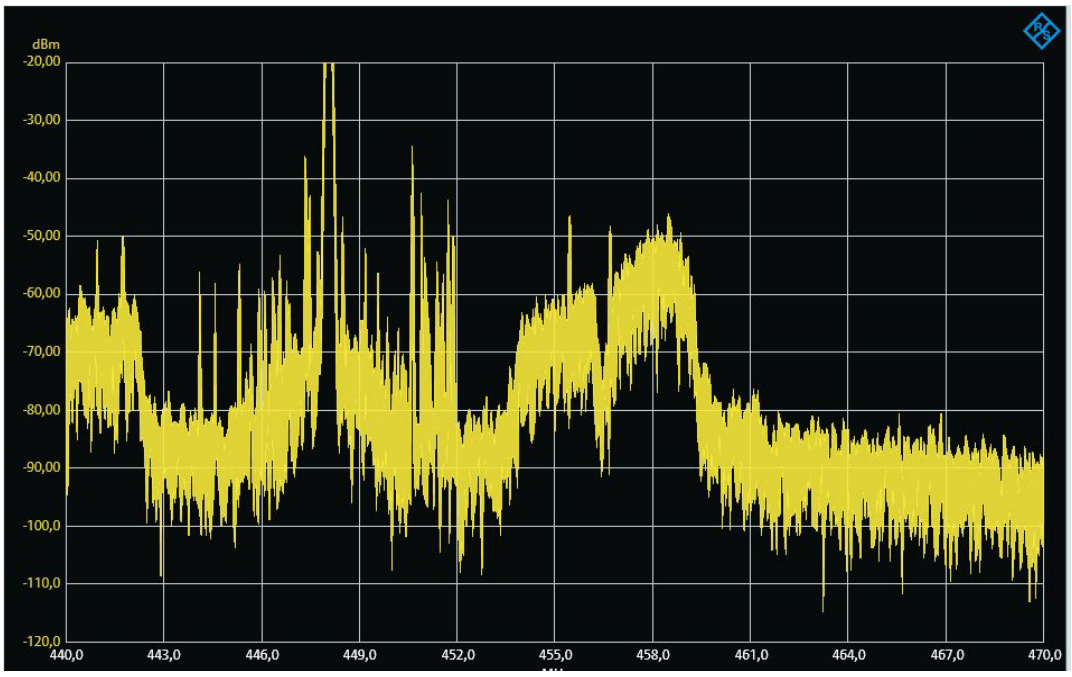


Рис. 3.8. Спектрограмма сигнала трех НКПД и стороннего аналогового радиосредства, настроенного на тот же частотный диапазон

Четвертым этапом эксперимента является изучение спектра 3 НКПД и стороннего цифрового радиосредства, настроенного на тот же частотный диапазон работы. Спектр приведен на рис. 3.9.

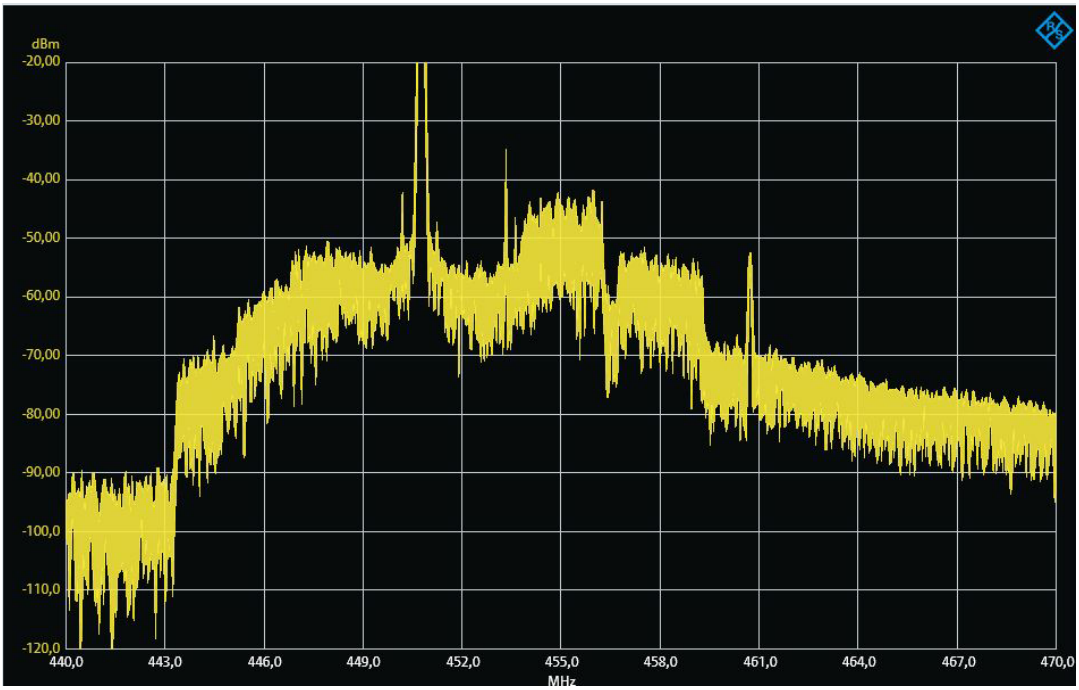


Рис. 3.9. – Спектрограмма сигнала трех НКПД и стороннего цифрового радиосредства, настроенного на тот же частотный диапазон

Как видно из спектрограммы, спектр сигнала также очень сильно искажается и происходят интермодуляционные эффекты, но, однако, на ЦПУ не происходит замираний видеосигнала, а спектр периодически принимает нормальную форму. Это объясняется тем, что в цифровой связи используется пакетная передача данных, а между передачей двух пакетов существует определенная пауза. Особенности спектра сигнала связаны с технологией временного разделения TDMA.

Решением для передачи видео и звука являются системы с модуляцией COFDM. Благодаря большому числу поднесущих частот в комбинации с помехоустойчивым кодированием возможно восстановление отдельных поднесущих, ослабленных вследствие частотно-селективных замираний в канале. При всех достоинствах рассматриваемых систем данный вид модуляции имеет существенные недостатки – большое отношение пиковой мощности сигнала к его усредненной мощности (пикфактор сигнала), а также эффект нарушения ортогональности поднесущих частот в нестационарных каналах связи с многолучевостью, приводящий к взаимным перекрестным помехам между поднесущими частотами. Информационные сигналы также очень чувствительны к системным нестабильностям, что в отдельных случаях может приводить к существенному росту внеполосных излучений. Помехи в радиоэфире от других радиоэлектронных средств на рабочем частотном канале приводят к искажениям изображения и звука. В этом случае необходимо сменить частотный канал, убедиться в отсутствии других радиоизлучающих средств, попадающих в полосу работы системы.

Методика количественной оценки влияния радиопомех и сигнала радиоэлектронных средств на показатели радиоэлектронной защиты рассмотрена авторами в работах [88 – 91].

Таким образом, в результате экспериментального исследования выявлено воздействие друг на друга радиосредств органов внутренних дел, работающих в одной полосе частот. Это наглядно показано в случае работы аналогового радиосредства, в том же частотном диапазоне. Однако при использовании цифрового радиосредства не входящего в состав комплекса, влияние на спектр также присутствует, но на передачу видеоданных это не оказывает существенного воздействия. Данные эксперимента показывают, что в случае возникновения селективных замираний и некорректной работы комплекса передачи видео и звука рекомендуется проводить работы по анализу спектра при настройке и монтаже систем связи специального назначения с целью минимизации взаимного влияния радиооборудования.

3.3. Защита информации в каналах связи методом формирования маскирующих сигналоподобных помех

Задача защиты от перехвата информации, циркулирующей в сетях передачи данных, является одной из актуальных задач технического обеспечения средств связи специального назначения [87].

Для решения задачи скрытия содержания переговоров по радиоканалу применяют комплекс технических и организационных мероприятий, которые в совокупности обеспечивают защиту передаваемых информационных потоков от радиоперехвата несанкционированными потребителями согласно ГОСТ Р 53110 – 2008 «Система обеспечения безопасности сети связи общего пользования».

При этом одним из эффективных методов борьбы с утечкой полезной информации по радиоканалу является радиочастотное маскирование передаваемых излучений. Вопросы маскирования информационных сообщений в каналах радиосвязи искусственно созданными радиопомехами подробно рассматриваются в ряде работ [88 – 93].

Целью данного раздела является обоснование нового метода маскирования полезных информационных сигналов в радиоканале при помощи специальных процедур и устройств, обеспечивающих формирование мультипликативных маскирующих радиопомех из полезных излучаемых сигналов.

Вопросы маскирования полезных сигналов искусственными помехами рассматриваются в работах В. В. Цветнова, А. И. Куприянова, Э. В. Кальянова, С. В. Канавина и др. Известны также патенты на способы и устройства формирования маскирующих помех для защиты информации в каналах связи: «Способ передачи и приема сигналов» – патент RU

2438250 C1 H04K1/00; «Способ повышения скрытности передачи группы бинарных полезных сигналов, манипулированных по амплитуде, фазе или частоте» – патент RU 2282941 C1 H04K1/02; «Способ повышения скрытности передачи группы узкополосных сигналов» – патент RU 2232475 C1 H04K1/2.

Маскирование осуществляют в зависимости от информационных пара-метров полезного сигнала по несущей частоте, амплитуде, фазе и спектру. В результате маскирования ухудшаются параметры обнаружения, увеличиваются ошибки определения параметров сигналов. Эффективность маскирующих радиопомех зависит от частотной и временной структуры помехового и полезного сигналов и их энергетического соотношения на входе приемника.

Для осуществления радиомаскировки используют аддитивные и мультипликативные маскирующие и имитирующие помеховые сигналы.

1. Сущность метода формирования маскирующих мультипликативных радиопомех.

Все известные современные методы формирования маскирующих помех основаны на создании прицельных или заградительных по частоте, шумовых или имитационных помех с помощью специальных устройств – формирователей помех. При этом процессы формирования в радиоканале полезных сигналов и радиопомех выполняются отдельными устройствами для сигналов (модуляторы, усилители мощности и др.) и помех (генераторы шума, формирователи помех, шумящие усилители и др.). Вопросам формирования эффективных для маскирования сигналов с известными видами модуляции помех уделяется большое внимание, тогда как вопросы комплексирования аппаратуры для формирования сигналов и помех до настоящего времени в специальных исследованиях не рассматривались. Существующие методы маскирования радиоканалов основаны на аддитивной модели: шумы или помехи при оценке эффективности маскирующих помех складываются.

Формирование сигналоподобных (коррелированных с сигналами) помех является перспективным направлением в технике радиоэлектронного подавления РЭС. В первую очередь такие помехи реализуются в станциях создания активных помех средствам радиосвязи при формировании имитационных радиопомех. Наличие такого рода помех в канале связи существенно затрудняет обработку сигнальной смеси сигнал+помеха+шум на входе приемника. Технологии применения сигналоподобных помех являются продуктивными также при решении задач маскировки полезных сигналов в каналах с зашумлением.

В предлагаемом новом методе предполагается использовать сам полезный информационный маскируемый сигнал в качестве маскирующей его же помехи. При этом маскирующая мультипликативная помеха формируется из полезного информационного маскируемого сигнала путем его

усиления в усилителе с существенно нелинейными свойствами. Отличительной особенностью такой помехи является корреляция ее с исходным сигналом, то есть такая ответная или ретранслированная помеха является сигналоподобной, коррелированной, мультипликативной.

Известно, что усиление мощности сигнала в любом усилителе, кроме усилителя, работающего в режиме А [99], всегда сопровождается нелинейными искажениями сигнала. Объясняется это свойствами усилительного нелинейного элемента (УНЭ). Спектр сигнала на выходе усилителя всегда имеет значительно более богатый спектральный состав, чем соответствующий спектр на входе.

Современные усилительные устройства характеризуются многообразием принципов работы и схемного исполнения. По принципам построения они разделяются на классы A, B, C, D, E, F, T и различные их комбинации и модификации. Способ усиления сигналов в том или ином режиме (классе) характеризуется либо выбором рабочей точки на выходной статической вольт-амперной характеристике УНЭ (классы A, B, C), либо особенностями схемных решений (классы E, F, T). Все указанные классы усилителей являются аналоговыми. Особый класс усилителей представляет усилитель класса D, называемый цифровым. На самом деле он таковым не является, поскольку не выполняет обязательных для цифрового устройства процедур дискретизации аналогового сигнала во времени с учетом теоремы Котельникова, квантования его по уровню и оцифровки. Применяемый в нем метод преобразования сигнала с помощью широтно-импульсной модуляции (ШИМ) хотя и применяется как в аналоговой, так и цифровой технике, однако не заменяет указанных обязательных для цифрового устройства процедур.

Простейший усилитель класса А [94] реализует усиление сигналов с минимальными нелинейными искажениями, однако он имеет чрезвычайно низкий КПД. Угол отсечки выходного тока в таком усилителе составляет 180^0, то есть сигнал усиливается без искажений. В усилителях с высоким КПД УНЭ работает в режиме с отсечкой тока.

С уменьшением угла отсечки (особенно при углах отсечки менее 90^0) КПД усилителя увеличивается, но при этом в спектре усиливаемого сигнала появляются как новые гармоники, так и комбинационные (интермодуляционные межгармонические составляющие). При угле отсечки менее 90^0 искажения спектра сигнала максимальны. Это явление в усилителях считается нежелательным, поскольку оно «до неузнаваемости» искажает спектр усиливаемого полезного информационного сигнала, поэтому его снижают путем специальных, подчас весьма сложных технических приемов. Однако эта самая «неузнаваемость» спектра исходного сигнала может быть очень полезна для его же маскировки при передаче по радиоканалу. Степень нелинейности выходного сигнала в усилителе количественно оценивается показателем «коэффициент нелинейных искажений». Применительно к ре-

чевым сигналам при значении этого показателя больше чем 20% речь становится полностью неразборчивой.

Пример искажения гармонического сигнала в усилителе с нелинейной вольт-амперной характеристикой приведен на рисунке 3.10.

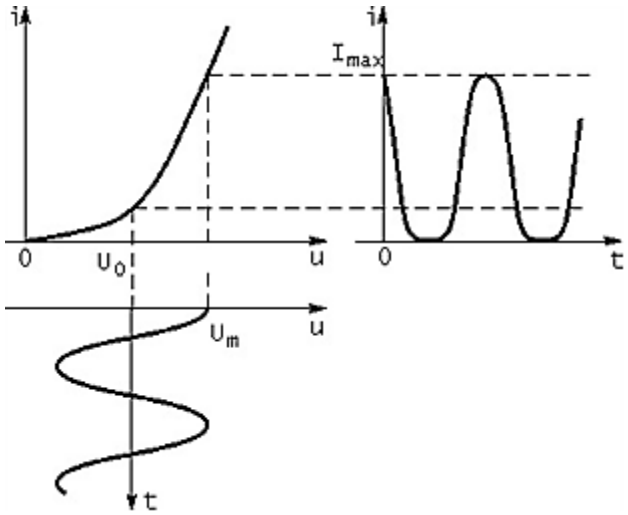


Рис. 3.10. Появление нелинейных искажений сигнала из-за нелинейности входной характеристики транзистора

Таким образом, предлагается новый принцип маскирования сигнала в радиоканале: дополнительное его усиление в усилителе мощности с высоким КПД, работающем в существенно-нелинейном режиме. Вместо обычной в усилителях борьбы с нелинейными искажениями их появление, наоборот, стимулируется известными из теории и практики усиления сигналов приемами. Их много: перегрузка усилителя по входу сигналами с большой амплитудой; выбор УНЭ с существенно нелинейной статической вольт-амперной характеристикой; применение магнитных усилителей; повышение напряжения источника питания усилителя; выбор рабочей точки на нелинейном участке вольт-амперной характеристики изменением напряжения смещения; применение ключевых режимов работы усилителя и др. По своей физической сущности нелинейные искажения в усилителе являются по отношению к усиливаемому сигналу классическими мультипликативными помехами [95, 96].

Указанный принцип положен в основу соответствующего метода маскирования сигналов в радиолинии. Практически метод реализуется в простейшей и экономичной схеме усилителя мощности, обеспечивающей наибольший КПД при максимально возможных нелинейных искажениях.

Структурная схема установки, реализующей метод маскирования информационного сигнала в радиоканале, приведена на рис 3.11.

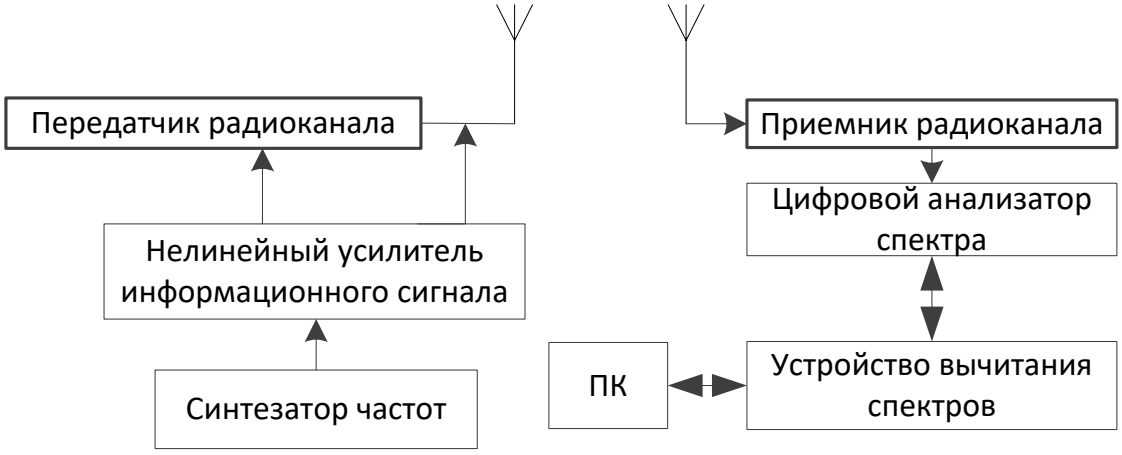


Рис. 3.11. Структурная схема установки, реализующей метод маскирования информационного сигнала в радиоканале

Основным дополнительным новым элементом схемы является нелинейный усилитель информационного сигнала, сопрягаемый со штатным передатчиком радиосредства. В зависимости от принципов построения и особенностей передатчика нелинейный усилитель может быть подключен к передатчику радиоканала следующим образом:

1. Как выходной каскад штатного усилителя мощности передатчика радиоканала между передатчиком и антенной (мультипликативная помеха формируется на большой мощности).

2. Маломощный нелинейный усилитель подключают к выходу формирователя информационного сигнала (до модулятора), помеха формируется на видеочастоте.

3. Между модулятором и оконечным усилителем мощности информационного сигнала.

4. В любой каскад усилителя мощности.

5. Нелинейный усилитель может быть выполнен в виде ретранслятора информационного сигнала, но с нелинейными искажениями (маскирующая помеха формируется не в тракте, а по электромагнитному полю). При этом передатчик работает в штатном режиме.

6. Один из каскадов штатного передатчика переводится в существенно нелинейный режим.

Возможны и другие варианты практической реализации предлагаемого метода. Каждый из указанных технических вариантов реализации метода маскирования сигнала в радиолинии имеет свои достоинства и недостатки.

На рис. 3.11 приведена обобщенная схема для реализации предлагаемого метода зашумления канала связи. Конкретные инженерные решения поставленной задачи могут быть самыми разнообразными. Как вариант,

приведем один из возможных фрагментов реализации усилителя сигнала с нелинейными искажениями.

Формирователь-усилитель может быть выполнен по схеме Кана. Методу Кана присущи специфические нелинейные искажения, вызванные несинхронностью воздействия на перемножитель усиленных компонентов сигнала. Структурная схема формирователя-усилителя, реализующая метод Кана, приведена на рис. 3.12.

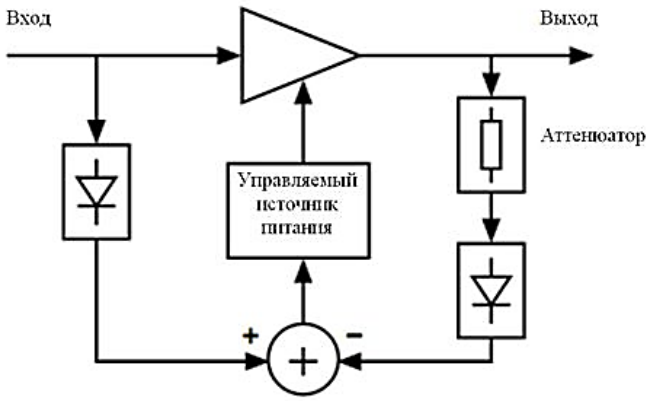


Рис. 3.12. Структурная схема усилителя по методу Кана

Это связано с разностью временных задержек сигнала в высокочастотном и низкочастотном трактах передатчика (в основном за счет инерционности ФНЧ, выделяющего огибающую сигнала). С целью компенсации этих задержек либо вводят линию задержки (ЛЗ) в ВЧ тракт, либо применяют дополнительное фазовое детектирование клиппированного сигнала в схеме Кана с последующей фазовой модуляцией на той же или на другой несущей частоте с фильтром НЧ в фазовом детекторе, вносящем такую же задержку, что и фильтр (на выходе тракта огибающей). Сигналы помехи на выходе схемы Кана являются коррелированными с полезным сигналом.

Специалисты по разработке высококачественных аудиосистем знают, что появление высших гармоник (октав) в спектре звука приводит к снижению качества воспринимаемого ухом сигнала, но почти не приводит к уменьшению разборчивости речи. В наибольшей степени разрушают разборчивость речи комбинационные межгармонические составляющие спектра. Исходя из этого, на вход нелинейного усилителя сигналов целесообразно подавать дополнительно сетку гармонических сигналов с большой амплитудой для получения на выходе усилителя большого количества новых искусственно созданных комбинационных спектральных составляющих. Наилучшими маскирующими свойствами обладают комбинационные излучения 3-го и 5-го порядков, поскольку они на частотной оси либо

близко прилегают к спектру усиливаемого сигнала, либо находятся внутри него.

Технически такой прием обогащения спектра излучаемого сигнала комбинационными составляющими просто реализуется с помощью дополнительно применяемого синтезатора частот.

Поясним механизм образования указанных комбинационных составляющих (в передатчиках при внешнем воздействии в теории электромагнитной совместимости их также называют интермодуляционными).

Комбинационные составляющие возникают на выходе усилителя при действии на его входе двух или более сигналов. В результате взаимодействия сигналов с частотами $f1$ и $f2$ на нелинейном усилительном элементе в передатчике возникают интермодуляционные продукты вида

$$f_{mn} = \pm m \cdot f1 \pm n \cdot f2, \qquad (3.11)$$

где m и n – целые числа.

Результаты нелинейного преобразования сигналов вплоть до третьего порядка приведены на рис. 3.13. В нашем случае они являются мультипликативными помехами для разведывательного приемника.

При подаче на вход УНЭ двух сигналов с частотами f_1 и f_2 вследствие его нелинейных свойств возникают продукты нелинейного преобразования (комбинационные составляющие в обогащенном спектре).

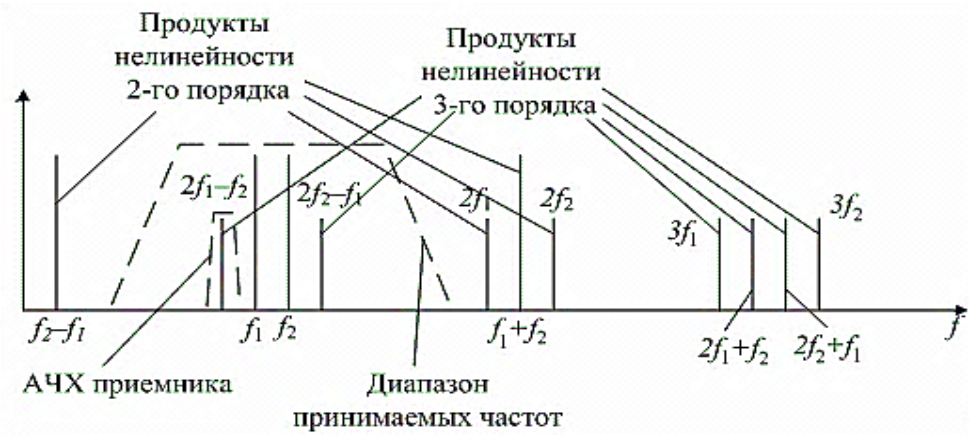


Рис. 3.13. Механизм возникновения комбинационных искажений

2. Сущность метода приема и обработки информационных сигналов на фоне мультипликативных помех

Замаскированный мультипликативной помехой и излученный в пространство информационный сигнал необходимо принять на другом конце радиоканала и извлечь из него полезную информацию. Для решения этой задачи используются приемник радиоканала и цифровое устройство вычитания спектров. Методика обработки полезных сигналов на фоне мультипликативных помех сводится к выделению полезных спектральных составляющих информационного сигнала из спектра искаженного сигнала. Она включает следующие технологические операции:

– с помощью цифрового анализатора спектра, подключаемого к выходу промежуточной частоты (ПЧ) приемника радиоканала (при необходимости – через алфавитно-цифровой преобразователь), анализируют спектральный со-став принятого сигнала;

– в цифровом устройстве вычитания спектров после масштабирования вычитают из широкого общего искаженного спектра известный усредненный спектр информационного сигнала и таким образом получают спектр искажений (он же – спектр маскирующей мультипликативной помехи);

– восстанавливают полезный информационный сигнал на приемной стороне путем вычитания спектра искажений из широкого общего искаженного спектра.

Методика тестирования модели канала с аддитивными и мультипликативными помехами и результаты оценки пропускной способности представлены в работах [95, 96].

3. Экспериментальная проверка метода.

Проверка работоспособности метода производится с помощью простого эксперимента. Посредством применения векторного генератора сигналов формируется аналог OFDM-сигнала в звуковом диапазоне: например два гармонических сигнала одинаковой амплитуды с разносом по частоте в 50 кГц. Указанный сигнал усиливается в любом усилителе низкой частоты с небольшим коэффициентом усиления и наблюдается его спектр. Усилитель переводится в нелинейный режим простейшим способом, например, перегрузкой по входу путем увеличения амплитуды входного сигнала (аналога OFDM). Спектры фотографируются и анализируются. Вычитание спектров производится с помощью векторного анализатора спектра, подключенного к персональному компьютеру.

При измерении амплитуд комбинационных помех на вход усилителя подают два гармонических сигнала (рис. 3.14). Методика измерения комбинационных помех приведена в ГОСТ 12252 – 86.

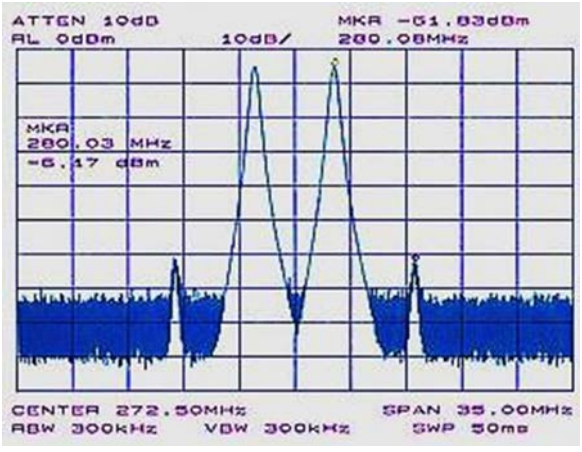


Рис. 3.20. Спектр сигнала при подаче на вход усилителя двух гармонических сигналов одинаковой амплитуды

Коэффициент интермодуляционных искажений второго порядка определяется как отношение амплитуды комбинационной составляющей (f2 ± f1) к амплитуде одного из входных сигналов. Обычно этот коэффициент выражается в относительных единицах – децибелах относительно несущей (дБс). Если диапазон частот приемного устройства достаточно узок, как это имеет место для систем УКВ мобильной связи или систем сотовой связи, то комбинационные частоты второго порядка образуются за диапазоном принимаемых частот и подавляются входным фильтром приемника.

На практике для количественной оценки комбинационных и интермодуляционных искажений (InterModulation Distortion, IMD) используют коэффициенты, вычисляемые при подаче на вход приемника двух внеполосных гармонических сигналов f1 и f2 с равными ам-плитудами: коэффициент интермодуляционных искажений третьего порядка – отношение амплитуды комбинационной составляющей (2·f2 – f1) или (2·f1 – f2) к амплитуде одного из этих сигналов на входе.

Продукты третьего и более высоких порядков, возникающие при смешивании двух интерферирующих радиосигналов представляют для нас наибольший интерес. Так как полоса обрабатываемых частот обычно ограничивается в преселекторе на входе приемника, то нелинейность измеряется путем подачи на вход приемного устройства двух сигналов равной амплитуды с частотами f1 и f2, достаточно близко расположенными к частоте настройки приемника. При этом измеряется уровень продуктов интермодуляции третьего порядка (2·f1 – f2) и (2·f2 – f1). Другие комбинационные продукты обычно находятся вне полосы рабочих частот приемника и подавляются фильтром основной избирательности.

Предложенный метод маскирования сигналов радиосвязи в радиоканале характеризуется простотой аппаратурной реализации. Недостатком метода является усложнение проблемы электромагнитной совместимости радиосредств. Эффективность получаемых мультипликативных маскирующих помех необходимо исследовать метода-ми моделирования и экспериментальной проверки в лабораторных и натурных условиях применительно к различным видам модуляции полезных сигналов.

3.4. Методика построения нейронной сети, решающей задачи выбора способов противодействия деструктивным электромагнитным воздействиям в сетях связи специального назначения

Для решения задачи выбора способов противодействия деструктивным электромагнитным воздействиям авторами были выбраны нейронные сети, поскольку технологии искусственного интеллекта в информационной безопасности радиосетей являются перспективными. Существует большое количество программных продуктов, позволяющих осуществить моделирование различного типа нейронных сетей, таких как Cortex, NeuroShell

Predictor, STATISTICA и др. Выберем в качестве инструмента моделирования программный пакет STATISTICA Neural Networks (SNN) поскольку эта программная реализация поддерживает выбор наиболее популярных сетевых архитектур (многослойные персептроны, радиальные базисные функции и самоорганизующиеся карты признаков) при этом могут быть реализованы самые современные алгоритмы обучения, включая метод сопряженных градиентов, алгоритм Левенберга – Марквардта, BFGS, алгоритм Кохонена [105].

Первым этапом построения является задание процентного отношения количества правил для обучения. Согласно [105] выбрано следующее процентное соотношение:

– тренировочная выборка – 70%;

– тестовая выборка – 30%;

– проверочная выборка – 15%.

Вторым этапом является использовние полученной ранее базы знаний по методам противодействия, построенной с использованием аппарата нечетких множеств [105]. Как пример, такая база может содержать реализацию следующих входных параметров: мощность помехи (power), возможность функционирования системы (functioning), оперативность передаваемой информации (operativeness), наличие информации рангом выше (rank). Выходными параметрами являются способы противодействия деструктивным электромагнитным воздействиям: обычный режим (normal mode), ожидание (expectation), использование многосекторной антенной системы (MIMO), очередь (turn) и использование резервного канала (backup channel). Используемая в статья база знаний для обучения сети приведена в табл. 3.1.

Используемые в таблице способы противодействия и входные параметры нейронной сети были выбраны в соответствии с [105]. В столбце functioning значению 0,1 соответствует нормальное функционирование, значению 0,5 – частичное функционирование, значению 0,9 – система не функционирует. В столбце operativeness значению 0,1 соответствует повседневная информация, значению 0,5 – срочная информация, значению 0,9 – оперативная информация. В столбце rank значению 0,2 соответствует отсутствие информации рангом выше, значению 0,8 – наличие информации рангом выше.

Следует отметить, что данная база знаний не является исчерпывающей и при появлении новых данных ее элементы будут пополняться.

Третьим этапом является выбор структуры нейронной сети и алгоритма обучения. Программа поддерживает структуру многослойного перцептрона (MLP) и радиальной базисной функции (RBF). Алгоритмы обучения: BFGS и RBFT.

Таблица 3.23. – База знаний для обучения системы.

№	power	functioning	operativeness	rank	way to counter
1	-156	0,1	0,9	0,2	normal mode
2	-135	0,1	0,1	0,2	normal mode
3	-144	0,1	0,5	0,2	normal mode
4	-133	0,1	0,9	0,8	normal mode
5	-154	0,1	0,1	0,2	normal mode
6	-131	0,1	0,5	0,2	normal mode
7	-145	0,1	0,9	0,8	normal mode
8	-158	0,1	0,1	0,8	normal mode
9	-115	0,5	0,1	0,2	expectation
10	-115	0,5	0,5	0,2	MIMO
11	-108	0,5	0,9	0,2	MIMO
12	-115	0,5	0,1	0,8	turn
13	-114	0,5	0,5	0,8	turn
14	-108	0,5	0,5	0,2	MIMO
15	-106	0,5	0,5	0,8	turn
16	-110	0,5	0,9	0,2	MIMO
17	-105	0,5	0,1	0,2	expectation
18	-104	0,9	0,1	0,2	backup channel
19	-78	0,9	0,5	0,2	backup channel
20	-102	0,9	0,9	0,2	backup channel
21	-89	0,9	0,1	0,8	turn
22	-100	0,9	0,5	0,8	turn
23	-54	0,9	0,9	0,2	backup channel
24	-65	0,9	0,1	0,2	backup channel
25	-78	0,9	0,5	0,2	backup channel
26	-96	0,9	0,9	0,2	backup channel
27	-89	0,9	0,1	0,8	turn
28	-94	0,9	0,5	0,8	turn

Метод BFGS или алгоритм Бройдена – Флетчера – Гольдфарба – Шанно (Broyden – Fletcher – Goldfarb – Shanno) для вычисления обратного гессиана H^{-1} (обратный гессиан $V \approx H^{-1}$ – это матрица размера $n \times n$, где n – длина вектора градиента g) использует изменение значений градиента ∇E и изменения весов ΔW. Значения V вычисляются на каждом шаге алгоритма следующим образом:

$$V_0 := 1$$

$$V_{k+1} := V_k - \frac{V_k \cdot s \cdot s^T \cdot V_k}{s^T \cdot V_k \cdot s} + \frac{r \cdot r^T}{s^T \cdot s}, \qquad (3.2)$$

где $r = \Delta g_k = g_k - g_k - 1$ – изменение градиента, $s = \Delta W_k = W_k - W_{k-1}$ – изменение весов.

Общая схема алгоритма BFGS подразумевает выполнения следующих этапов:

1. Инициализируются веса W (случайными малыми значениями) и задается начальное значение приближения обратного гессиана $H^{-1} \approx V0=1$

2. Вычисляются значения градиента g.

3. Корректируются веса: $\Delta W:=g\cdot\tau$, $W:=W-\Delta W$, где $\tau = 0.01$ – параметр скорости обучения.

4. Сохраняется старое значение градиента $g_{old}:=g$; вычисляется новое значение градиента g(W) и изменение градиента $\Delta g:=g-g_{old}$.

5. Вычисляется приближенное значение обратного гессиана $V(\Delta g,\Delta W)$ по формуле (3.12).

6. Вычисляется изменение весов и корректируются параметры: $\Delta W:=V\cdot g \Delta W:=V\cdot g$, $W:=W-\Delta W$.

7. Вычисляется ошибка E(W).

8. Если результат E(W) удовлетворительный, то конец работы.

9. Переход на п. 4.

Алгоритм RBFT является реализацией рекурсивной задачи Византийских генералов [105], описывающей взаимодействия нескольких удалённых абонентов, которые получили приказы из одного центра. Часть абонентов, включая центр, могут быть злоумышленниками. Нужно выработать единую стратегию действий, которая будет выигрышной для абонентов [105].

В качестве функции активации скрытых и выходных слоев нейронов примем логистическую (сигмоидальную или Softmax) функцию активации, так как она является наиболее подходящей функцией для задач идентификации рис. 3.15 [109]. Данная функция стремится привести значения к одной из сторон кривой, что позволяет находить четкие границы при предсказании. Такой вид функции применяется в машинном обучении для задач идентификации, когда количество возможных классов больше двух.

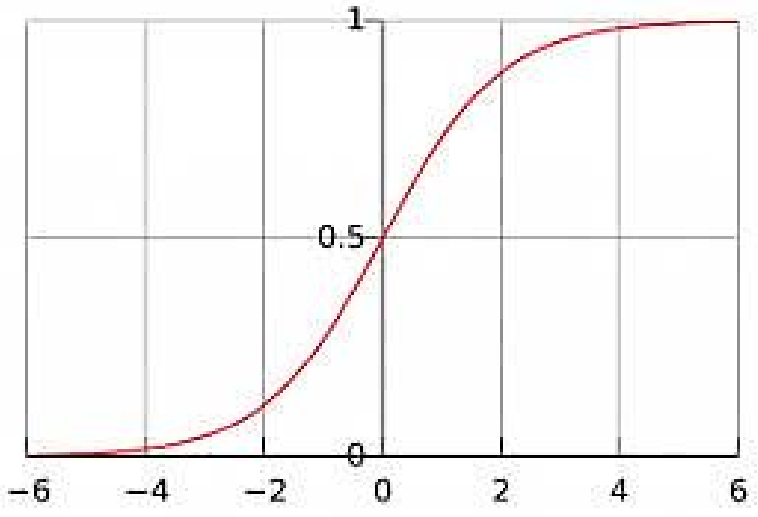


Рис. 3.15. Функции активации Softmax

Количество эпох обучения зададим равным 2000, скорость обучения 1000, поскольку такое количество эпох при данной скорости обучения позволяет хорошо обучить сеть и свести показатель ошибки к значению 0,0000001. Веса зададим по умолчанию одинаковыми и равными 1. Смоделировано было по 10 сетей каждого из 2 типов. Выборка результатов моделирования приведена в таблице 3.2.

Таблица 3.2. – Выборка из результатов моделирования структуры сетей

№	Структура сети	Тренировочная последовательность	Тестовая последовательность	Проверочная последовательность	Алгоритм обучения
1	RBF 4-3-5	70,0000	100,0000	0,0000	RBFT
2	RBF 4-3-5	65,0000	100,0000	50,0000	RBFT
3	RBF 4-3-5	100,0000	75,0000	100,0000	RBFT
4	RBF 4-3-5	95,0000	50,0000	25,0000	RBFT
5	RBF 4-3-5	80,0000	75,0000	25,0000	RBFT
6	RBF 4-3-5	75,0000	100,0000	50,0000	RBFT
7	MLP 4-3-5	85,0000	100,0000	75,0000	BFGS 6
8	MLP 4-3-5	95,0000	100,0000	100,0000	BFGS 14
9	MLP 4-5-5	90,0000	100,0000	75,0000	BFGS 11
10	MLP 4-3-5	100,0000	100,0000	100,0000	BFGS 7
11	MLP 4-3-5	90,0000	100,0000	100,0000	BFGS 8
12	MLP 4-3-5	95,0000	100,0000	100,0000	BFGS 23

Результаты выбора нейронной сети. На основании результатов проведенного моделирования было выявлено, что задачу выбора способов противодействия деструктивным элекромагнитным воздействиям решает нейронная сеть типа многослойный перцептрон структуры 4-3-5 с весами связей, (4 входных нейрона, 3 нейрона на скрытом слое, 5 выходных нейронов) рис. 3.16.

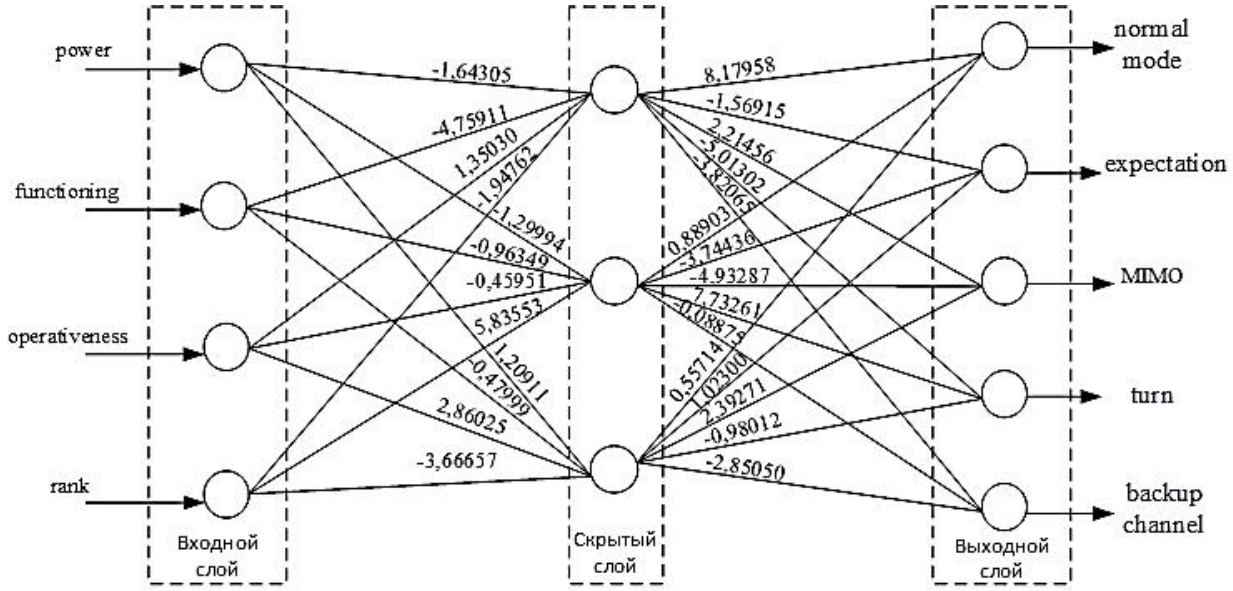


Рис 3.16. Структура и веса связей сети MLP 4-3-5

В результате моделирования, показатели чувствительности нейронной сети к обучению характеризуются значениями, приведенными в табл. 3.3.

Таблица 3.3. – Анализ чувствительности.

functioning	rank	power	operativeness
11,31203	5,878662	2,078399	1,193872

Согласно данным из таблице 3.3 наибольшее влияние на выбор способов противодействия оказывают переменная functioning и rank, переменные power и operativeness оказывают влияние в меньшей мере.

На основе результатов моделирования также были получены лифтовые карты, (рис. 3.17), представляющие собой зависимость необходимого для обучения сети количества наблюдений от общего количества наблюдений.

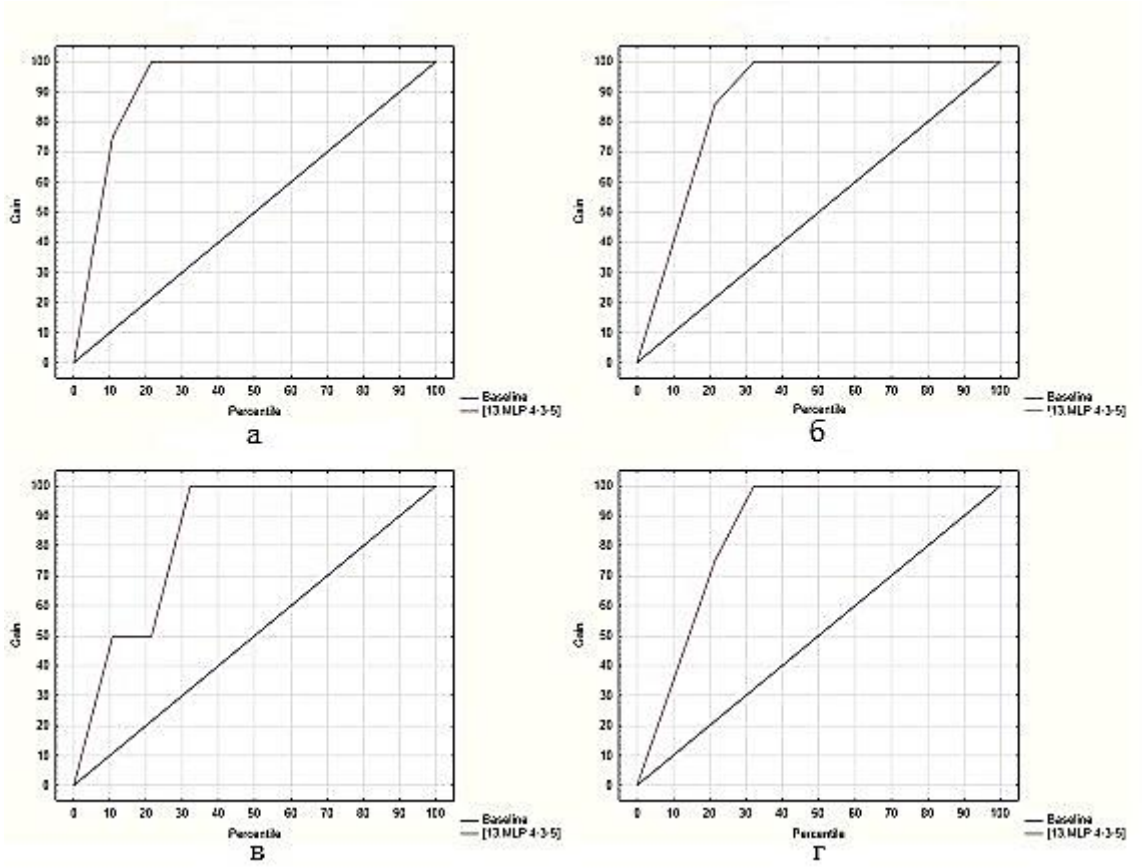


Рис. 3.17. Лифтовые карты полученной сети

Из рисунка видно, что при обучении нейронной сети имеют наибольшее значение: первые 20% наблюдений для способа MIMO (рис. 3.17, а), 32% наблюдений для способа turn (очередь) (рис. 3.17, б), 34 % наблюдений для способа expectation (ожидание) (рис. 3.17, в), 30 % наблюдений для способа backup channel (резервный канал) (рисунок не приведен) и 32 % наблюдений для способа normal mode (обычный режим) (рис. 3.17, г). Построим поверхность зависимостей способа противодействия normal mode от входных данных power и operativeness от (рис. 3.18).

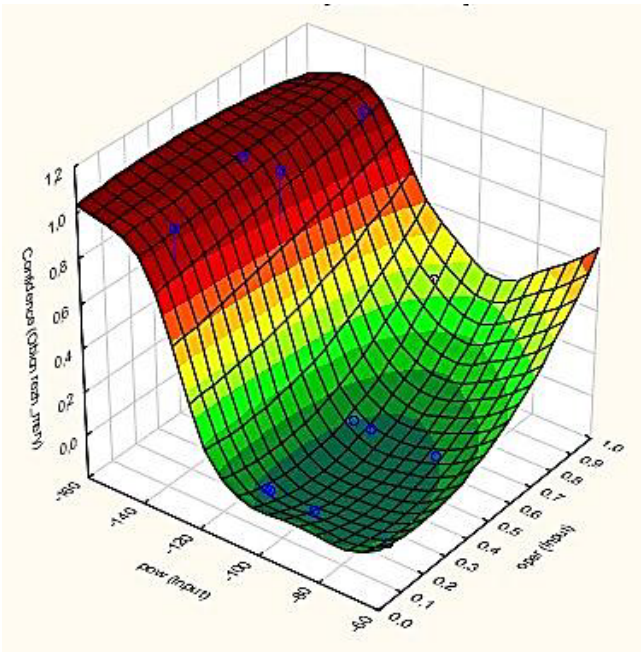


Рис. 3.18. Поверхность зависимостей способа противодействия «normal mode» от входных данных «power» и «operativeness»

Из данных представленных на рис. 3.18, видно, что при любом значении переменной operativeness (оперативность информации) и переменной power (мощность помехи) менее –140 Дбм в качестве способа противодействия деструктивному электромагнитному воздействию может быть выбрано использование normal mode (обычного режима функционирования). При увеличении переменной power (мощности помехи), воздействующей на систему связи, будут применяться другие способы противодействия, а эффективность применения данного способа сводится к минимуму.

Работоспособность сети также была протестирована на выборке новых входных параметров, в ходе которой сети задавались входные переменные и в результате работы сети был выбран корректный способ противодействия. Например, при заданной переменной power (мощность помехи) –79 Дбм, значении переменной functioning = 0,9 (не функционирует), oper = 0,9 (оперативная информация) и значении перменной rank = 0,2 (отсутствие информации рангом выше) сеть определяет корректный способ противодействия backup channel (использование резервного канала).

Таким образом, в данной разделе была разработана методика построения нейронной сети для выбора способов противодействия деструктивным электромагнитным воздействиям в системах связи специального назначения. Результаты моделирования показали, что наиболее эффективно задачу выбора способа противодействия деструктивным электромагнитным воздействиям решает нейронная сеть, структуры многослойный перцептрон с тремя скрытыми нейронами. Были построены лифтовые кар-

ты, описывающие обучение сети на входных данных, определены весовые коэффициенты нейронной сети. Работоспособность сети протестирована на новых, не известных ранее ситуациях, и работа сети продемонстрировала осуществление выбора корректной меры противодействия деструктивным электромагнитным воздействиям. Программная реализация данной методики позволяет автоматизировать выбор способов противодействия деструктивным электромагнитным воздействиям с целью минимизации их негативного влияния на сети связи специального назначения.

Выводы

В третьей главе разработана и обоснована методология моделирования комплекса средств противодействия угрозам информационной безопасности в условиях информационного конфликта. Разработанная методология моделирования комплекса средств противодействия угрозам информационной безопасности отличается применением внутрисистемных и внешних показателей эффективности функционирования и позволяет в итерационном режиме осуществлять оптимизацию эргатических систем предметного назначения.

Методической основой решения задачи разработки математических моделей для оценки эффективности средств интегрированной защиты информации комплексных систем безопасности объектов являются правила структуризации показателей эффективности противодействия. В основу синтеза структуры показателей эффективности средств интегрированной защиты информации комплексных систем безопасности объектов положено их представление в виде иерархической системы, отражающей существующую иерархию задач защиты информации. Классификация показателей эффективности средств интегрированной защиты информации комплексных систем безопасности объектов отражает степень влияния возможностей этих средств на обеспечение защищенности объектов:

– первый класс характеризует возможности средств интегрированной защиты информации, связанные с особенностями реализации механизмов обработки и защиты информации в комплексных системах безопасности объектов;

– второй класс характеризует возможности, связанные с предупреждением условий появления угроз, поиском, обнаружением и обезвреживанием как самих угроз, так и их источников, а также с восстановлением информационных процессов после воздействия угроз;

– третий класс характеризует возможности, связанные с предотвращением нарушения основных состояний информации – конфиденциальности, доступности и целостности;

– четвертый класс описывает свойство средств интегрированной защиты информации, характеризующее степень достижения целей функцио-

нирования этих средств – предотвращение ущерба объекту от нарушения его информационной безопасности.

Для оценки характеристик средств интегрированной защиты информации как элементов комплекса средств противодействия угрозам информационной безопасности СССН в монографии применяются логико-лингвистические модели. Для формализации отношений между причинами из их множества с использованием аппарата синтагматических цепей логическое выражение, описывающее произвольную комбинацию причинно-следственных связей, можно представить в виде цепочки синтагм, связанных между собой.

Анализ результативности процедур систематизации характеристик комплекса средств противодействия угрозам информационной безопасности СССН при систематизации характеристик средств интегрированной защиты информации в условиях традиционного, количественного подхода выявил, что в условиях иерархически структурированной системы характеристик традиционный подход к их обобщенной оценке является нерезультативным ввиду низкого значения показателя точности моделирования.

При рассмотрении алгоритмов противодействия при воздействии сверхширокополосных помех на системы передачи видеоинформации получены следующие выводы. Решением для передачи видео и звука являются системы с модуляцией COFDM. Благодаря большому числу поднесущих частот в комбинации с помехоустойчивым кодированием возможно восстановление отдельных поднесущих, ослабленных вследствие частотно-селективных замираний в канале. При всех достоинствах рассматриваемых систем данный вид модуляции имеет существенные недостатки – большое отношение пиковой мощности сигнала к его усредненной мощности (пикфактор сигнала), а также эффект нарушения ортогональности поднесущих частот в нестационарных каналах связи с многолучевостью, приводящий к взаимным перекрестным помехам между поднесущими частотами. Информационные сигналы также очень чувствительны к системным нестабильностям, что в отдельных случаях может приводить к существенному росту внеполосных излучений. Помехи в радиоэфире от других радиоэлектронных средств на рабочем частотном канале приводят к искажениям изображения и звука. В этом случае необходимо сменить частотный канал, убедиться в отсутствии других радиоизлучающих средств, попадающих в полосу работы системы. Методика количественной оценки влияния радиопомех и сигнала радиоэлектронных средств на показатели радиоэлектронной защиты рассмотрена авторами в работах [88 – 91].

Таким образом, в результате экспериментального исследования выявлено воздействие друг на друга радиосредств органов внутренних дел, работающих в одной полосе частот. Это наглядно показано в случае работы аналогового радиосредства в том же частотном диапазоне. Однако при

использовании цифрового радиосредства, не входящего в состав комплекса, влияние на спектр также присутствует, но на передачу видеоданных это не оказывает существенного воздействия. Данные эксперимента показывают, что в случае возникновения селективных замираний и некорректной работы комплекса передачи видео и звука рекомендуется проводить работы по анализу спектра при настройке и монтаже систем связи специального назначения с целью минимизации взаимного влияния радиооборудования.

Предложенный метод защиты информации в каналах связи методом формирования маскирующих сигналоподобных помех характеризуется простотой аппаратурной реализации. Недостатком метода является усложнение проблемы электромагнитной совместимости радиосредств. Эффективность получаемых мультипликативных маскирующих помех необходимо исследовать методами моделирования и экспериментальной проверки в лабораторных и натурных условиях применительно к различным видам модуляции полезных сигналов.

Разработана методика построения нейронной сети для выбора способов противодействия деструктивным электромагнитным воздействиям в системах связи специального назначения. Результаты моделирования показали, что наиболее эффективно задачу выбора способа противодействия деструктивным электромагнитным воздействиям решает нейронная сеть, структуры многослойный перцептрон с тремя скрытыми нейронами. Были построены лифтовые карты, описывающие обучение сети на входных данных, определены весовые коэффициенты нейронной сети. Работоспособность сети протестирована на новых, не известных ранее ситуациях, и работа сети продемонстрировала осуществление выбора корректной меры противодействия деструктивным электромагнитным воздействиям. Программная реализация данной методики позволяет автоматизировать выбор способов противодействия деструктивным электромагнитным воздействиям с целью минимизации их негативного влияния на сети связи специального назначения.

Глава 4.
МЕТОДЫ И МОДЕЛИ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕТЯХ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

4.1. Математическая модель комплекса средств противодействия угрозам информационной безопасности в СССН, основанная на применении лингвистических переменных и нечетких экспертных систем

Существует большое количество работ посвященных вопросам моделирования вопросов безопасности инфокоммуникационных систем с позиции управления и развития теории информационной безопасности: А. Н. Буренин, К. Е. Легков [2, 3], С. И. Макаренко [4, 5], Н. С. Хохлов [7], В. И. Новосельцев, С. С. Кочедыков, Д. Е. Орлова [8], А. А. Малюк [9], Д. А. Новиков [12], И. М. Ажмухамедов [53], В. И. Завгородний [54] и др.

В данном разделе монографии рассмотрим построение математической модели комплекса средств противодействия угрозам информационной безопасности в СССН, построенной с применением лингвистических переменных и нечетких экспертных систем. В качестве основного инструмента при прогнозировании состояния и средств противодействия угрозам информационной безопасности целесообразно использовать нечеткие экспертные системы, поскольку задача прогнозирования состояния системы в условиях информационных поражающих воздействий является сложной (с математической точки зрения) задачей и требует учета всех возможных параметров системы и воздействий [16]. В качестве исходной авторами предложена модель, основанная на концепции комплексной защиты информации [9].

Данная модель позволяет визуализировать эффективность средств противодействия с учетом реализации защиты СССН. Для моделирования нечеткой экспертной системы уместно использовать пакет Fuzzy Logic Toolboks программы Matlab [13, 106]. Для заполнения базы знаний введем в рассмотрение значения лингвистических переменных:

f1 – предупреждение возникновения условий, способствующих возникновению деструктивных факторов, F1 = {НЕ СОБЛЮДАЕТСЯ, СОБЛЮДАЕТСЯ}, [0,1];

f2 – предупреждение непосредственного проявления деструктивных факторов, F2 = {НЕ СОБЛЮДАЕТСЯ, СОБЛЮДАЕТСЯ}, [0,1];

f3 – обнаружение проявившихся деструктивных факторов, F3 = {НЕ СОБЛЮДАЕТСЯ, СОБЛЮДАЕТСЯ}, [0,1];

f4 – предупреждение воздействия на защищаемую информацию и обнаружение деструктивных факторов, F4 = {НЕ СОБЛЮДАЕТСЯ, СОБЛЮДАЕТСЯ}, [0,1];

f5 – обнаружение воздействия деструктивных факторов на защищаемую информацию, F5 = {НЕ СОБЛЮДАЕТСЯ, СОБЛЮДАЕТСЯ}, [0,1];

f6 – локализация обнаруженного воздействия деструктивных факторов на защищаемую информацию, F6 = {НЕ СОБЛЮДАЕТСЯ, СОБЛЮДАЕТСЯ}, [0,1];

f7 – ликвидация последствий локализированного обнаруженного воздействия деструктивных факторов на информацию, F7 = {НЕ СОБЛЮДАЕТСЯ, СОБЛЮДАЕТСЯ}, [0,1].

Функции принадлежности термов комплекса средств противодействия изображены на рисунке 4.1. OUT – результаты противодействия O = {ЗАЩИТА ОБЕСПЕЧЕНА, ЗАЩИТА НАРУШЕНА, ЗАЩИТА РАЗРУШЕНА}, [0,1].

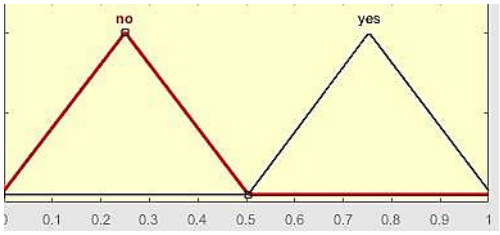


Рис. 4.1. Функции принадлежности термов комплекса средств противодействия

На рис. 4.2 приведена структурная схема модели комплекса средств противодействия угрозам информационной безопасности в СССН, основанная на применении лингвистических переменных и нечетких экспертных систем.

В модели каждый из исходов является случайным, а все вместе они составляют полную группу событий, не происходящих единовременно. Из теории вероятностей известно, что сумма таких событий равна единице. Благоприятными с точки зрения работы комплекса будут те исходы, при которых сумма их вероятностей будет равна единице «Z1 – Защита обеспечена». В ином случае результатами работы комплекса будут «Z2 – Защита нарушена» или «Z3 – Защита разрушена».

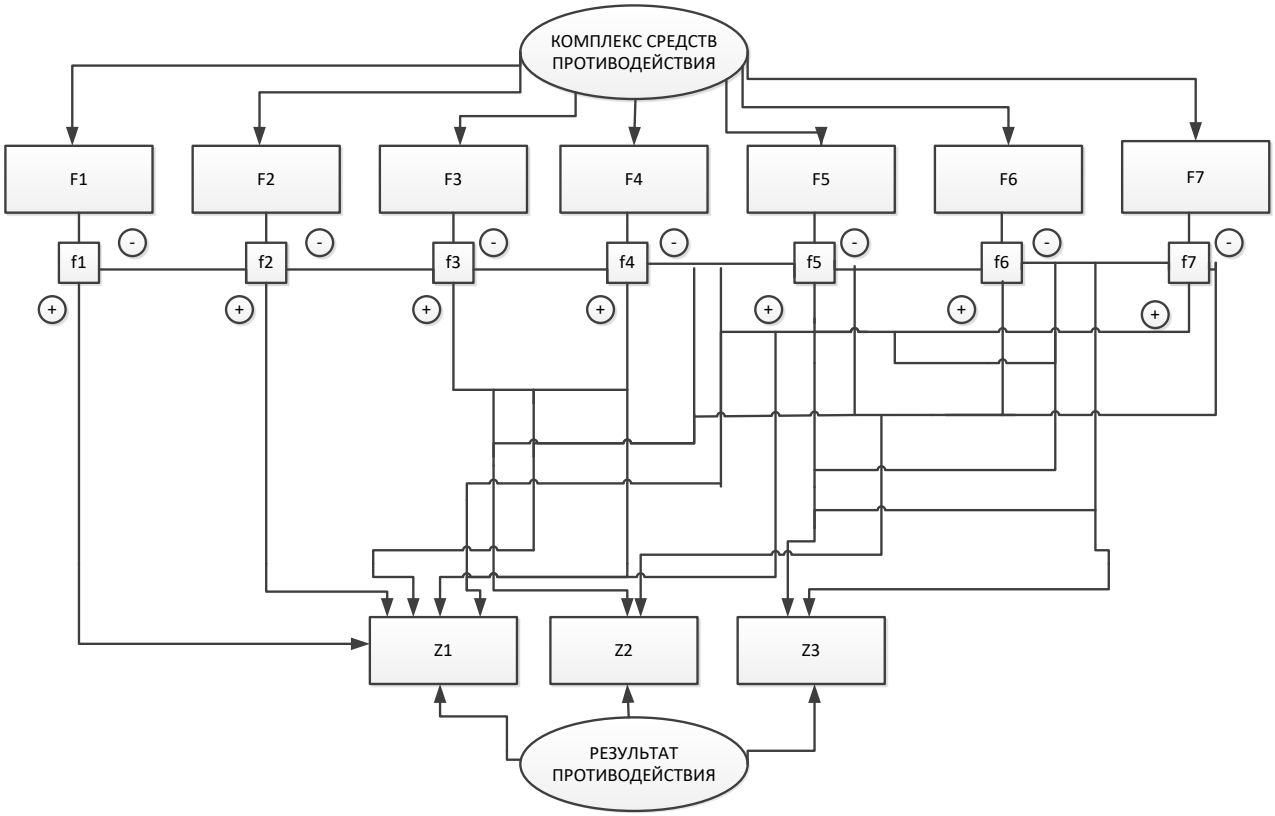


Рис. 4.2. Структурная схема модели комплекса средств противодействия угрозам информационной безопасности в СССН, основанная на применении лингвистических переменных и нечетких экспертных систем

Следующим шагом является создание базы правил, на основании которых будут выбираться определенные средства противодействия. Пример заполнения базы правил на ряде элементов приведен ниже:

1. If f1 = СОБЛЮДАЕТСЯ then Z1 = ЗАЩИТА ОБЕСПЕЧЕНА;

2. If f1 = НЕ СОБЛЮДАЕТСЯ & f2 = СОБЛЮДАЕТСЯ then Z1 = ЗАЩИТА ОБЕСПЕЧЕНА;

3. If f1 = НЕ СОБЛЮДАЕТСЯ & f2 = НЕ СОБЛЮДАЕТСЯ & f3 = СОБЛЮДАЕТСЯ & f4 = СОБЛЮДАЕТСЯ then Z1 = ЗАЩИТА ОБЕСПЕЧЕНА;

4. If f1 = НЕ СОБЛЮДАЕТСЯ & f2 = НЕ СОБЛЮДАЕТСЯ & f3 = НЕ СОБЛЮДАЕТСЯ & f4 = СОБЛЮДАЕТСЯ then Z1 = ЗАЩИТА ОБЕСПЕЧЕНА;

5. If f1 = НЕ СОБЛЮДАЕТСЯ & f2 = НЕ СОБЛЮДАЕТСЯ & f3 = НЕ СОБЛЮДАЕТСЯ & f4 = НЕ СОБЛЮДАЕТСЯ & f5 = СОБЛЮДАЕТСЯ & f6 = НЕ СОБЛЮДАЕТСЯ & f7 = НЕ СОБЛЮДАЕТСЯ then Z3 = ЗАЩИТА РАЗРУШЕНА.

Рисунок 4.3 иллюстрирует пример реализации правила 1, если первое правило соблюдается, то система делает вывод о том, что безопасность обеспечена.

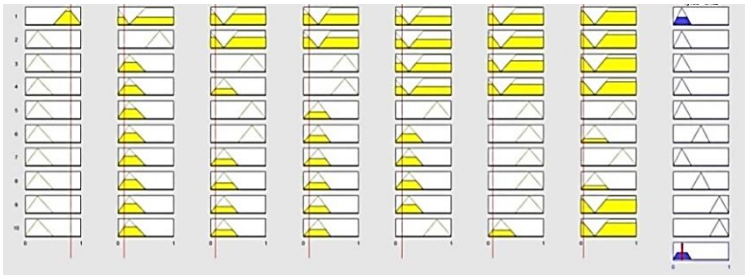


Рис. 4.3. Пример правила 1, если первое правило соблюдается, то система делает вывод о том, что безопасность обеспечена

На рис. 4.4 приведена функциональная схема модели системы.

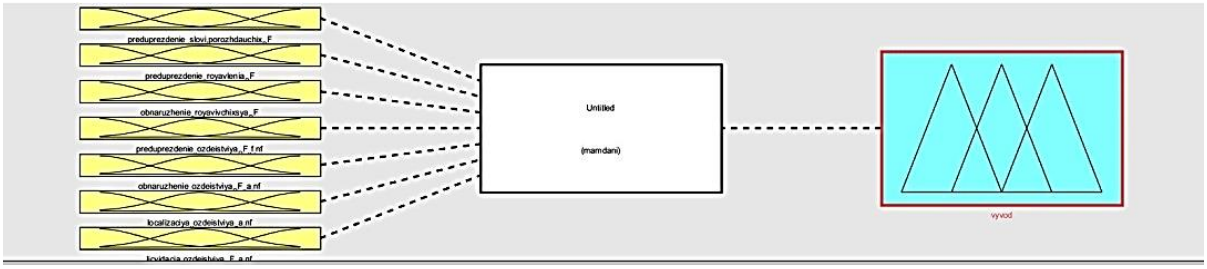


Рис. 4.4. Функциональная схема модели системы

На рис. 4.5 приведена нечеткая зависимость входных переменных от выходных. На данном рисунке представлена зависимость f4 и f2 от выходных переменных.

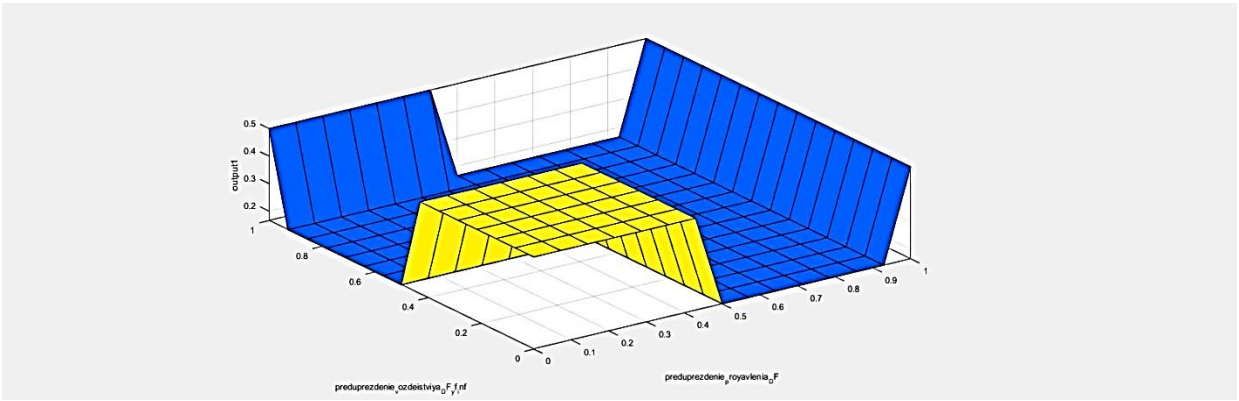


Рис. 4.5. Зависимости средств противодействия от входных переменных

При равенстве f4 и f2 = 0,4 (не соблюдается) из графика видно, что безопасность является нарушенной, а при значении f4 и f2 больше 0,5 вы-

ходное значение будет близко к 0, следовательно, в данном случае можно сделать вывод, что безопасность обеспечивается.

Опираясь на полученные результаты математического моделирования комплекса средств противодействия угрозам информационной безопасности в СССН с применением лингвистических переменных и нечетких экспертных систем, можно разработать требования к формированию комплекса средств противодействия угрозам информационной безопасности в сетях связи специального назначения.

Предложена модель формирования комплекса средств противодействия угрозам информационной безопасности в сетях связи специального назначения, осуществлено исследование общих технологических особенностей формирования комплекса средств противодействия угрозам информационной безопасности в СССН. Авторами проведено моделирование функционирования комплекса средств противодействия на основе аппарата лингвистических переменных и нечетких экспертных систем. На основе полученных результатов могут быть предложены требования к формированию комплекса средств противодействия угрозам информационной безопасности в СССН. Математический аппарат, использованный в данном разделе, основан на применении лингвистических переменных и нечетких экспертных систем, может в полной мере характеризовать зависимость эффективности средств противодействия от совокупности реализуемых средств защиты. В рамках комплексного подхода возможно построение такого рода систем с применением элементов искусственного интеллекта, что будет рассмотрено авторским коллективом в дальнейших исследованиях.

4.2. Методы противодействия угрозам нарушения информационной безопасности в цифровых сетях связи специального назначения

Общую классификацию методов и средств защиты от угроз ИБ можно представить в следующем виде – рис. 4.6.

Процессы защиты от угроз ИБ можно разделить на три группы: предотвращения, парирования и нейтрализации угроз [98].

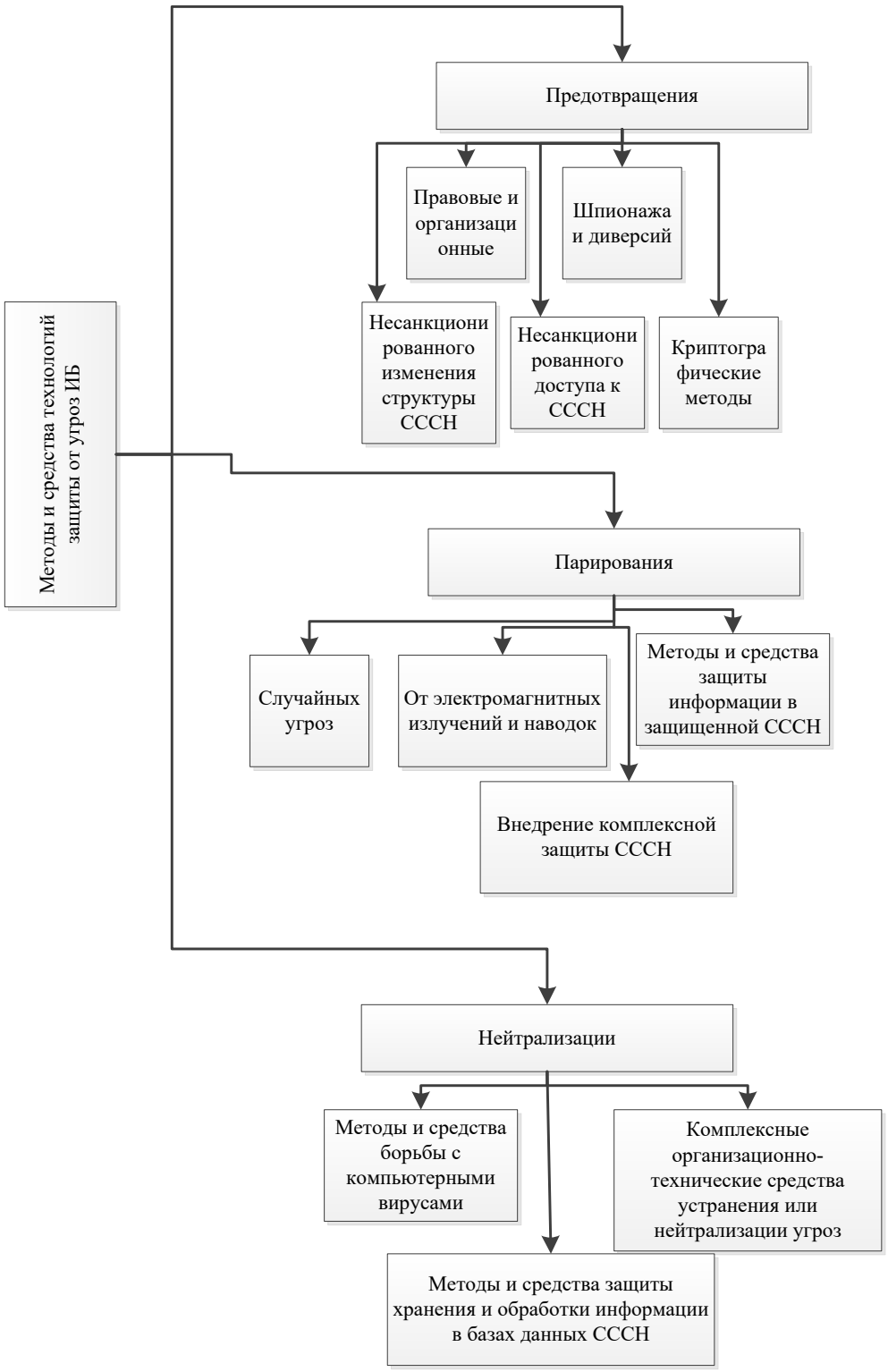


Рис. 4.6. – Схема классификации методов и средств защиты от угроз ИБ

К группе предотвращения угроз ИБ относятся технологические решения, осуществляющие упреждение и предупреждение проникновения, организацию и реализацию защиты СССН при начальном этапе нападения.

К группе технологий парирования отнесены методы и приемы, препятствующие или ограничивающие воздействие на СССН.

К технологиям нейтрализации угроз отнесены средства устранения и ликвидации угроз, а также либо частичной, либо полной нейтрализации в случае успешной реализации вредоносного воздействия на СССН.

4.3. Аппаратно-программные методы и организационные средства защиты информации систем сетевого мониторинга, систем радиосвязи МВД России и навигационно-мониторинговых систем

Актуальным направлением развития навигационно-мониторинговых систем является создание единой технической политики в области реализации, внедрения и интеграции навигационно-информационных систем, создание единой инфраструктуры навигационно-временного обеспечения подразделений МВД России. Создание данной инфраструктуры должно проводиться в тесной взаимосвязи с развитием единой системы информационно-аналитического обеспечения деятельности МВД России (ИСОД МВД России) [98].

В соответствии с концепцией построения ИСОД МВД России все информационные системы должны быть интегрированы в единое информационное пространство.

Интеграция информационных систем – это процесс установки связей между информационными системами подразделений ОВД для получения единого информационного пространства и организации его управления.

В настоящее время большая часть НМС реализована разными производителями для решения вполне конкретных задач, и зачастую такие системы содержат только простые механизмы интеграции с другими ИС ОВД (обычно на уровне передачи информации файлами определенной структуры).

В интересах МВД для комплексной интеграции НМС необходимо создание отраслевой инструментальной системы для интеграции производственных данных (СИПД), сочетающей гибкость универсальных платформ интеграции с высокой производительностью и предметной ориентированностью частных интеграционных решений. Такая инструментальная система должна учитывать специфику выполняемых задач ОВД и легко адаптироваться при решении задач интеграции, используемых НМС в единое информационное пространство. Обобщенная схема СИПД изображена на рисунке 4.7.

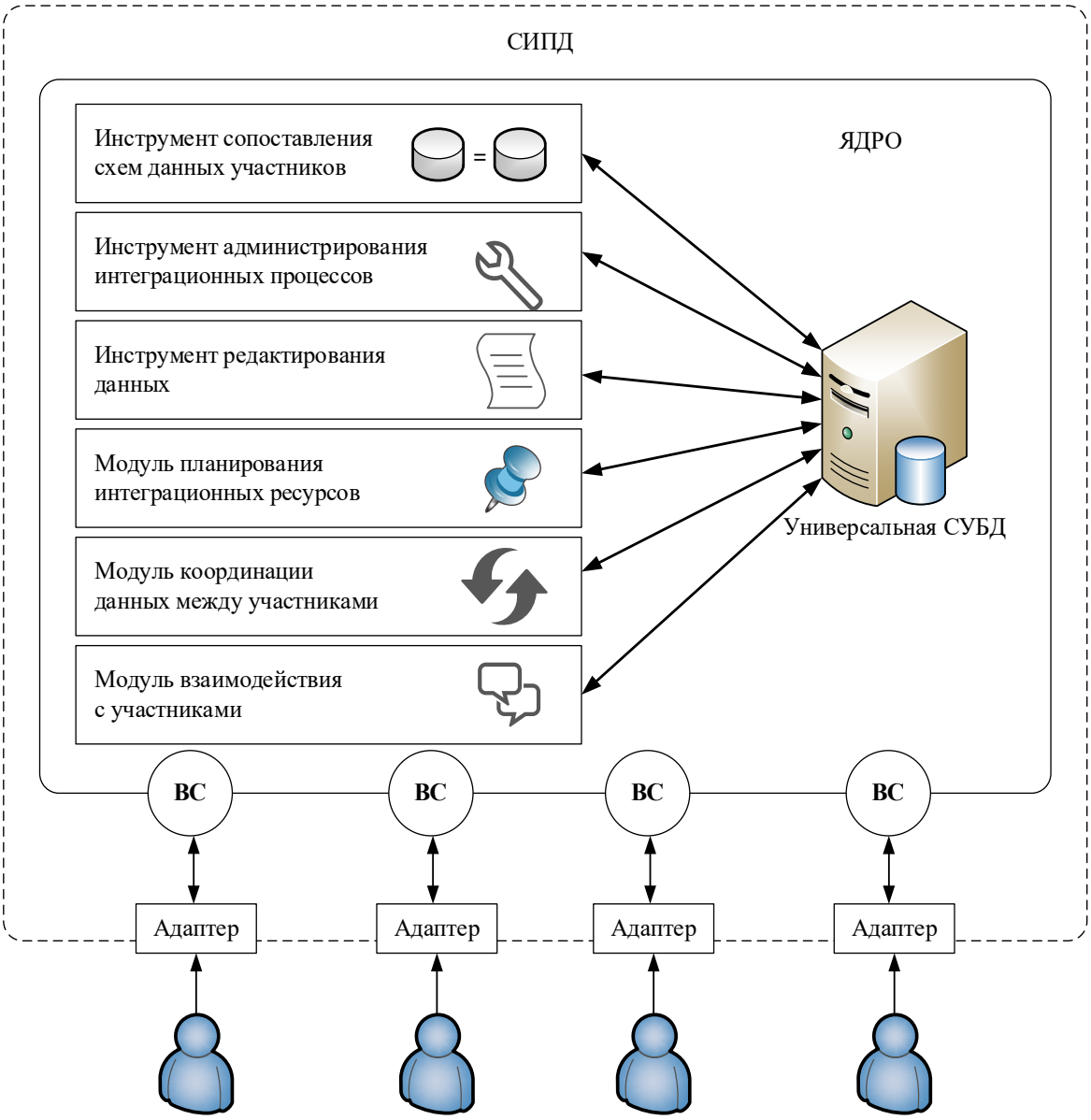


Рис. 4.7. Обобщенная структура СИПД

Для каждого участника интеграции необходим адаптер, предоставляющий СИПД интерфейс к данным этого участника. Адаптер может представлять собой как сервис, так и приложение с пользовательским интерфейсом. Передача информации от адаптера к СИПД осуществляется через веб-сервер (ВС).

Важной особенностью инструментальной системы, отличающей ее от существующих платформ интеграции, является объединение при создании ее архитектуры подхода к интеграции данных на основе интеграционной модели, базирующейся на том или ином отраслевом стандарте, с принципами сервисно-ориентированной архитектуры. Особенностью инструментальной системы, отличающей ее от существующих платформ интеграции, является объединение при создании ее архитектуры подхода к интеграции данных

на основе интеграционной модели, базирующейся на том или ином отраслевом стандарте, с принципами сервисно-ориентированной архитектуры.

Существует перспектива развития НМС в составе ИСОД МВД России. В случае продолжения развития в данном направлении и реализации возможностей СИПД, представляется возможным комплексная интеграция НМС в существующее информационное пространство.

4.4. Исследование возможности информационной безопасности доступа абонентов к базам данных с использованием «облачных технологий» и реализация модели противодействия от различным видам воздействий

Информационные технологии по праву считаются самой быстроразвивающейся сферой деятельности человечества. В связи с этим, информационная безопасность становится неотъемлемой частью деятельности любой организации, начиная с предприятий малого бизнеса и заканчивая крупными корпорациями и государственными учреждениями.

Многие уважаемые аудиторские, аналитические и технологические компании сделали постоянной практикой публикацию обзорных материалов, пытаясь в них проанализировать грядущие угрозы в информационной сфере и предсказать актуальные методы по противостоянию им.

Международная компания PricewaterhouseCoopers, специализирующаяся в области консалтинга и аудита, в своем глобальном исследовании тенденций информационной безопасности выделяет следующие основные тенденции, которые актуальны в том числе и для МВД России:

– наличие систем киберрезведки и обмена информацией о киберугрозах становится критичным для организаций;

– наблюдается рост геополитических угроз.

При этом аутсорсинг облачных технологий защиты информации, переход на открытое программное обеспечение, безопасность корпоративной цифровой архитектуры – ключевые технологические тренды кибербезопасности.

В исследовании отмечено повышение доверия к облачным технологиям: организации стали чаще использовать облачные сервисы для повседневных и важных процессов. Большинство организаций (63% респондентов) по всему миру и 46% респондентов в России) утверждают, что перевели свои ИТ-сервисы в облачную среду. Кроме того, приблизительно треть организаций во всем мире и в России доверяют поставщикам облачных технологий такие важные для бизнеса функции, как операционная деятельность и финансы.

Дэвид Берг, руководитель международной практики PricewaterhouseCooper по оказанию услуг в области кибербезопасности и защиты данных, подчеркнул: «В результате синтеза новейших технологий с об-

лачными архитектурами организации получат возможность более оперативно распознавать угрозы и реагировать на них, лучше понимать своих клиентов и экосистему бизнеса и в конечном итоге снижать свои затраты. В последние годы облачные технологии завоевывают популярность, и, по мере того как преимущества будут становиться все более очевидными, эта тенденция, скорее всего, будет сохраняться».

Одним из самых современных веяний является использование аналитики «больших данных» для обеспечения кибербезопасности. Стоит отметить, что в России эта тенденция получила даже большее распространение, чем во всем мире (56% против 51%). Да и в целом в нашей стране передовые сервисы обеспечения информационной безопасности используются чаще (73% против 62%).

Среди направлений инвестиций игроков рынка, указанных в исследовании, следует выделить инвестиции на цифровую архитектуру и биометрические системы и методы усиленной аутентификации.

Trend Micro Incorporated, японская компания-разработчик программного обеспечения для кибербезопасности, также опубликовала ежегодный отчет с прогнозами по информационной безопасности «Новый уровень – 8 прогнозов по кибербезопасности».

Лейтмотивом проведенного анализа можно назвать факт, что в наступающем году размах и глубина атак увеличится, при этом злоумышленники будут применять разнообразные тактики, чтобы получить максимальную выгоду в условиях изменения технологического ландшафта.

Из прогноза угроз, актуальных как для отдельных государственных учреждений Российской Федерации, так и для государства в целом, особое внимание вызывают следующие:

– разработчики не смогут своевременно обеспечить защиту устройств промышленного интернета вещей от DoS- и других видов атак;

– поскольку 46% мирового населения имеет доступ к интернету, усилится роль киберпропаганды с целью оказания влияния на общественное мнение;

– пример атаки на центральный банк Бангладеш в начале 2016 года доказывает, что атаки со взломом бизнес-процессов позволяют злоумышленникам получать значительную прибыль. В то же время методы мошенничества с использованием корпоративной почты по-прежнему останутся эффективным методом незаконного обогащения с использованием ничего не подозревающих сотрудников;

– новые методы целенаправленных атак будут направлены на то, чтобы уклониться от современных технологий обнаружения и совершать атаки на учреждения в самых разных областях.

Американская компания Fortinet, специализирующаяся на про-

граммно-аппаратных комплексах сетевой безопасности, представила свой список основных тенденций в кибербезопасности.

По их мнению, уязвимость безопасности облака заложена не в его архитектуре, а в огромном количестве устройств, имеющих удаленный доступ. Безопасность облака зависит от того, как ей управляют, каким пользователям разрешен доступ к сети и насколько этим пользователям доверяют. В наступающем году ожидаются нападения, ставящие под угрозу эту модель за счет использования конечных устройств. Атаковать будут пользователя, но под угрозой окажется и владелец ресурсов.

Облака часто используются для обеспечения повсеместного доступа к приложениям, ресурсам и услугам. Аналитики уверены, что используя все те же уязвимости в устройствах пользователей, хакеры будут заражать и облачные решения.

В конце августа 2020 года компания Microsoft опубликовала результаты исследования посвященного влиянию пандемии COVID-19 на рынок информационной безопасности. По данным Microsoft, облачные технологии могут облегчить оценку рисков кибербезопасности и создание планов действий на случай противодействия. Более половины облачных и гибридных компаний в опросе Microsoft сообщили, что разработали стратегию киберустойчивости для большинства сценариев риска, тогда как эта доля среди локальных организаций составила только 40%. В то же время 40% предприятий отдают приоритет инвестициям в облачную безопасность, чтобы снизить риск взлома. Следом идут безопасность данных и информации (28%) и средства защиты от фишинга (26%). По данным компании Microsoft, предприятиям и организациям необходима интегрированная система безопасности с применением облачных технологий [11].

В МВД России уже несколько лет проводится единая техническая политика по агрегации всех информационных ресурсов и систем в облачной инфраструктуре. Учитывая, что мнения специалистов по информационной безопасности сходятся в том, что облачные технологии были, есть и будут целью для злоумышленников, необходимо сконцентрировать внимание на обеспечении ее кибербезопасности.

Основным ядром функционирования облачных технологий являются центры обработки данных. Атаки против групп серверов могут привести к нарушению работоспособности сервисов и ресурсов, а также к краже конфиденциальной информации или информации, представляющей особую ценность. Для того чтобы снизить вероятность катастрофических последствий, организациям необходимо обеспечить надежную защиту как локальных сетей, так и сетей хранения данных (SAN).

SAN традиционно считались относительно безопасными, в первую очередь потому, что способ подключения SAN предусматривает весьма ограниченный доступ к ним со стороны других компонентов центра

данных – по существу, SAN представляет собой изолированную сеть. Такое представление является сильно упрощенным, так как один пораженный хост может потенциально заблокировать работу других хостов, подключенных к сети SAN, получить несанкционированный доступ к данным в пределах SAN и, наконец, обойти существующие межсетевые экраны и системы обнаружения вторжений в случае использования каналов IP поверх соединений Fibre Channel.

В связи с этим в настоящее время актуальным становится вопрос о том, что традиционная защита сетевого периметра центров обработки данных или информационных систем в целом, фокусирующаяся на трафике «север – юг» (межсетевые экраны, системы обнаружения и предотвращения, защищающие от атак извне), не способна оградить с высоким процентом эффективности от проникновения в систему в связи с тем, что наблюдается неумолимый рост циркуляции трафика между серверами, так называемый «восток – запад», не выходящий за его пределы.

Действенным решением проблемы разграничения трафика внутри центра обработки данных, а соответственно, и повышения уровня информационной безопасности, является микросегментация, то есть разделение на многочисленные защищенные зоны. Благодаря современным виртуализированным решениям практически каждая виртуальная машина может быть снабжена собственным межсетевым экраном, что позволяет создать сеть с нулевым уровнем доверия внутри ЦОДа. Вместе с тем более эффективным решением оказывается реализация средств безопасности на уровне гипервизора – речь идет о встроенном в этот гипервизор виртуальном коммутаторе.

Появление такого устройства стало ответом на потребность в обеспечении оперативного развертывания и динамической миграции виртуальных машин и приложений. Например, при развертывании нового приложения после запуска виртуальной машины нужно было вручную задать VLAN, сконфигурировать маршрутизацию в физической сети, настроить политики МСЭ. Все эти операции занимали время, и к тому же они оказывались уникальными для каждой аппаратной платформы, на которой построен ЦОД. Иначе говоря, приложения и виртуальные машины были привязаны к конкретной физической сети. Необходимо было устранить эту привязку, то есть виртуализировать сеть. У каждой платформы виртуализации есть свой коммутатор, который является для нее «родным».

Поверх виртуального коммутатора на программном уровне реализуются базовые сетевые функции: коммутация, маршрутизация, брандмауэр и балансировка нагрузки. Каждый физический сервер с гипервизором становится не просто вычислительной платформой, на которой можно выделить ресурсы виртуальным машинам, но еще и многогигабитным коммутатором и маршрутизатором (старый слоган «сеть – это

компьютер» получает новый смысл). Чтобы эти функции работали, нужна базовая IP-связность между серверами. На физической сети больше не нужно тратить время на настройку VLAN – достаточно один раз настроить транспортную сеть. Для передачи трафика через физическую сеть используется инкапсуляция VxLAN.

Использование виртуальных коммутаторов позволяет автоматизировать рутинные операции по настройке сети, ускорить аварийное восстановление и, конечно, повысить эффективность защиты. Когда функции безопасности и фильтрации трафика выполняются на уровне виртуальной платформы, на уровне гипервизора, приложения можно защитить независимо от нижележащей физической архитектуры.

4.5. Принципы и технические решения применения детерминированного хаоса для защиты информации в каналах связи и управления

В настоящее время хаотические процессы широко применяются для передачи сообщений в системах связи и управления. Динамический (детерминированный) хаос – это сложные непериодические колебания, порождаемые нелинейными динамическими системами с непрерывным спектром, характеризуемые высокой чувствительностью к начальным условиям. Причиной непредсказуемости является собственная динамика системы, а не влияние внешних помеховых факторов. Динамическому хаосу присущи как чисто динамические свойства, так и свойства случайных процессов: сплошной спектр мощности, экспоненциально спадающая корреляционная функция, непредсказуемость в течение длительного интервала времени.

Необходимо отметить следующие свойства динамического хаоса привлекательные для систем связи и управления [113]:

– разнообразие способов ввода информационного сигнала в хаотический;

– увеличение скорости модуляции по отношению к модуляции регулярных сигналов;

– возможность самосинхронизации передатчика и приемника;

– обеспечение конфиденциальности передачи сообщения;

– способность на базе одного устройства реализовать большое количество различных хаотических мод;

– возможность управления хаотическими режимами путем внесения малых изменений в параметры системы.

Применение динамического хаоса в системах связи возможно в таких направлениях, как: синхронизация приемника и передатчика, маскировка передаваемой информации, фильтрация шумов, восстановление сигналов, а также разработка систем кодирования и декодирования цифровых сообщений. Использование хаотических колебаний для скрытной передачи

информации является одним из перспективных направлений в современной технике связи. Однако проблема качественного выделения информационного сигнала из хаоса остается недостаточно изученной. Это обусловлено тем, что синхронизуемая динамическая приемная система должна генерировать хаотические колебания, которые должны быть идентичны передаваемым. Этот фактор делает такую систему трудно реализуемой. В этом случае система скрытной связи должна обеспечивать требуемую идентичность за счет синхронизации двух генераторов.

Необходимым условием функционирования системы является получение синхронного хаотического отклика, от качества которого зависит извлечение информационного сигнала из хаотического. Качество отклика определяется наличием и степенью влияния возмущающих факторов. Проблема заключается в том, что при передаче сигнал должен пройти процедуры модуляции, усиления, фильтрации. А они, в свою очередь, с учетом сложной структуры сигнала и нелинейных характеристик могут приводить к искажениям сигнала и десинхронизации отклика. Также к возмущающим факторами необходимо отнести внешние и внутренние помехи, способные ухудшить качество передачи.

В научной литературе схемы передачи информации на основе хаотического синхронного отклика принято делить на несколько групп: хаотическая маскировка (chaotic masking), переключение хаотических режимов (chaos shift keying), нелинейное подмешивание информационного сигнала к хаотическому (nonlinear signal mixing).

Рассмотрим структуру системы связи по передаче речевых сигналов в радиодиапазоне с использованием хаотических модулей, осуществляющих нелинейное подмешивание информации. В передатчике низкочастотный информационный сигнал с микрофона поступает на вход хаотического модуля. В хаотическом модуле передатчика производится нелинейное подмешивание информационного сигнала к хаотическому. Для схемы с нелинейным подмешиванием были проведены успешные эксперименты по передаче реальных речевых и музыкальных сигналов, как в низкочастотном, так и в радиодиапазонах [113].

Выходной сигнал модуля, представляющий собой смесь хаотического и информационного сигналов, осуществляет амплитудную модуляцию высокочастотных колебаний радиодиапазона. Этот сигнал усиливается и излучается.

В приемнике радиосигнал, принятый антенной, усиливается в полосе частот излучаемого передатчиком сигнала, демодулируется и проходит через низкочастотный фильтр. Хаотический модуль приемника осуществляет выделение информационного сигнала из его смеси с хаотическим сигналом.

Структура хаотической системы связи отличается от обычной наличием в передатчике и приемнике дополнительных элементов – хаотических модулей.

Динамический (детерминированный) хаос – это сложные непериодические колебания, порождаемые нелинейными динамическими системами с непрерывным спектром, характеризуемые высокой чувствительностью к начальным условиям. Динамическая система хаотична, если ее система обладает некоторыми свойствами, присущими случайным процессам, которые рассматриваются в теории вероятностей. Динамический хаос подобно случайному процессу требует статистического описания. При этом могут быть использованы вероятностные характеристики хаотических систем, такие как стационарное распределение вероятности, корреляционные функции, спектры мощности, показатели Ляпунова, энтропия и другие.

Существуют два подхода к описанию хаотических сигналов. В первом случае предполагается что процессы, происходящие в хаотической системе являются сложными, но детерминированными, реализуемыми с помощью определенного алгоритма. Поведение такой системы описывается системой дифференциальных или разностных уравнений с заданными начальными условиями, и определяется такими характеристиками, как показатель Ляпунова, фрактальные размерности аттрактора и т.д.

В другом подходе подлежащий описанию сигнал является случайным, алгоритмически непредсказуемым процессом. В ходе наблюдения за множеством итераций такого процесса выявляются определенные статистические закономерности во временной структуре сигнала, в вероятностях появления различных значений величин сигнала или их сочетаний. Это подход опирается на математический аппарат, включающий теорию вероятностей и математическую статистику.

Рассмотрим вероятностные характеристики хаотических процессов.

Корреляционная функция (КФ) характеризует статистическую зависимость двух процессов, отличающихся каким-либо параметром. В случае модуляции начальными условиями хаотической последовательности корреляционная функция имеет вид

$$R(\Delta x_0) = \frac{\sum_{n=0}^{N} (f_1^{(n)}(x_0) - m_1)(f_2^{(n)}(x_0 + \Delta x_0) - m_2)}{\sum_{n=0}^{N} (f_1^{(n)}(x_0) - m_1)^2}. \qquad (4.1)$$

Необходимо, чтобы среднее значение сигнала в системе передачи данных было равно нулю, иначе трудно найти ортогональный базис. Для дискретных систем автокорреляционная функция определяется следующим образом:

$$R(k) = \frac{1}{N} \sum_{n=1}^{N} (x_n - x_{cp})(x_{n+k} - x_{cp}), \qquad (4.2)$$

где $x_{ср}$ – среднее значение амплитуды колебаний, k – временной сдвиг при единичном временном периоде дискредитации [113]. На практике часто используется нормированная автокорреляционная функция (АКФ). Если с течением времени АКФ стремится к нулю, система не будет иметь устойчивых стационарных точек, то будет наблюдаться хаотический режим колебаний. Стремление к нулю АКФ может быть использовано в качестве критерия динамического хаоса.

Кроме АКФ о хаотичности движения можно судить по спектральной плотности (энергетическому спектру колебания). Спектральная плотность показывает распределение энергии сигнала по частотам и может быть вычислена при помощи преобразования Фурье.

Исследуя спектральную плотность, можно определить, каким является поведение системы – хаотическим, периодическим или квазипериодическим. Если система характеризуется периодической динамикой, то спектр такого движения будет дискретным и состоящим из узких линий. Линейчатость спектра указывает на явный детерминизм процесса. Если же динамика системы не является регулярной, то спектр будет сплошным или непрерывным. Сплошной спектр может быть признаком наличия детерминированных хаотических колебаний в системе.

В окрестности стационарной точки динамику системы можно изучить с помощью собственных значений матрицы линеаризации. Близко расположенные траектории экспоненциально разбегаются во времени в отличие от регулярных траекторий, которые разбегаются лишь линейно. Разбегание траекторий вследствие неограниченности энергии системы или диссипативных процессов в системе не может продолжаться бесконечно, что приводит к возникновению хаотических колебаний. Для анализа поведения в окрестности произвольной траектории движения используются показатели Ляпунова. Геометрически показатели Ляпунова характеризуют степень растяжения и сжатия вдоль устойчивых и неустойчивых направлений. Положительным значениям показателя Ляпунова соответствует локальная неустойчивость. Область значения управляющего параметра, которой соответствует положительное значение показателя Ляпунова, соответствует хаотическому режиму. Из этого можно сделать вывод, что показатели Ляпунова могут быть использованы для определения множества управляющих параметров, которые обеспечивают хаотическое поведение нелинейной динамической системы. Совокупность всех возможных показателей Ляпунова называется ляпуновским спектром.

Теория показателей Ляпунова получила обоснование после доказательства мультипликативной эргодической теоремы, которая устанавливает их существование для почти всякого $x \in M$. Показатели Ляпунова – это универсальные инвариантные характеристики, которые позволяют судить о некоторых свойствах динамической системы. Сумма всех ляпуновских

показателей равна среднему вдоль траектории значению дивергенции векторного поля, задающего динамику системы:

$$\lim_{t\to\infty}\frac{1}{t}\int_0^t div\dot{\xi}dt = \sum_{j=1}^{n}\lambda_j . \qquad (4.3)$$

В связи с тем, что показатели Ляпунова определяют степень неустойчивости, они оказываются связанными с энтропией динамической системы. Энтропия – это в известном смысле мера (не) упорядоченности системы. В теории информации энтропия H вводится для систем, которые могут находится в состоянии x_i с некоторыми вероятностями $p_i = p(x_i)$, с помощью формулы Шеннона [131]:

$$H = -\sum_i p_i \log p_i . \qquad (4.4)$$

Похожим образом можно дать определение метрической энтропии динамической системы, или энтропии Колмогорова–Синая. Энтропия Колмогорова показывает степень хаотичности динамической системы. Величина энтропии Колмогорова (КС-энтропия – по именам Колмогорова, Крылова, Синая) определяется как средняя скорость потери информации о системе. Энтропия служит мерой экспоненциального разбегания или сближения траекторий динамической системы. Этот факт был известен давно, но энтропийный подход дал возможность по-новому подойти к исследованию сложных систем.

По сравнению с показателями Ляпунова энтропия Колмогорова гораздо труднее вычисляется на практике. Она определяется по аналогии с энтропией в статистической механике (учитывает разбиение фазового пространства). Если известны показатели Ляпунова можно найти КС-энтропию по соотношению

$$K \le \int_P \sum_{\lambda_i>0} \lambda_i d\mu , \qquad (4.5)$$

которое представляет собой сумму всех положительных показателей Ляпунова, усредненную по некоторой области фазового пространства P с мерой $d\mu$ [132, 133].

Величина энтропии h не зависит от способа разбиения фазового пространства. Кроме того, если две динамические системы имеют равные энтропии, то их статистические законы движения одинаковы. На практике считают, что выполняется строгое равенство. Энтропия динамической системы K также определяет время предсказуемости для динамической системы.

При изучении хаотических систем в компьютерных или физических экспериментах возникает необходимость рассчитывать или измерять вероятностные характеристики. Одно из перспективных направлений применения динамического хаоса в системах связи и управления – это использование широкополосности хаотических режимов. Широкополосные сигналы

могут быть использованы для борьбы с искажениями и затуханием сигнала в каналах распространения. Перспективным направлением является использование хаотических сигналов сложной формы для шифрации передаваемых сообщений. Ведутся разработки новых методов передачи информации с более высокими скоростями и более надежным восстановлением полезной информации, снижением влияния шумов и других возмущающих факторов. Все вышеперечисленное подчеркивает перспективность применения детерминированного хаоса в системах связи и управления.

4.6. Принципы и технические решения применения оптимальной обработки сигналов на основе информационно-энтропийного критерия для защиты информации в каналах связи специального назначения

Анализ угроз информационной безопасности таких систем показывает, что при необходимости защиты конфиденциальных данных в каналах связи все более широко используются методы зашумления и маскирования полезных сигналов. В связи с этим задача совершенствования методов защиты информации в каналах связи путем их зашумления является актуальной.

Целью данного раздела монографии является обоснование структурной схемы канала связи с зашумлением, в котором происходит скрытая передача и прием полезного сигнала. Маскирование полезного сигнала производится мощным узкополосным фазомодулированным сигналом помехи.

Принципы построения канала связи с зашумлением.

Широко известны методы и техника скрытной передачи информации в канале связи, где для эффективного маскирования информационного сигнала в канале связи в передающем тракте полезный сигнал синхронно суммируется с мощным сигналом помехи. В приемном тракте сигнал отделяется от помехи на основе известного закона формирования шумового сигнала.

На основе известных методов способа разработана функциональная схема канала связи с зашумлением, представленная на рис. 4.8.

В передающей части полезный сигнал $S(t)$ линейно суммируется с маскирующим фазомодулированным маскирующим сигналом $n(t)$. После этого аддитивная смесь поступает на вход антенны и передается по линии связи, в общем случае по радиолинии. На приемной стороне используется оптимальный обнаружитель для извлечения полезного сигнала $S(t)$ из замаскированного $Y(t)$.

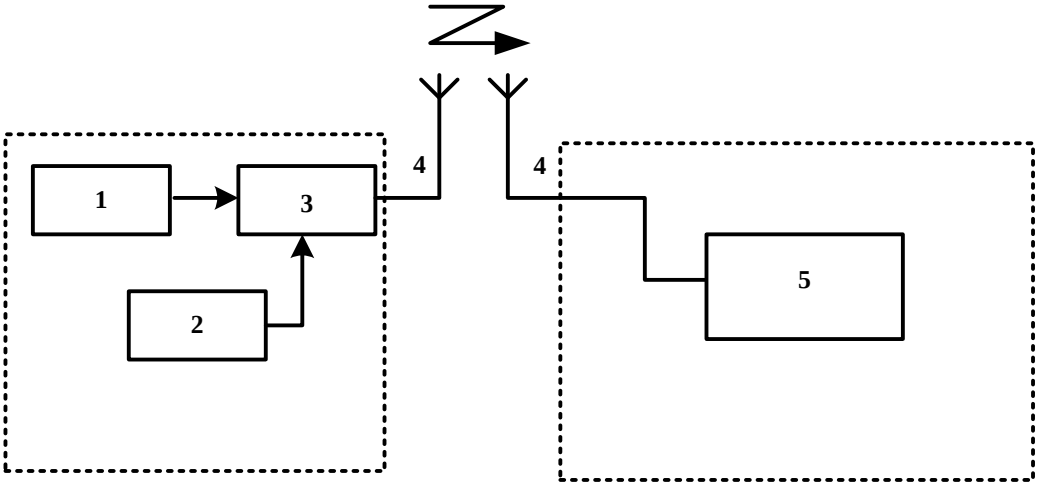


Рис. 4.8. Функциональная схема канала связи с зашумлением:
1 – генератор опорного сигнала; 2 – формирователь ФМ – помеховых сигналов; 3 – сумматор; 4 – каналы связи; 5 – оптимальный обнаружитель на базе корреляционной схемы обработки

Основным блоком передающей части канала связи с зашумлением является формирователь узкополосных фазомодулированных сигналов, отвечающий за генерирование маскирующей составляющей. Подробно он рассмотрен в работах [92, 93]. Известно, что узкополосные шумовые помехи с угловой модуляцией, несмотря на малую ширину излучаемого спектра частот, обеспечивают (в отличие от широкополосных помех) более высокие маскирующие свойства в части подавляемой полосы за счёт совпадения их характеристик с характеристиками модулирующего шума.

Формирователь узкополосных ФМ-сигналов с использованием квадратурного метода основан на нелинейном расширении спектра модулирующего напряжения и квадратурном сложении высокочастотных составляющих. Структурная схема КФМ квадратурного фазового модулятора на базе балансных модуляторов в квадратурных каналах приведена на рис. 4.9.

На рис. 4.9 приведены следующие обозначения: ГВЧ – генератор высокой частоты, ИМС – источник модулирующего сигнала, БМ1, БМ2 – балансные модуляторы (высокочастотные перемножители), ФВ $\pi/2$ – фазовращатель на $\pi/2$, С – линейный сумматор, ВКФ – вычислитель функции *cos(x)*, вычислитель функции *sin(x).* Алгоритмы работы схемы, амплитудные и фазовые модуляционные характеристики устройства приведены в монографии [4].

Сформированный таким образом маскирующий сигнал обладает ярко выраженными шумоподобными свойствами.

После того как узкополосный фазомодулированный сигнал помехи сформирован в КФМ, он в сумматоре складывается с полезным сигналом и

на выходе сумматора получаем аддитивную смесь полезного сигнала с узкополосной маскирующей помехой. Применение указанной схемы обеспечивает формирование маскирующего шума в передатчике (рис. 4.9).

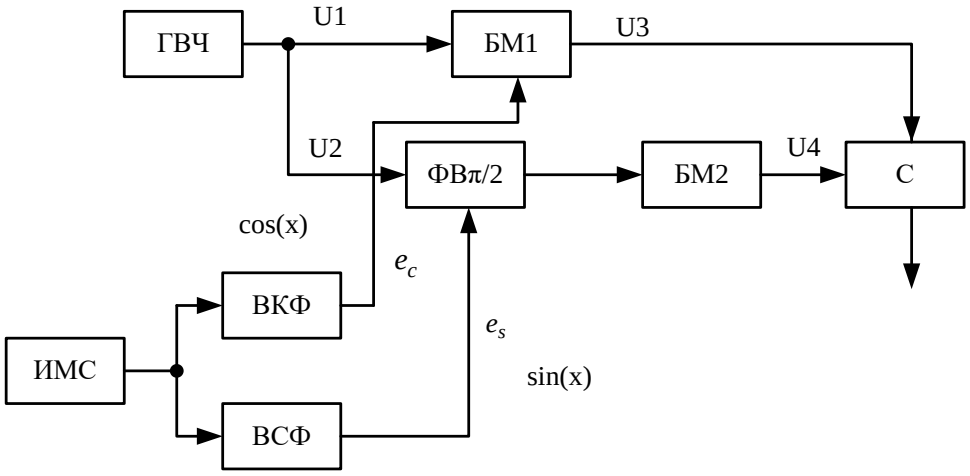


Рис. 4.9. Структурная схема КФМ на базе балансных модуляторов

Для эффективного извлечения полезного сигнала из смеси собственных шумов приемника и шумоподобного маскирующего сигнала широко применяется корреляционная схема обработки. Особенностью работы корреляционной схемы является то, что при корреляционном перемножении двух сигналов $y(t)$ и $x(t)$ на выходе корреляционного перемножителя происходит значительное возрастание амплитуды сигнала. Увеличение отношения сигнал/(шум+помеха) тем больше, чем более сильна корреляционная зависимость двух перемножаемых сигналов, один из которых является опорным.

Отношение правдоподобия является монотонной функцией корреляционного интеграла. Корреляционный интеграл сигнала с полностью известными параметрами определяется выражением

$$Z(t) = \int_{-\infty}^{\infty} x(t) \cdot y(t) dt , \qquad (4.6)$$

где $x(t)$ – ожидаемый полезный сигнал;

$y(t)$ – принимаемое колебание, представляющее собой аддитивную смесь маскирующего шума $n_m(t)$, полезного принимаемого сигнала $S(t)$ и собственных шумов приемника $n_c(t)$:

$$x(t) = n_m(t) + n_c(t) + A \cdot S(t) . \qquad (4.7)$$

Параметр A принимает значения 1 (полезный сигнал есть в шуме) и 0 (полезного сигнала нет).

Корреляционный способ выделения сигнала для канала связи с зашумлением является предпочтительным. Вместе с тем существуют и дру-

гие перспективные методы оптимальной обработки сигналов на фоне узкополосных и широкополосных шумов.

Сущность метода оптимальной вероятностной фильтрации сигналов.

Традиционный прием сигналов в канале с зашумлением с помощью супергетеродинного панорамного обнаружительного приемника на фоне внутренних шумов и внешних помех крайне неэффективен из-за низкого энергетического отношения сигнал/шум на выходе приемника. Это обусловлено широким спектром маскирующего сигнала и узкой полосой пропускания супергетеродинного приемника. В этой ситуации, как уже отмечалось, оптимизация процедур обнаружения и обработки сигналов фильтровым и корреляционным способами не обеспечивает требуемого качества обнаружения. Покажем, что альтернативным путем разрешения этого противоречия является применение вероятностного метода оптимальной фильтрации.

Основной функцией оптимального вероятностного фильтра, в отличие от энергетического, является не только увеличение отношения сигнал/шум на его выходе, но и получение количественной информации о различии законов распределений шумов приемника и сигнальной смеси сигнал + шум. На практике это достигается путем оценивания параметров формы плотностей распределения вероятностей (ПРВ) указанных оцениваемых случайных процессов. Из радиотехнических приложений теории вероятности известно, что наиболее информативными показателями, характеризующими форму ПРВ, являются такие числовые моментные характеристики закона распределения случайной величины, как энтропия ПРВ и производная от нее характеристика коэффициент качества шума. Энтропия ПРВ, как моментная (числовая) характеристика закона распределения, является интегральным показателем, количественно показывающим отличие формы закона распределения от стандартного нормального закона распределения. Аппаратурное измерение энтропии ПРВ и коэффициента качества шума с помощью современных цифровых технологий реализуется достаточно просто [5].

Теоретической предпосылкой, обеспечивающей возможность обнаружения регулярного сигнала на фоне маскирующего шума является тот факт, что при появлении полезного сигнала форма ПРВ сигнальной смеси шум + сигнал отличается от формы ПРВ шума. Измерение энтропии сигнальной смеси и шума позволяет решать задачу обнаружения полезных сигналов на фоне маскирующего шума следующим образом.

Так же, как и статистический энергетический оптимальный фильтр, вероятностный фильтр определяет отношение правдоподобия, сравнивает его с порогом и принимает решение о наличии сигнала среди шумов.

По сравнению с традиционным алгоритмом обнаружения в нашем подходе отличие заключается в новой физической сущности отношения

правдоподобия, которое определяется следующим соотношением:

$$I(x) = \frac{H_{СШ}(x)}{H_{Ш}(x)}, \tag{4.8}$$

где $I(x)$ – относительное количество информации, полученное в результате обработки смеси сигнала и шума (помехи); $H_{СШ}(x)$, $H_{Ш}(x)$ – соответственно энтропии ПРВ $\rho_{СШ}(x)$ и $\rho_{Ш}(x)$; x – оцениваемый параметр полезного сигнала (амплитуда, время запаздывания импульса и т.д.).

Аппаратурное измерение плотностей распределения параметров случайных сигналов и помех реализуется статистическим путем: определяется сглаженная гистограмма оцениваемого параметра случайного процесса при обработке статистически достаточного количества реализаций. На следующем этапе статистических измерений определяют энтропию ПРВ сигнальной смеси и шума на основе известных соотношений

$$H_{Ш}(x) = \int_{-\infty}^{\infty} \rho_{Ш}(x) \ln \rho_{Ш}(x) dx \ ,$$

$$H_{СШ}(x) = \int_{-\infty}^{\infty} \rho_{СШ}(x) \ln \rho_{СШ}(x) dx \, . \tag{4.9}$$

Таким образом, решение о наличии полезного сигнала в принимаемой и обрабатываемой смеси принимается путем сравнения измеренных энтропий (4) относительно заранее установленного порога (3). При этом результирующая энтропия сигнальной смеси является аддитивной смесью шумовой и сигнальной составляющих:

$$\begin{aligned} H(x) &= H_{Ш}(x) + AH_{C}(x) = \\ &= -\int_{-\infty}^{\infty} \rho_{Ш}(x) \cdot \ln \rho_{Ш}(x) + A \int_{-\infty}^{\infty} \rho_{C}(x) \ln \rho_{C}(x) dx \end{aligned} \tag{4.10}$$

Оптимальный вероятностный параметрический фильтр должен обеспечивать возможность наилучшего различения энтропий ПРВ вида (4.9). Параметр А принимает значения 0 или 1.

Рассмотренные выше теоретические предпосылки к обоснованию вероятностного метода оптимальной фильтрации позволяют синтезировать структурную схему фильтра, обеспечивающего максимизацию отношения (4.8) на его выходе. В частных случаях в вероятностном критерии (4.9) отношение энтропий можно заменить любым другим измеряемым параметром ПРВ, т. е. математическим моментом закона распределения, влияющим на его форму (эксцесс, асимметрия и т.д.).

Алгоритм оптимального обнаружения и структурная схема оптимального вероятностного фильтра.

Как следует из сущности метода оптимальной вероятностной фильтрации сигналов, важнейшими обнаружительными процедурами являются

измерение ПРВ шумов их смеси с сигналом, расчет энтропии указанных ПРВ и их различение с помощью пороговой процедуры. В соответствии с этим алгоритмом структурная схема оптимального вероятностного фильтра имеет вид, представленный на рис. 4.10.

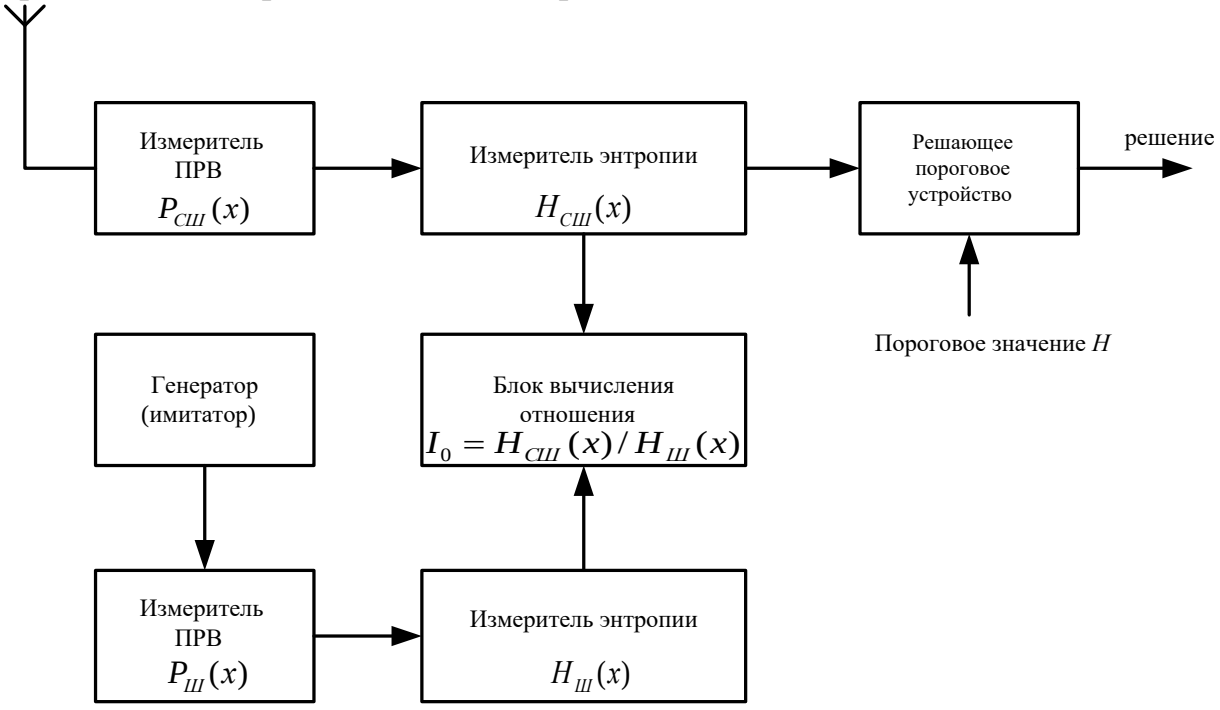


Рис. 4.10. Структурная схема оптимального вероятностного фильтра

Для принятия решения об обнаружении полезного сигнала на фоне шумов применяется пороговое устройство. Порог обнаружения задается исходя из требуемой вероятности обнаружения сигнала при фиксированном уровне ложных тревог. Предложенная схема реализует корреляционный принцип различения случайных процессов сигнал + шум и шум, соответственно, путем выявления отличий в их законах распределений. Корреляционный прием требует формирования опорного колебания (например, эталона маскирующего сигнала), что, как уже указывалось, усложняет аппаратурную реализацию приемника. Для упрощения аппаратуры приема в схеме, приведенной на рис. 4.10, использован блок имитатора шумов приемника. В качестве имитатора шумов на практике целесообразно использовать второй приемный тракт, по техническим характеристикам идентичный основному каналу. При этом основной канал подключен к антенне, а вспомогательный канал должен быть защищен от внешних воздействий.

Фильтр предложенной структуры будет оптимальным только в том случае, если он будет обеспечивать максимум отношения (4.8) на выходе решающего устройства. Максимизация различий законов распределений, как показано в работе [93], в ряде типовых ситуаций приема и обработки

сигнала достигается включением в приемный тракт элемента с нелинейной вольт-амперной характеристикой. При прохождении случайного сигнала с определенным законом распределения одного из его параметров через нелинейный элемент форма закона распределения существенно изменяется. Это свойство способствует повышению вероятности обнаружения полезного сигнала на фоне маскирующего шума с известной статистикой.

В данном разделе монографии изложено теоретическое обоснование нового метода формирования и обработки сигналов в каналах связи с зашумлением на основе применения вероятностной фильтрации. Этот метод лежит в основе новой технологии, позволяющей преодолеть ограничения существующих способов обнаружения сигналов и обеспечить эффективный прием сигналов на фоне искусственно организованных шумов. Указанный подход позволит с помощью относительно простой и, следовательно, дешевой приемо-передающей аппаратуры обеспечить защиту информации в перспективных средствах связи специального назначения.

4.7. Разработка методики оценки эффективности противодействия разрушению информации при воздействии сверхширокополосного сигнала по критерию сигнал/шум

Актуальной проблемой последнего времени является деструктивное электромагнитное воздействие, способное парализовать работу беспроводных систем связи или вовсе вывести из строя оборудование систем связи. С целью снижения или нейтрализации таких воздействий на системы радиосвязи был рассмотрен перечень возможных способов противодействия таким воздействиям. Следующим этапом является оценка эффективности противодействия разрушению информации по различным критериям, в данном разделе таким критерием выберем отношение сигнал/шум. Прежде чем перейти к рассмотрению данной оценки необходимо рассмотреть вопрос о применении способов противодействия. Решение о выборе способа мер противодействия осуществляется исходя из нескольких критериев, в частности:

1. Появление на приемной стороне помехового воздействия, мощность которого превышает мощность полезного сигнала более чем на 10 ДБм.

2. Способность системы связи функционировать.

3. Работоспособность оборудования, входящего в состав системы связи.

4. Наличие связи по обратному каналу.

5. Важность передаваемой информации.

Предположим, что мощность помехового воздействия превосходит мощность полезного сигнала на 10 ДБм, система связи не функционирует в нормальном режиме, оборудование находится в работоспособном состоя-

нии, связь по обратному каналу отсутствует, предаваемая информация классифицирована как срочная. На основании данных критериев, выбирается способ противодействия деструктивным электромагнитным воздействиям, заключающийся в использовании многосекторной антенной системы MIMO [97]. Информация передается через промежуточный пункт на антенную систему, не облученную помехой, или влияние помехи на данный сектор антенной системы, не мешает передаче, т.е. из передаваемого сигнала возможно декодировать информационное сообщение. Эффективность применения данного способа возможно оценить по критерию сигнал/шум (ОСШ). Данный критерий выражается отношением мощности полезного сигнала к мощности помехи и является безразмерной величиной (4.11), где

$$\text{ОСШ} = \frac{\text{Р}_{\text{сигнала}}}{\text{Р}_{\text{помехи}}}. \quad (4.11)$$

Применение данного способа можно считать эффективным, если SNR > 1, если SNR = 1 (частично эффективный способ противодействия), то система связи функционирует частично, т.е. могут быть большие ошибки в декодировании сообщений, которые могут привести к утрате полезной информации, если SNR < 1 (неэффективный способ противодействия), то помеха полностью блокирует поступление полезного сигнала на приемной стороне и, как следствие, передача сообщений между двумя приемопередающими станциями невозможна.

В данном разделе рассмотрен методический подход к оценке способа противодействия деструктивным электромагнитным воздействиям по критерию сигнал/шум. Было предложено использовать зависимость (4.11) в качестве оценки эффективности противодействия деструктивным электромагнитным воздействиям, в соответствии с которой способ противодействия считается эффективным, частично эффективным или неэффективным.

4.8. Разработка методики оценки эффективности противодействия разрушению информации при воздействии сверхширокополосного сигнала по информационному критерию

В последнее время большое распространение получило распространение электромагнитного оружия. Мощное электромагнитное излучение, оказываемое таким типом вооружения, способно вывести из строя или частично парализовать работу критически важных для охраны и обороны государства систем связи специального назначения. В связи с этим актуальной задачей становится разработка способов и алгоритмов противодействия. В работах [86, 97, 105, 106] был рассмотрен перечень возможных

способов противодействия таким воздействиям. Следующим этапом является оценка эффективности противодействия разрушению информации по различным критериям, в данном разделе таким критерием выберем информационный критерий, а именно коэффициент Bit Error Rate (BER) [107]. Коэффициент BER характеризует вероятность получения искажений передаваемого бита данных. Прежде чем перейти к рассмотрению данной оценки, необходимо рассмотреть вопрос о применении способов противодействия. Решение о выборе способа противодействия осуществляется исходя из нескольких критериев, в частности:

1. Мощности помехового воздействия.
2. Способности функционирования системы связи.
3. Наличия связи по обратному каналу.
4. Важности и срочности передаваемой информации.

Предположим, что мощность помехового воздействия превосходит мощность полезного сигнала на 10 ДБм, система связи не функционирует в нормальном режиме, связь по обратному каналу отсутствует, предаваемая информация классифицирована как срочная. На основании имеющихся данных выбирается способ противодействия деструктивным электромагнитным воздействиям, заключающийся в использовании многосекторной антенной системы MIMO [97]. Информация передается через промежуточный пункт на сектор антенной системы, не облученный помехой, или влияние помехи на данный сектор антенной системы не оказывает значительного влияния на передаваемые данные, т.е. из передаваемого сигнала возможно декодировать информационное сообщение. Эффективность применения данного способа возможно оценить с помощью коэффициента BER. В зависимости от передаваемых данных данный коэффициент может значительно отличаться, от BER = $10E^{-3}$ до BER = $10E^{-6}$. Для систем WIMAX стандарт IEEE 802.16 определяет максимально допустимый уровень битовой ошибки, равный BER = $10E^{-6}$ (процент приема ошибочных бит информации не более 0,005%). При данном уровне ошибок система WIMAX способна поддерживать с требуемым качеством самый критичный к ошибкам сервис цифровой телефонии (сервис TDM). Стандарт IEEE 802.16-2004 определяет для поддержки модуляции 64QAM ¾ на уровне ошибок не выше BER = $10E^{-6}$ с учетом коррекции ошибок FEC = 3/4.

Применение данного способа противодействия можно считать эффективным, если BER<$10E^{-6}$, если BER=$10E^{-6}$ (частично эффективный способ противодействия), то система связи функционирует частично, т.е. могут быть большие ошибки в декодировании сообщений, которые могут привести к утрате полезной информации, если BER>$10E^{-6}$ (неэффективный способ противодействия), то помеха полностью блокирует поступление полезного сигнала на приемной стороне и, как следствие, передача сообщений между двумя приемопередающими станциями невозможна.

Таким образом, в данном разделе был рассмотрен методический подход к оценке способа противодействия деструктивным электромагнитным воздействиям по информационному критерию. Было предложено использовать зависимость коэффициент BER в качестве оценки эффективности способа противодействия деструктивным электромагнитным воздействиям.

4.9. Способ противодействия деструктивным электромагнитным воздействиям, основанный на дополнительной модуляции с применением вейвлет-преобразования в сетях связи специального назначения

В настоящее время оборудование сетей связи специального назначения может быть реализовано на основе технологических решений, заложенных в стандартах IEEE 802.16 e и d WIMAX. Концепции построения сетей мобильного широкополосного доступа, разработанные в данном стандарте, нашли свое применение не только для организации связи и передачи данных, но и активно используются в системах управления БПЛА и робототехническими комплексами. Однако решения, применяемые в СССН на основе мобильного широкополосного доступа, не в полной мере, обеспечивают защищенность ведомственного мобильного широкополосного радиодоступа от воздействия электромагнитных излучений направленного характера. Средством нарушения защищенности могут являться устройства, генерирующие электромагнитные помехи в диапазонах частот, используемых СССН. Такое воздействие осуществляется с помощью широкополосных генераторов, рассчитанных на определенный частотный диапазон, путем постановки широкополосной шумовой заградительной помехи [97]. Генерируемая помеха может оказать на информационный сигнал СССН деструктивное влияние, в результате чего утрачивается возможность обмена информацией между удаленными объектами, аппаратура связи может быть выведена из стоя.

С учетом этого актуальной задачей становится совершенствование комплекса мер противодействия деструктивным электромагнитным воздействиям, оказывающим влияние на СССН. В качестве объекта исследования выберем систему широкополосного доступа стандарта WiMAX, в качестве помехового широкополосного воздействия – гауссовский биполярный импульс, рассмотренный в работе [84].

В качестве способа противодействия деструктивным электромагнитным воздействиям авторами предлагается осуществление переноса спектра сигнала WiMAX в другой частотный диапазон и его расширение при помощи дополнительной модуляции информационного сигнала МНАТ-вейвлетом. Описание стандарта WIMAX и способа противодействия, осно-

ванного на переносе спектра при помощи вейвлет-преобразования, будет рассмотрено далее.

Описание стандарта WIMAX.

ССCH на основе стандарта IEEE 802.16 WiMAX функционируют в частотных диапазонах в пределах от 2 до 11 ГГц. Одной из главных особенностей стандарта является то, что помимо традиционной антенной системы «один вход–один выход» (SISO) может быть применена технология многосекторной антенной системы (MIMO). Ширина канала составляет от 1,25 до 28 МГц [84, 97, 105]. Стандартом IEEE 802.16 предусмотрено применение различных видов модуляции, таких как BPSK и многоуровневая QAM. Кроме того, стоит отметить поддержку данным стандартом технологии ортогонального частотного мультиплексирования (OFDM), при помощи которой осуществляется расширение спектра радиосигналов. Постоим спектр сигнала OFDM (4.12) для визуального отображения сигнала системы WiMAX (рис. 4.11). Реализация построения сигнала WiMAX осуществлялась с помощью языка программирования Python, поскольку он имеет большой спектр возможностей, необходимых современному исследователю в различных областях научной деятельности, и позволяет достаточно просто осуществить визуализацию графиков функций, благодаря встроенным модулям.

$$G(\omega) = \sum_{n=-N/2}^{\frac{N}{2-1}} A_n^2 T^2 \frac{sin^2(\frac{\omega T - 2\pi n}{2})}{(\frac{\omega T - 2\pi n}{2})^2}, \tag{4.12}$$

где An – амплитуда n-й поднесущей, T – длительность огибающей, N – количество поднесущих.

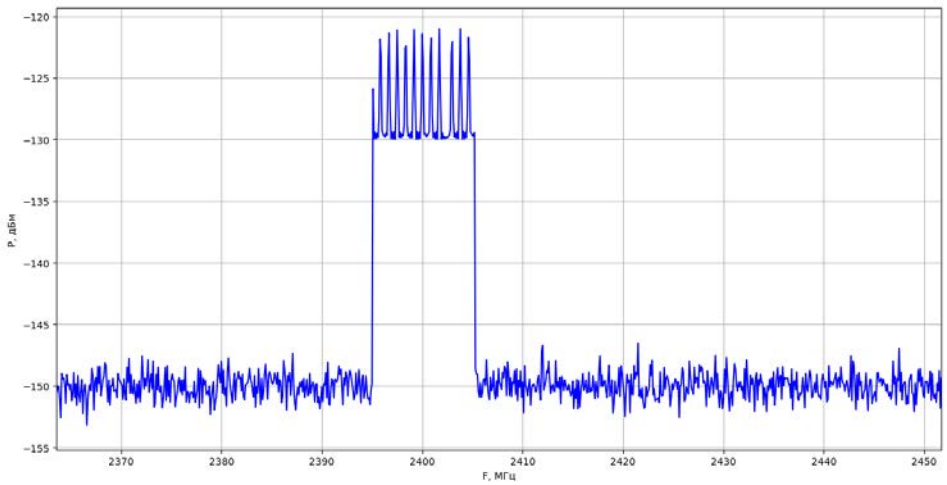


Рис. 4.11. Спектр WiMAx-сигнала

Для построения были использованы следующие параметры:

1. Количество поднесущих $N = 64$.

2. Амплитуда сигнала -150 дБм.

3. Центральная частота 2500 МГц.

4. Ширина спектра 10 МГц.

5. Шум накладывался с помощью встроенной функции «rand» в диапазоне от 0 до 1.

Далее будет рассмотрен способ противодействия деструктивным электромагнитным воздействиям, основанный на переносе спектра сигнала при помощи дополнительной модуляции сигнала OFDM вейвлет–функцией. В следующем разделе будет приведено описание MHAT-вейвлета, используемого в качестве дополнительной модулирующей функции.

Описание вейвлет-функции и способа противодействия на ее основе.

Вейвлет-преобразование представляет собой математическое преобразование, способное анализировать и модифицировать различные частотные компоненты сигналов. Вейвлет-преобразование проецирует одномерный сигнал на полуплоскость время – частота, что позволяет разделять разномасштабные события и исследовать зависимость спектральных характеристик от времени, одинаково хорошо выявляет как низкочастотные, так и высокочастотные характеристики сигнала на разных временных отрезках.

Вейвлет-анализ является одним из наиболее мощных и при этом гибких средств исследования и обработки радиотехнических сигналов: их фильтрации и сжатия. Так же технология вейвлет-преобразования активно используется для достижения определенных результатов, в частности для улучшения системы OFDM в соответствии с характеристиками канала с замиранием при многолучевом распространении. Кроме того, для того чтобы повысить как SNR, BER, улучшить спектральную эффективность, в то же время уменьшить передаваемую мощность и для управления сдвигом частоты и фазовым шумом.

Во временном виде вейвлет-преобразование представляет собой функцию

$$\psi(t) = \frac{1}{\sqrt{a}} \cdot \varphi(\frac{t-b}{a}), \tag{4.13}$$

где a – масштабирующий множитель; b – временной сдвиг.

Спектральную плотность вейвлет-преобразования можно выразить в следующем виде:

$$\psi(\omega) = \frac{2\pi}{\sqrt{a}} \cdot \omega^2 \cdot e^{-\omega^2/2}, \tag{4.14}$$

где a – масштабирующий множитель.

На основании анализа литературы [6, 8, 9, 13] авторами предлагается новый способ использования вейвлет–преобразования – в качестве меры противодействия деструктивным электромагнитным воздействиям, а именно для переноса спектра полезного сигнала в другой частотный диа-

пазон и его расширения. В качестве модулирующей функции был выбран МНАТ-вейвлет, поскольку он описывается в частотно-временной полуплоскости и его параметры зависят от определенных коэффициентов (масштабирующего множителя и временного сдвига) формула 4.14. Таким образом, можно менять параметры модулированного сигнала путем изменения коэффициентов вейлвлет-функции, которой он модулируется. МНАТ-вейвлет получается в результате двукратного дифференцирования функции Гаусса.

Учитывая то, что вейвлет–преобразование проецируется в полуплоскости частота-время, процесс модуляции сигнала можно представить в следующем виде:

$$G_m(\omega) = A \cdot \frac{1}{\sqrt{a}} \cdot e^{-0{,}5\cdot\left(\frac{t-b}{a}\right)^2} \cdot \left(\left(\frac{t-b}{a}\right)^2 - 1\right) \cdot \sum_{n=-N/2}^{\frac{N}{2-1}} A_n^2 T^2 \frac{sin^2\left(\frac{\omega T - 2\pi n}{2}\right)}{\left(\frac{\omega T - 2\pi n}{2}\right)^2}. \quad (4.15)$$

Далее будет рассмотрено моделирование помехового воздействия на полезный сигнал стандарта WiMAX.

Определение параметров помехового воздействия.

В качестве модели деструктивного электромагнитного воздействия будет рассматриваться гауссовский биполярный импульс.

Такой импульс можно представить путем перемножения гауссова импульса на линейную функцию времени:

$$\mathrm{S(t)} = 2\sqrt{\mathrm{e}} \cdot A t f_0 \cdot e^{-2(\pi f_0 t)^2}. \quad (4.16)$$

Спектральная плотность гауссовского биполярного импульса:

$$\mathrm{S}(j\omega) = \frac{\sqrt{2\mathrm{e}}A}{2\sqrt{\pi}{f_0}^2} \cdot e^{-0{,}5\left(\frac{f^2}{f_0}\right)^2}. \quad (4.17)$$

Для построения гауссовского биполярного импульса, являющегося моделью широкополосной помехи, был применен программный комплекс [7]. Временная и частотная зависимость представлены на рис. 4.12.

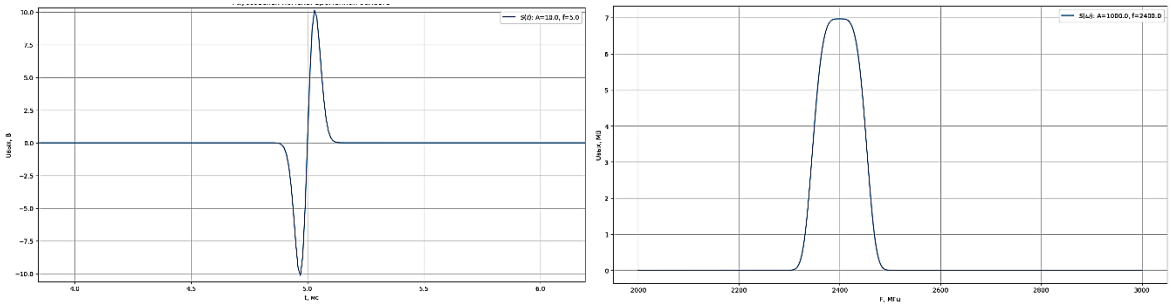


Рис. 4.12. Гауссовский биполярный импульс во временной и частотной областях

Данный импульс имеет длительность 0,25 мс, мощность около 7 МВт, ширина импульса около 180 МГц. Расположен в частотном диапазоне функционирования оборудования WiMAX, в нашем случае на частоте 2400 МГц. В следующем разделе будет рассмотрено функционирование СССН стандарта WiMAX в условиях деструктивных электромагнитных воздействий.

Функционирование СССН, реализованной на оборудовании стандарта WIMAX, в условиях деструктивного воздействия.

Предположим, что на информационный сигнал оказывает воздействие широкополосная деструктивная помеха. Структурная схема функционирования СССН в условиях деструктивного воздействия приведена на рис. 4.13.

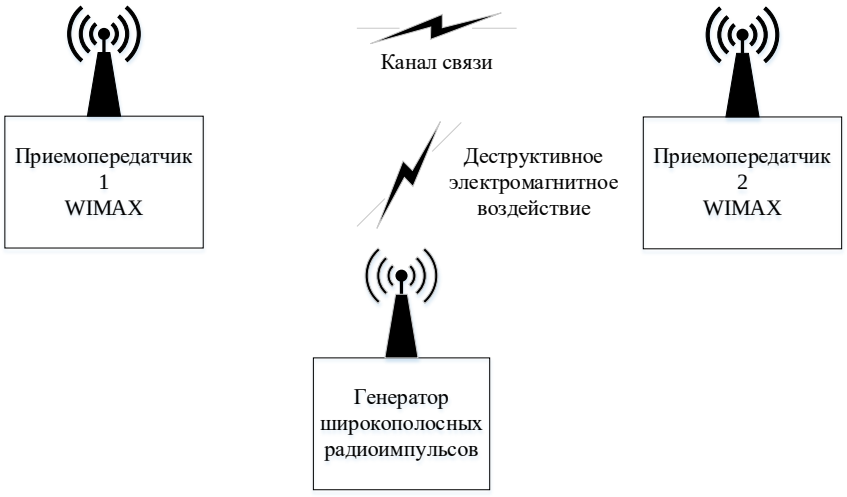


Рис. 4.13. Структурная схема функционирования СССН в условиях деструктивного электромагнитного воздействия.

На сигнал, передающийся от приемо-передающего устройства 1 на приемо-передающее устройство 2 СССН, оказывает влияние деструктивная помеха в виде гауссовского биполярного импульса, в результате чего на вход приемо-передатчика 2 СССН поступает аддитивная смесь полезного сигнала и действующей помехи. Спектр аддитивной смеси полезного сигнала системы WiMax и помехи приведен на рис. 4.14.

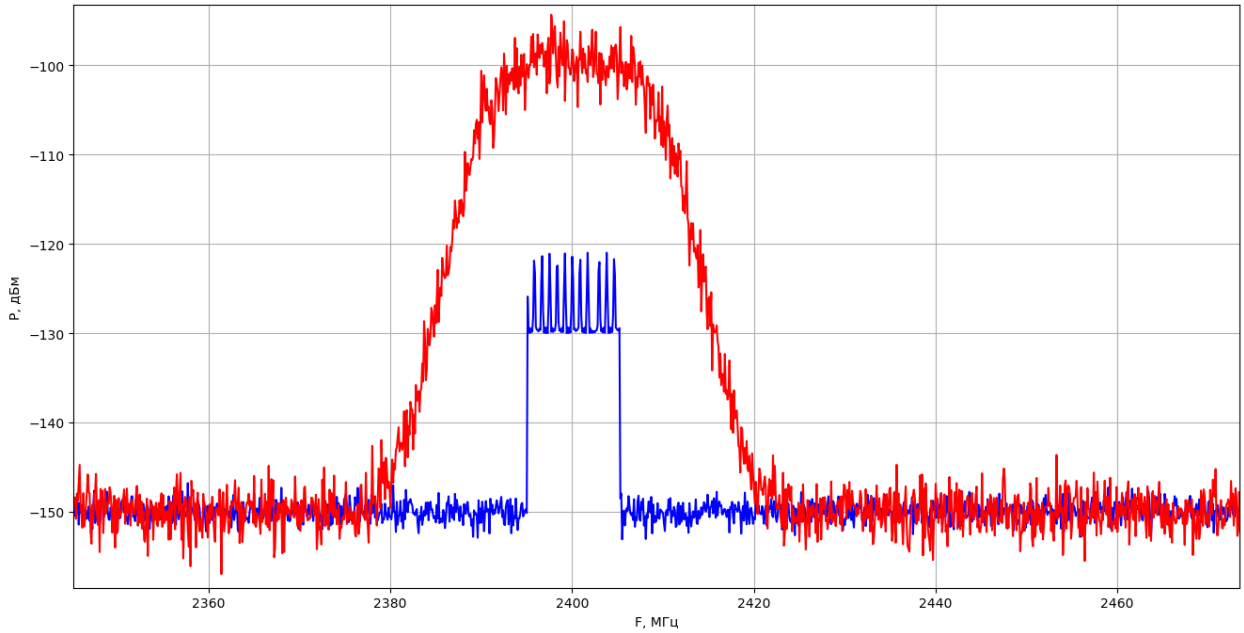


Рис. 4.14. Спектр аддитивной смеси полезного сигнала системы WiMax и помехи

Ширина помехи составляет 40 МГц, мощность –100 Дбм, что превосходит параметры полезного сигнала (ширина спектра 10 МГц, мощность –130 Дбм). Поскольку уровень воздействующей помехи превышает уровень полезного сигнала более чем на 10 дБм, детектировать сигнал не представляется возможным. Поскольку осуществить передачу информации от приемопередающей станции 1 на приемопередающую станцию 2 не представляется возможным в связи с воздействием помехи, авторами предлагается способ противодействия деструктивному электромагнитному воздействию, который будет рассмотрен далее.

Способ противодействия деструктивным электромагнитным воздействиям.

В качестве способа противодействия деструктивному воздействию предложим применение дополнительной модуляции WiMAX-сигнала МНАТ-вейвлетом. Данный способ предполагается применять в случаях, если между двумя приемопередающими станциями СССН отсутствует связь по обратному каналу (основываясь на текущем состоянии канала (отношение сигнал/шум)). Например, между приемопередатчиком 2 и приемопередатчиком 1 отсутствует соединение по обратному каналу, предполагается, что причиной этому является действие помехи на вход приемопередатчика 2. В качестве способа противодействия предполагается использование дополнительной модуляции МНАТ-вейвлетом. На приемопередающей станции 1 выходной CDMA сигнал системы WIMAX перемножается на вейвлет функцию формула 4.15. Изменяя значения коэффициентов a и b, формулы 4.15 можно осуществить расширение спектра сигнала и его перенос в другой диапазон частот. Зададим такие значения коэффици-

ентов, чтобы перенести спектр сигнала на частоту 5,5 МГц с увеличением ширины спектра на 10 МГц. Проведенные расчеты показывают, что такому результату соответствуют следующие значения масштабирующего множителя и временного сдвига: $a = 8$, $b = 3100$. Необходимо подчеркнуть, что все преобразования сигнала осуществляются в приемопередатчике еще до воздействия помеховой компоненты. В результате этого система связи после перехода в другой частотный диапазон осуществляет указанный способ противодействия. Количество возможных вариантов расширения спектра зависит от доступных для СССН диапазонов частот.

В результате подстановки в выражение (4.15) коэффициентов с такими значениями будет получен спектр WiMax-сигнала, представленный на рис. 4.15.

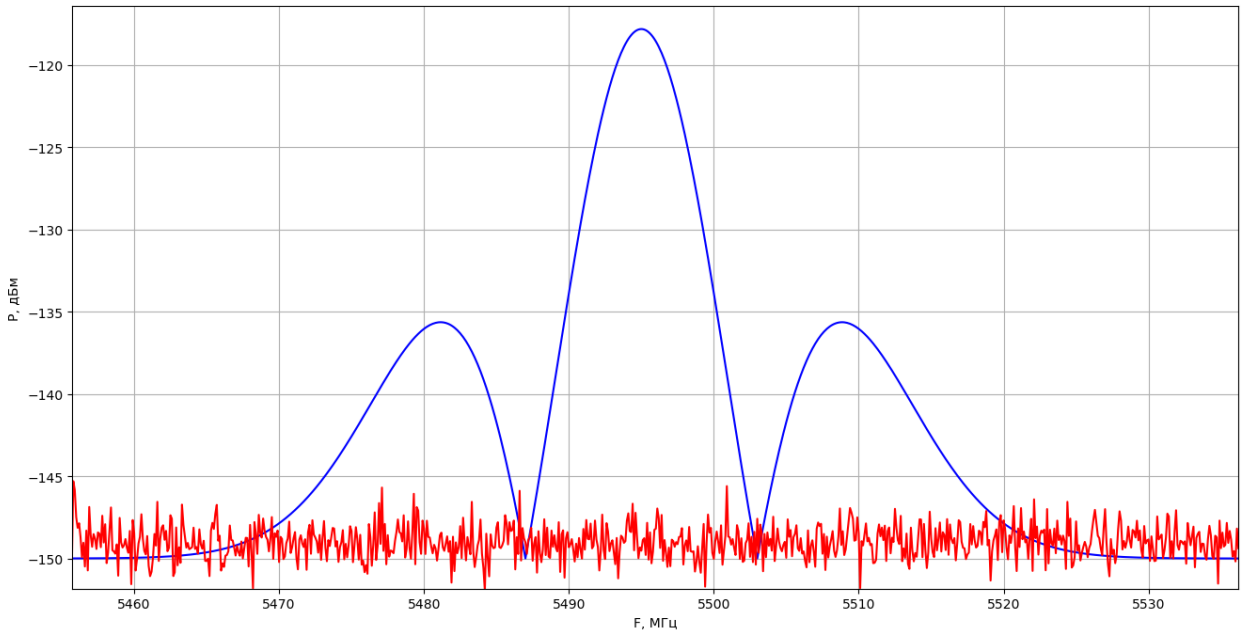


Рис. 4.15. Спектр WiMax-сигнала, модулированного вейвлет-функцией

Из спектра видно, что сигнал благодаря дополнительной модуляции МНАТ-вейвлетом расширился (ширина 16 МГц), увеличился по мощности (–115 ДБм) и передвинулся в другой частотный диапазон, где также функционирует оборудование стандарта WiMax (5,5 ГГц), что исключает воздействие помехи. Данное преобразование может быть реализовано в виде программного решения или отдельного устройства, функционирующего в составе приемо-передающего оборудования СССН стандарта WiMAX.

Был предложен способ противодействия деструктивным электромагнитным воздействиям, заключающийся в переносе и расширении спектра, реализуемый с применением вейвлет–преобразований в СССН стандарта WiMAX. Авторами было выявлено, что системы связи стандарта WiMax, используемые в качестве СССН, являются уязвимыми к деструктивным электромагнитным воздействиям. В качестве объекта рассмотрения вы-

брана система широкополосного доступа WiMax, а в качестве модели помехового воздействия – биполярный экспоненциальный импульс. Были построены спектры полезного сигнала WiMax, а также воздействующего на него помехового воздействия. При поступлении на приемопередающее устройство 2 сигнала и действующей на него помехи, декодировать переданное сообщение не представляется возможным поскольку уровень помехи значительно превосходит уровень полезного сигнала, а также утрачивается связь с приёмопередающей станцией 1 по обратному каналу. В качестве способа противодействия деструктивным электромагнитным воздействиям авторами было предложено использование дополнительной модуляции, осуществляемой МНАТ-вейвлетом. В результате перемножения полезного сигнала WiMax и вейвлет-функции спектр полезного сигнала переносится в другую полосу частот, в которой также имеется возможность функционирования систем WiMax, усиливается по мощности и расширяется по ширине. Предложенный в данном разделе способ противодействия деструктивным электромагнитным воздействиям в СССН с применением вейвлет- преобразования может быть реализован на практике в виде программного или технического решения, входящего в состав аппаратуры СССН.

Выводы

В главе 4 предложена математическая модель комплекса средств противодействия угрозам информационной безопасности в СССН, основанная на применении лингвистических переменных и нечетких экспертных систем формирования комплекса средств противодействия угрозам информационной безопасности в сетях связи специального назначения, осуществлено исследование общих технологических особенностей формирования комплекса средств противодействия угрозам информационной безопасности в СССН. Авторами проведено моделирование функционирования комплекса средств противодействия на основе аппарата лингвистических переменных и нечетких экспертных систем. На основе полученных результатов могут быть предложены требования к формированию комплекса средств противодействия угрозам информационной безопасности в СССН. Математический аппарат, использованный в данном разделе, основан на применении лингвистических переменных и нечетких экспертных систем, может в полной мере характеризовать зависимость эффективности средств противодействия от совокупности реализуемых средств защиты. В рамках комплексного подхода возможно построение такого рода систем с применением элементов искусственного интеллекта, что будет рассмотрено авторским коллективом в дальнейших исследованиях.

Методы противодействия угрозам нарушения информационной безопасности в цифровых сетях связи специального назначения можно разделить на три группы: предотвращения, парирования и нейтрализации угроз.

Предложены принципы и технические решения применения оптимальной обработки сигналов на основе информационно-энтропийного критерия для защиты информации в каналах связи специального назначения. В данном разделе монографии изложено теоретическое обоснование нового метода формирования и обработки сигналов в каналах связи с зашумлением на основе применения вероятностной фильтрации. Данный метод лежит в основе новой технологии, позволяющей преодолеть ограничения существующих способов обнаружения сигналов и обеспечить эффективный прием сигналов на фоне искусственно организованных шумов. Указанный подход позволит с помощью относительно простой и, следовательно, дешевой приемо-передающей аппаратуры обеспечить защиту информации в перспективных средствах связи специального назначения.

В качестве способа противодействия деструктивным электромагнитным воздействиям было предложено использование дополнительной модуляции, осуществляемой MHAT-вейвлетом. В результате перемножения полезного сигнала WiMax и вейвлет-функции, спектр полезного сигнала переносится в другую полосу частот, в которой также имеется возможность функционирования систем WiMax, усиливается по мощности и расширяется по ширине. Предложенный способ противодействия деструктивным электромагнитным воздействиям в СССН с применением вейвлет-преобразования может быть реализован на практике в виде программного или технического решения, входящего в состав аппаратуры СССН.

Глава 5.
МЕТОДИКА АНАЛИЗА И РЕГУЛИРОВАНИЯ РИСКОВ ПРИ РЕАЛИЗАЦИИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕТЯХ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

5.1. Анализ рисков нарушения информационной безопасности и уязвимости процессов переработки информации в сетях связи специального назначения

Системный подход к управлению рисками информационной безопасности как к непрерывному процессу помогает идентифицировать потребности МВД России в обеспечении информационной безопасности и создать эффективную систему управления информационной безопасностью. В ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения информационной безопасности. Менеджмент риска информационной безопасности» указывается, что риск-ориентированный подход содействует адекватному обеспечению информационной безопасности. Деятельность по обеспечению информационной безопасности обеспечивает своевременное и эффективное реагирование на риски информационной безопасности там и тогда, где и когда это наиболее необходимо. В Концепции обеспечения информационной безопасности ОВД Российской Федерации до 2020 года среди основных направлений обеспечения ИБ ОВД выделяют «проведение оценки уязвимости и рисков информации при имеющемся множестве угроз и каналов утечки» (приказ МВД России от 14 марта 2012 г. №169).

Анализ рисков информационной безопасности увеличил число сложных вопросов информационной безопасности, требующих участия специалистов в различных областях знаний. Это приводит к неспособности таких систем тщательно оценивать состояние безопасности информационных, телекоммуникационных систем ОВД. Интеллектуальный анализ рисков и уязвимостей становится наиболее важным аспектом при проектировании и эксплуатации системы управления рисками информационной безопасности [107, 108]. Необходимо минимизировать время, затрачиваемое на формирование критериев оценки рисков и процесс анализа рисков, обнаружения уязвимостей информационных, телекоммуникационных систем ОВД. Для этой задачи могут быть использованы математические инструменты искусственной нейронной сети и вероятностного дерева атак, построенного с применением теории графов.

Федеральный закон №184-ФЗ «О техническом регулировании» дает такое определение понятию риск – это вероятность причинения вреда с учетом его тяжести. Процесс взаимодействия элементов системы управления рисками ИБ представлен на рис. 5.1.

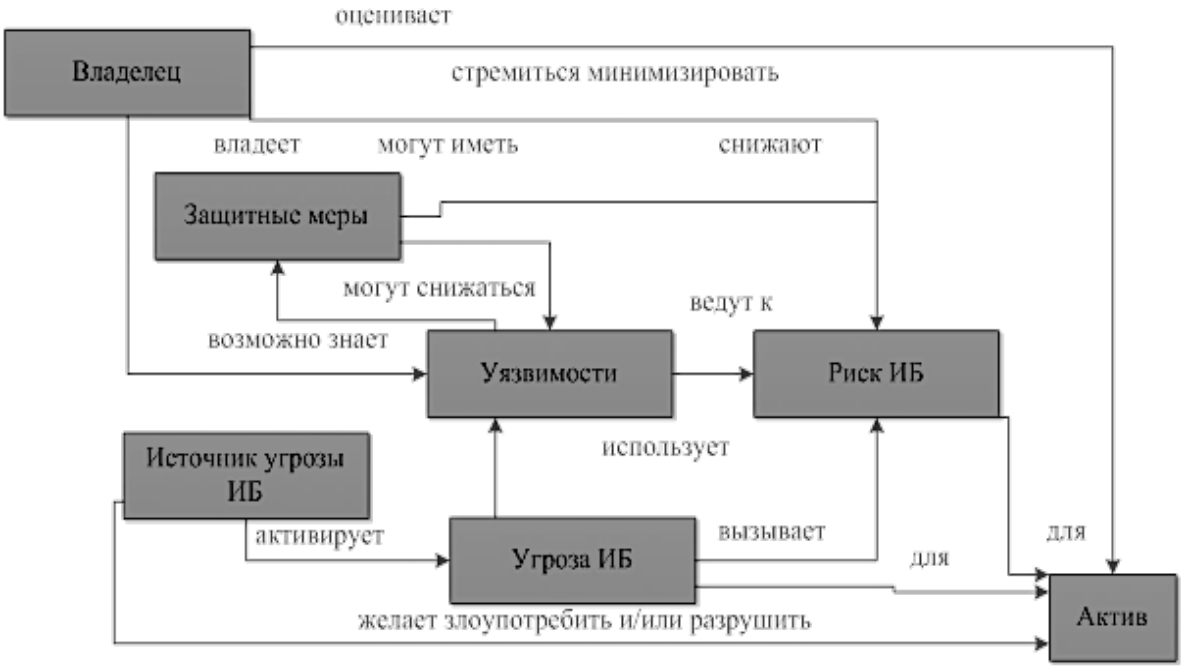


Рис. 5.1. Процесс взаимодействия элементов системы управления рисками ИБ

Риск нарушения информационной безопасности – потенциальная возможность использования уязвимостей активов МВД России угрозами информационной безопасности для причинения ущерба МВД России, измеряемая с учетом вероятности реализации угроз информационной безопасности и величины ущерба от реализации угроз.

В соответствии с ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «Информационные технологии. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий» расчет риска происходит по формуле $R = P(t) \times P(v) \times S$, где $P(t)$ – вероятность реализации угрозы информационной безопасности; $P(v)$ – вероятность наличия уязвимости; S – ценность актива. Под обработкой риска понимается процесс минимизации последствий от реализации риска и/или процесс минимизации вероятности реализации риска ИБ. Пример деятельности по обработке рисков ИБ представлен в соответствии с ГОСТ Р ИСО/МЭК 27005-2010. Предложения по оптимизации функционирования в условиях рисков угроз нарушения информационной безопасности в информационных, телекоммуникационных системах ОВД основываются на модели нарушителя и банке данных угроз безопасности информации ФСТЭК России.

Организация и проведение оценки рисков нарушения информационной безопасности в информационных, телекоммуникационных системах ОВД позволяет получать обоснованные оценки рисков, уязвимостей, эффективности защиты. Для оценки эффективности разработанной системы была проведена оценка безопасности для информационных, телекоммуни-

кационных систем ОВД. В результате было подтверждено соответствие между реальной безопасностью информационной системы и назначенными оценками.

5.2. Методический подход к оценке рисков нарушения информационной безопасности в самоорганизующихся мобильных сетях на основе аппарата нечеткой логики

В современных условиях значительно возрастает роль мобильных систем связи специального назначения, предназначенных для управления силами и средствами, обеспечивающими выполнение задач в различных условиях оперативной обстановки. Такие системы связи должны быстро реагировать на изменения оперативно-служебной обстановки, при необходимости изменяя свою структуру, надежно функционировать в отрыве от базовой инфраструктуры связи, обеспечивая главную задачу, а именно обеспечение информационного обмена в системе [107].

Современные мобильные системы связи зачастую строятся по принципу самоорганизующихся сетей, что предполагает динамическую архитектуру построения радиосетей, в которой могут отсутствовать как базовые станции, так и фиксированные маршруты передачи информации. Такие сети относятся к MANET–сетям (MANET – Mobile Ad-Hoc Networks) [164, 165]. Применительно, например, к мобильным сетям связи органов внутренних дел России такие сети могут быть реализованы на аппаратуре цифровой радиосвязи «Гранит Р-86АЦ» «Волновая сеть».

Комплекс цифровой радиосвязи «Волновая сеть» является современным решением в сфере цифровой радиосвязи. Данная система разработана как альтернатива зарубежным системам, таким как APCO 25, DMR и другие.

Цифровой комплекс «Волновая сеть» обеспечивает:

– обмен речевой информацией между абонентами;

– обмен данными между устройствами, подключаемыми к радиостанции;

– ретрансляцию сигналов;

– передачу телеметрии;

– защиту передаваемой информации от несанкционированного доступа;

– индивидуальный, групповой, циркулярный вызов;

– функционирование по командам дистанционного управления;

– контроль перемещения мобильных абонентов в реальном времени;

– обработку данных с различных датчиков с записью в базу данных.

В основу принципа работы данного комплекса ложится временное разделение канала. Особенностью функционирования комплекса выступа-

ет протокол маршрутизации, являющийся коммерческой тайной ООО «Радиотехника». Он обладает рядом особенностей, а именно:

– за одну секунду система способна сформировать до 7 пакетов данных (ПД);

– тайм слоты (ТС) объединяются в пакеты данных;

– каждое устройство в сети передает данные в свой тайм слот;

– каждому каналу связи может быть выделено несколько тайм слотов в одном пакете данных;

– все устройства принимают пакеты от всех.

Рассмотрим принцип работы протокола, представленный на рис. 5.2.

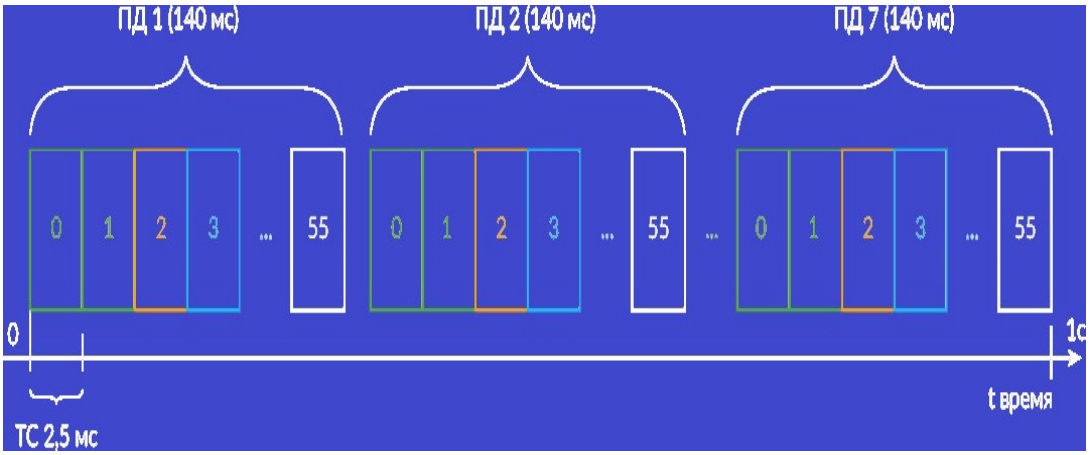


Рис. 5.2. Принцип работы протокола

Основными техническими характеристиками данного комплекса являются:

– эффективная излучаемая мощность приемопередатчика – 25 мВт;

– ширина спектра модулированного сигнала 0,5 МГц по уровню минус 30 дБ;

– рабочая частота приемопередатчика – 868,95 МГц;

– чувствительность приемника – минус 90 дБм (при вероятности ошибки принятых пакетов 1%);

– скорость передачи данных – 250 кбит/с;

– тип модуляции – QPSK;

– длительность работы приемопередатчика от полностью заряженной штатной аккумуляторной батареи в нормальных климатических условиях при соотношении времени «дежурный приём» – «приём» – «передача» 8:1:1 и номинальной мощности передатчика – 24 ч;

– наработка на отказ ТО не менее 6000 ч;

– срок службы – 3 года;

– рабочий диапазон температур – от –10 до + 50.

Рассмотрим преимущества системы «Волновая сеть»:

1) Комплекс обладает возможностью адаптации как к росту зоны необходимого радиопокрытия, так и к изменению условий приема и передачи сигнала.

2) «Волновая сеть» дистанционно управляема, технологическая платформа позволяет увеличить покрытие сети или перемещать его из одной области в другую.

3) Безопасность системы обеспечивается с помощью алгоритмов AES, DES или реализацией алгоритма шифрования ГОСТ 28147-89.

4) Система предлагает индивидуальные, групповые и конференц-вызовы в радиосети.

5) Способность организации связи в удаленных и труднодоступных зонах, таких как подвалы, подземные парковки, шахты, метрополитен и т.д.

6) «Волновая сеть» позволяет разделять абонентов на группы, такие как полиция, службы Министерства здравоохранения, службы спасения и т.д.

7) Комплекс позволяет сформировать до 250 логических каналов.

8) В системе управление сетью осуществляется диспетчером, который может комбинировать группы, включать и исключать абонентов из групп, осуществлять общий вызов и оповещение. Все управление происходит по беспроводному каналу.

9) «Волновая сеть» имеет малое время развертывания сети, так как не требуется проводить дорогостоящие монтажные работы.

10) В данном комплексе все устройства являются ретрансляторами, что позволяет увеличить надежность и зону покрытия. Каждая радиостанция может совершать до 8 ретрансляций одновременно, не прерывая прием или передачу сообщений.

11) Система способна передавать голосовую информацию, данные, сведения о местоположении и состоянии абонентов и сигналы с различных датчиков.

12) «Волновая сеть» поставляется с модулем беспроводного управления сетью и специальным программным обеспечением с широким спектром возможностей, которое устанавливается на персональный компьютер, ноутбук, планшет и т.д.

13) Комплекс включает широкий выбор антенно-фидерного оборудования для увеличения зоны покрытия, а также продукцию для выполнения различного вида задач.

14) Система обладает автономностью работы при чрезвычайных ситуациях, так как все оборудование имеет встроенные источники питания, способные обеспечить время автономной работы до 4 суток.

15) «Волновая сеть» способна взаимодействовать с различными системами связи.

16) Комплекс обладает широкой сферой применения.

Цифровой комплекс «Волновая сеть» включает в себя радиостанции, представленные в табл. 5.1.

Отмечая возможности и достоинства комплекса цифровой радиосвязи «Волновая сеть», рассмотрим несколько моделей комплексного применения средств связи данного типа [107].

Таблица 5.1 – Радиостанции цифрового комплекса «Волновая сеть»

Радиостанции				
«Гранит Р-86АЦ.210»	«Гранит Р-86АЦ.230»	«Гранит Р-86АЦ.270»	«Гранит Р-86АЦ.280»	«Гранит Р-86АЦ.290»
				

Особенностью самоорганизующихся сетей является то, что каждый узел сети может быть как оконечным устройством, так и ретранслятором, сети динамичны и их структура непостоянна и всё время изменяется, таким сетям не требуется заранее существующая инфраструктура связи, и они быстро разворачиваемы. Подобные свойства мобильных радиосетей обуславливают их широкое применение как в качестве беспроводных сетей управления, так и в условиях чрезвычайных обстоятельств, оперативного обеспечения значимых общественно-политических и массовых мероприятий.

В то же время, именно эти сферы и особенности применения таких сетей привлекают к ним внимание многочисленных нарушителей [109, 110]. При этом возможно разнообразие как потенциальных атак, так и применяемых при этом технических средств, что приводит к необходимости обеспечения информационной безопасности мобильных самоорганизующихся сетей.

Характерно, что при реализации атак на такую беспроводную сеть в силу присущих ей уязвимостей ущерб наносится не только ресурсам самой сети и ее элементов, но и целевой задаче функционирования сети в целом. Для реализации адекватной политики обеспечения информационной безопасности рассматриваемых в работе беспроводных сетей связи помимо оценки угроз информационной безопасности необходимы анализ и управление рисками в области информационной безопасности.

Предварительный анализ условий и задач функционирования мобильных сетей связи позволяет выявить принципиально возможные угрозы информационной безопасности. Выполненная идентификация опасностей (угроз безопасности) позволяет оценить их уровень и последствия, к кото-

рым они могут привести, а именно как вероятность деструктивных событий, так и вызванный ими потенциальный ущерб. В данной работе спектр угроз информационной безопасности, равно как и типы нарушителей, осуществляющих деструктивное воздействие на беспроводные мобильные сети, не рассматриваются. Будем полагать, что идентификация опасностей для рассматриваемых объектов реализована, и рассмотрим методы оценки риска для них. Покажем, что получить необходимые оценки рисков возможно на основе применения аппарата нечеткой логики, в том числе с использованием алгоритма Мамдани.

Построение в рассматриваемом объекте (беспроводной мобильной сети связи) системы защиты информационной безопасности требует учета рисков нарушения. При построении таких систем необходимо [111]:

– проанализировать возможные угрозы нарушения информационной безопасности, с учётом возможности их возникновения и возможного ущерба;

– определить угрозы, которые могут возникнуть в сети связи, провести анализ рисков информационной безопасности;

– построить систему, в которой данные риски учтены и против них существуют контрмеры.

Большую роль играет второй этап. Так, анализ рисков угроз позволяет произвести ранжирование рисков по заданному критерию. Согласно ГОСТ Р ИСО/МЭК 27002–2012, риск – это сочетание вероятности события и его последствия. Риск характеризуется также возможным ущербом, выраженным в качественном или количественном виде. Именно данные критерии могут быть использованы для оценки риска нарушения информационной безопасности.

Методы оценки риска нарушения информационной безопасности, в общем виде, делятся на качественные и количественные [108]. В настоящее время имеются формализованные процедуры качественной процедуры оценки рисков. В то же время имеющиеся работы в области защиты информации, посвященные вопросам анализа информационных рисков и управления ими, не содержат ряда важных деталей, которые надо обязательно конкретизировать при разработке применимых на практике методик. Таким образом, на сегодня отсутствует какая-либо единая, универсальная методика, соответствующая определенной концепции управления рисками. В каждом частном случае приходится адаптировать общую методику анализа рисков и управления ими под конкретные нужды объекта с учетом специфики его функционирования и решаемых задач.

Для оценки мобильной сети связи с точки зрения нарушения ИБ необходимо произвести анализ каждого риска в отдельности или сгруппировать риски по определённым параметрам. Такая систематизация рисков позволяет выбрать дальнейшие действия, предложить необходимые меры по снижению рисков до приемлемого уровня и выработать план организа-

ционно-технических мероприятий по противодействию при реализации риска. После чего становится возможным проводить повторный анализ сети с учетом используемых контрмер, заложенных в стратегию политики информационной безопасности, для оценки остаточных рисков.

В качестве примера рассмотрим случай риска нарушения информационной безопасности с использованием угрозы типа несанкционированное включение в радиосеть дополнительного узла [109].

При анализе данного риска используем аппарат нечёткой логики и алгоритм Мамдани. В рамках алгоритма Мамдани, удобного для описания системы с одним входом и одним выходом, рассматриваемая система связи может быть представлена в виде черного ящика, не требующего знания детальной информации о происходящих внутри него физических процессах.

Расчёт риска может быть произведен по формуле [110]:

$$S = P \cdot R, \qquad (5.1)$$

где S – риск, P – вероятность реализации данного риска, R – последствия.

Для измерения рисков необходимо определить шкалы, по которым оцениваются риски.

Для использования алгоритма Мамдани необходимо каждой логической переменной присвоить терм-фактор. Для S – {ОЧЕНЬ ВАЖНЫЙ, ВАЖНЫЙ, УМЕРЕННО ВАЖНЫЙ, ПРИЕМЛЕМЫЙ, НЕ ВАЖНЫЙ}, для P – {ОЧЕНЬ ВЫСОКАЯ, ВЫСОКАЯ, УМЕРЕННАЯ, НИЗКАЯ, ОЧЕНЬ НИЗКАЯ}, для R – {КРИТИЧНЫЕ, ПРИЕМЛЕМЫЕ, НИЗКИЕ}.

После чего присваиваются качественные и количественные оценки используемым логическим переменным.

Таблица 5.2

Качественное обозначение риска	Количественная оценка риска
очень важный	1
важный	0,75
умеренно важный	0,5
приемлемый	0,25
не важный	0

Таблица 5.3

Качественное обозначение вероятности реализации	Количественная оценка вероятности
очень высокая	1
высокая	0,825
умеренная	0,65
низкая	0,475
очень низкая	0,3

Таблица 5.4

Качественное обозначение последствий риска	Количественная оценка последствий
критичные	1
приемлемые	0,5
низкие	0

При построении сети, где не требуется идентификация пользователя в сети, создаётся база знаний на основе правила: Если «…» и «…», то «…».
1) ЕСЛИ P = «ОЧЕНЬ ВЫСОКАЯ» И R = «КРИТИЧНЫЕ», ТО S = «ОЧЕНЬ ВАЖНЫЙ».

2) ЕСЛИ P = «ОЧЕНЬ ВЫСОКАЯ» И R = «ПРИЕМЛЕМЫЕ», ТО S = «УМЕРЕННО ВАЖНЫЙ».

3) ЕСЛИ P = «ОЧЕНЬ ВЫСОКАЯ» И R = «НИЗКИЕ», ТО S = «НЕ ВАЖНЫЙ».

4) ЕСЛИ P = «ВЫСОКАЯ» И R = «КРИТИЧНЫЕ», ТО S = «ОЧЕНЬ ВАЖНЫЙ».

5) ЕСЛИ P = «ВЫСОКАЯ» И R = «ПРИЕМЛЕМЫЕ», ТО S = «ПРИЕМЛЕМЫЙ».

6) ЕСЛИ P = «ВЫСОКАЯ» И R = «НИЗКИЕ», ТО S = «НЕ ВАЖНЫЙ».

7) ЕСЛИ P = «УМЕРЕННАЯ» И R = «КРИТИЧНЫЕ», ТО S = «УМЕРЕННО ВАЖНЫЙ».

8) ЕСЛИ P = «УМЕРЕННАЯ» И R = «ПРИЕМЛЕМЫЕ», ТО S = «ПРИЕМЛЕМЫЙ».

9) ЕСЛИ P = «УМЕРЕННАЯ» И R = «НИЗКИЕ», ТО S = «НЕ ВАЖНЫЙ».

10) ЕСЛИ P = «НИЗКАЯ» И R = «КРИТИЧНЫЕ», ТО S = «ПРИЕМЛЕМЫЙ».

11) ЕСЛИ P = «НИЗКАЯ» И R = «ПРИЕМЛЕМЫЕ», ТО S = «НЕ ВАЖНЫЙ».

12) ЕСЛИ P = «НИЗКАЯ» И R = «НИЗКИЕ», ТО S = «НЕ ВАЖНЫЙ».

13) ЕСЛИ P = «ОЧЕНЬ НИЗКАЯ» И R = «КРИТИЧНЫЕ», ТО S = «ПРИЕМЛЕМЫЙ».

14) ЕСЛИ P = «ОЧЕНЬ НИЗКАЯ» И R = «ПРИЕМЛЕМЫЕ», ТО S = «НЕ ВАЖНЫЙ».

15) ЕСЛИ P = «ОЧЕНЬ НИЗКАЯ» И R = «НИЗКИЕ», ТО S = «НЕ ВАЖНЫЙ».

Получаемые с помощью такого подхода зависимости лингвистической переменной S имеют вид, показанный на рис. 5.3, на котором приведена некоторая поверхность в системе координат P, R как один из возможных вариантов определения значений риска (согласно соотношению 5.1), при использовании рассмотренной базы знаний.

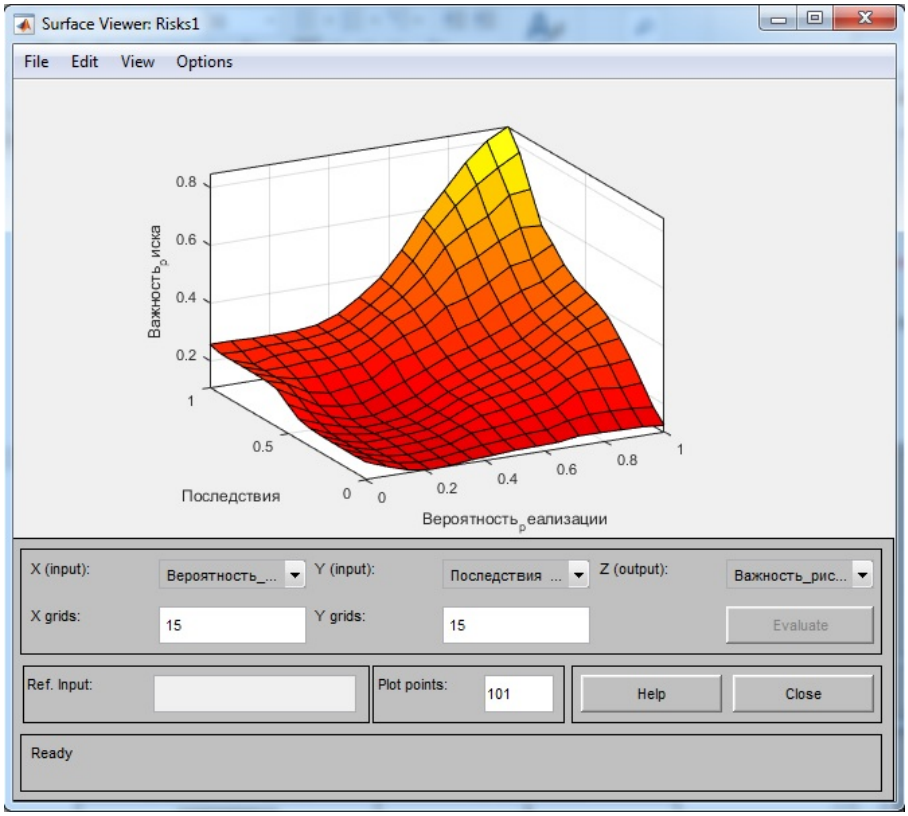


Рис. 5.3. Риск, обусловленный включением в сеть без идентификации узла

При использовании аутентификации узлов сети изменятся количественные оценки вероятности реализации данного риска сети. Они приведены в табл. 5.5, остальные качественные и количественные оценки остаются неизменными.

Таблица 5.5

Качественное обозначение вероятности реализации	Количественная оценка вероятности
очень высокая	1
высокая	0,75
умеренная	0,5
низкая	0,25
очень низкая	0

Использование новых количественных оценок вероятности реализации риска изменит базу знаний, она будет выглядеть следующим образом.

1) ЕСЛИ P = «ОЧЕНЬ ВЫСОКАЯ» И R = «КРИТИЧНЫЕ», ТО S = «ОЧЕНЬ ВАЖНЫЙ».

2) ЕСЛИ P = «ОЧЕНЬ ВЫСОКАЯ» И R = «ПРИЕМЛЕМЫЕ», ТО S = «УМЕРЕННО ВАЖНЫЙ».

3) ЕСЛИ P = «ОЧЕНЬ ВЫСОКАЯ» И R = «НИЗКИЕ», ТО S = «НЕ ВАЖНЫЙ».

4) ЕСЛИ P = «ВЫСОКАЯ» И R = «КРИТИЧНЫЕ», ТО S = «ВАЖНЫЙ».

5) ЕСЛИ P = «ВЫСОКАЯ» И R = «ПРИЕМЛЕМЫЕ», ТО S = «ПРИЕМЛЕМЫЙ».

6) ЕСЛИ P = «ВЫСОКАЯ» И R = «НИЗКИЕ», ТО S = «НЕ ВАЖНЫЙ».

7) ЕСЛИ P = «УМЕРЕННАЯ» И R = «КРИТИЧНЫЕ», ТО S = «УМЕРЕННЫЙ».

8) ЕСЛИ P = «УМЕРЕННАЯ» И R = «ПРИЕМЛЕМЫЕ», ТО S = «ПРИЕМЛЕМЫЙ».

9) ЕСЛИ P = «УМЕРЕННАЯ» И R = «НИЗКИЕ», ТО S = «НЕ ВАЖНЫЙ».

10) ЕСЛИ P = «НИЗКАЯ» И R = «КРИТИЧНЫЕ», ТО S = «ПРИЕМЛЕМЫЙ».

11) ЕСЛИ P = «НИЗКАЯ» И R = «ПРИЕМЛЕМЫЕ», ТО S = «НЕ ВАЖНЫЙ».

12) ЕСЛИ P = «НИЗКАЯ» И R = «НИЗКИЕ», ТО S = «НЕ ВАЖНЫЙ».

13) ЕСЛИ P = «ОЧЕНЬ НИЗКАЯ» И R = «КРИТИЧНЫЕ», ТО S = «НЕ ВАЖНЫЙ».

14) ЕСЛИ P = «ОЧЕНЬ НИЗКАЯ» И R = «ПРИЕМЛЕМЫЕ», ТО S = «НЕ ВАЖНЫЙ».

15) ЕСЛИ P = «ОЧЕНЬ НИЗКАЯ» И R = «НИЗКИЕ», ТО S = «НЕ ВАЖНЫЙ».

Получившаяся поверхность для важности рисков с использованием новой базы знаний изображена на рис. 5.4.

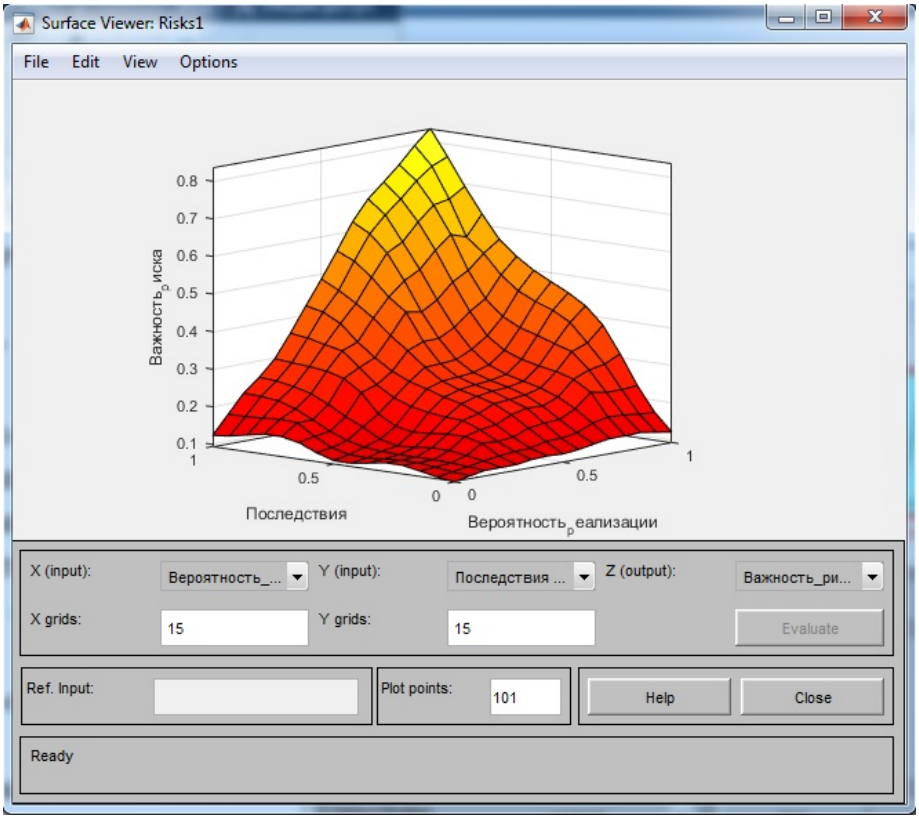


Рис. 5.4. Риск для случая включения в сеть с идентификацией узла

На рис. 5.4, видно, как изменяется риск, при использовании идентификации узлов при их новом включении в сеть.

Формирование базы знаний, с использованием аппарата нечеткой логики для анализа рисков нарушения информационной безопасности в самоорганизующихся сетях помогает выполнить количественную оценку рисков нарушения ИБ, что в дальнейшем может использоваться для построения системы защиты сети связи на основе полученных оценок рисков нарушения ИБ, характерных для рассмотренного типа угроз.

Использование алгоритма Мамдани для управления динамическими объектами позволяет исследовать риски нарушения информационной безопасности в самоорганизующихся сетях и дальнейшее управление ими. Полученная геометрическая поверхность быстро реагирует на изменение в изучаемой динамической системе и заданные новые выходные данные, это происходит из-за того, что геометрическая поверхность строится на основе нечеткой базы знаний, опираясь на информацию, полученную от исследуемой системы, что позволяет оперативно оценить полезность от введённой системы контрмер.

Выводы

Организация и проведение оценки рисков нарушения информационной безопасности в информационных, телекоммуникационных системах ОВД позволяет получать обоснованные оценки рисков, уязвимостей, эффективности защиты. Для оценки эффективности разработанной системы была проведена оценка безопасности для информационных, телекоммуникационных систем ОВД. В результате было подтверждено соответствие между реальной безопасностью информационной системы и назначенными оценками.

ЗАКЛЮЧЕНИЕ

Задача формирования комплекса средств противодействия угрозам информационной безопасности в сетях связи специального назначения в условиях цифровизации технологической инфраструктуры видоизменяется и усложняется. Для ее решения требуются новые наукоемкие методы, учитывающие специфику развивающихся СССН в условиях конвергенции и особенности их функционирования.

Предложенные в данной монографии методы и модели базируются на теории нечетких множеств, лингвистической неопределенности, нечеткой логики. Изложены принципы оптимального интегрирования разнородных информационных процессов в интересах противодействия угрозам информационной безопасности в сетях связи специального назначения

Разработан метод теории эффективности, декомпозиции и оптимизации показателей качества функционирования сетей связи специального назначения при условии защиты от разрушающих информационных воздействий. Методы используют лингвистические переменные и нечеткие экспертные системы.

Представленный в монографии материал не может претендовать на абсолютную полноту раскрытия рассматриваемой в нем научно-технической проблемы. С учетом большого количества интенсивно развивающихся методов исследования с привлечением аппарата математического моделирования можно сказать, что в данной работе рассмотрены лишь некоторые аспекты. К ним можно отнести методы вычислительного эксперимента, которые, несомненно, станут предметом следующих научных исследований.

Очевидным достоинством данного издания является попытка систематизации знаний, которые в своей совокупности и последовательности изложения смогли бы способствовать решению многих вопросов, связанных с формированием комплекса средств противодействия угрозам информационной безопасности в сетях связи специального назначения.

Особое значение для авторского коллектива имеет актуальность проблем исследования и совершенствования технологий обеспечения информационной безопасности в СССН. Данное направление стимулирует творческий поиск и формирует вектор дальнейших исследований.

Таким образом, авторы надеются, что это не последняя редакция данного издания. В следующих изданиях должны появиться результаты развития методов моделирования для обеспечения информационной безопасности сетей связи специального назначения.

ЛИТЕРАТУРА

1. О связи : федер. закон от 07.07.2003 № 126-ФЗ // СПС «Консультант Плюс». – URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=284635&fld=134&dst=1000000001,0&rnd=0.05115289769807 9736#08312366978414549 (дата обращения: 03.02.2020).

2. Буренин А. Н. Вопросы безопасности инфокоммуникационных систем и сетей специального назначения: основные угрозы, способы и средства обеспечения комплексной безопасности сетей / А. Н. Буренин, К. Е. Легков // Наукоемкие технологии в космических исследованиях земли. – Москва : II&ES RESEARH. – 2015. – №3. – С.46–61.

3. Модели процессов организации обработки оперативной информации современными вычислительными комплексами в условиях противодействий / К. Е. Легков, А. Н. Буренин // Вопросы оборонной техники. – Санкт-Петербург : Научно-производственное объединение специальных материалов, 2018. – № 3. – С. 87–95.

4. Макаренко С. И. Динамическая модель системы связи в условиях функционально-разноуровневого информационного конфликта наблюдения и подавления / С. И. Макаренко // Системы управления, связи и безопасности. – Санкт-Петербург : Интел Групп, 2015. – № 3. – С. 122–185.

5. Макаренко С. И. Описательная модель сети связи специального назначения / С. И. Макаренко // Системы управления, связи и безопасности. – Санкт-Петербург : Интел Групп, 2017. – № 2. – С. 113–164.

6. Боговик А. В. Эффективность военной связи и методы ее оценки // А. В. Боговик, В. В. Игнатов. – Санкт-Петербург : ВАС, 2006. – 183 с.

7. Хохлов Н. С. Моделирование и оптимизация противодействия разрушению информации в системах управления и связи органов внутренних дел в условиях противодействия угрозам информационной безопасности: монография / Н. С. Хохлов. – Воронеж : Воронежский институт МВД России, 2005. – 181 с.

8. Новосельцев В. И. Тензорный анализ Крона и его приложения : монография / В. И. Новосельцев, С. С. Кочедыков, Д. Е. Орлова ; под ред. В. И. Новосельцева. – Воронеж : Научная книга, 2017. – 260 с.

9. Малюк А. А. Основы политики безопасности критических систем информационной инфраструктуры : курс лекций / А. А. Малюк. – Москва : Горячая линия – Телеком, 2019. – 314 с.

10. Методы формирования элементов комплекса противодействия разрушению информации в системах связи специального назначения при деструктивных широкополосных воздействиях : свидетельство о государственной регистрации программы для ЭВМ от 05.02.2020 № 2020611635 / И. В. Гилев, С. В. Канавин, А. В. Попов. – Москва : ФИПС, 2020.

11. Главные тенденции в защите информации. – URL: https://www.tadviser.ru/index.php/ (дата обращения: 30.08.2020).

12. Новиков Д. А. Теория управления организационными системами. 2-е изд. – Москва : Физмалит, – 2007. – 584 с.

13. Гилев И. В. Модель противодействия разрушению информации при деструктивных электромагнитных воздействиях в системах радиосвязи специального назначения на основе нечетких экспертных систем / И. В. Гилев // Вестник Воронежского института МВД России. – 2020. – № 1. – С. 158–168.

14. Дунин В. С. Модель угроз информационной безопасности комплексной автоматизированной интеллектуальной системы «Безопасный город» / Н. С. Хохлов, В. С. Дунин // Вестник Воронежского института МВД России. – 2011. – № 4. – С. 74–79.

15. Программа выбора способов противодействия деструктивным электромагнитным воздействиям на основе нейронных сетей : свидетельство о государственной регистрации программы для ЭВМ от 04.06.2020 № 2020614645 / И. В. Гилев, С. В. Канавин, А. В. Попов, Н. С. Хохлов. – Москва : ФИПС, 2020.

16. Моделирование процессов вторичных геодинамических факторов в целях обеспечения правоохранительного сегмента АПК «Безопасный город» / О. И. Бокова, К. М. Бондарь, В. С. Дунин, С. В. Канавин, П. Б. Скрипко // Моделирование, оптимизация и информационные технологии: электрон. науч. журн. – 2018. – № 4 (23). – С. 507–522.

17. Хохлов Н. С. Требования к информационной безопасности систем радиомониторинга, сбора и обработки информации органов внутренних дел / Н. С. Хохлов, С. В. Канавин, А. С. Серпилин // Научно-технический портал МВД России. – Москва : ФКУ НПО СТИС МВД России, 2019. – № 1. – С. 14–22.

18. Gilev I. Modeling the Destructive Effect of Interference on Mobile Networks, Using the 3G Standard as an Example, Using a Noise Generator I. Gilev, S. Kanavin // Bulletin of the Lipetsk State Technical University. 1st International Conference on Control Systems, Mathematical Modelling, Automation and Energy Efficiency (SUMMA). – Lipetsk, 2019. – p. 407–410. DOI: – 10.1109/SUMMA48161.2019.8947533.

19. Сети связи следующего поколения NGN / под ред. А. В. Рослякова. – Москва : Эко-Трендз, 2008. – 424 с.

20. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / под ред. Д. П. Зегжды. – Москва : Горячая линия – Телеком, 2020. – 560 с.

21. Скрыль С. В. Угрозы несанкционированного доступа к компьютерной информации и предупреждение подобных деяний в компьютерных

сетях органов внутренних дел / С. В. Скрыль, Д. С. Мишин // Наука и практика. – № 3(29). – Орел : Орловский юридический институт МВД России, 2006. – С. 6–8.

22. Анализ угроз безопасности в информационно-телекоммуникационных системах / С. В. Скрыль [и др.]. // Системы безопасности: материалы девятой научно-технической конференции – СБ-2000 Международного форума информатизации. – Москва : Академия ГПС МВД России, 2000. – С. 91–94.

23. Классификация угроз безопасности информационно-телекоммуникационных систем / С. В. Скрыль [и др.]. // Системы безопасности : материалы девятой научно-технической конференции – СБ-2000 Международного форума информатизации. – Москва : Академия ГПС МВД России, 2000. – С. 94–98.

24. Неправомерное использование информации в виртуальном мире / С. В. Скрыль [и др.]. // Вестник Воронежского института МВД России. – Воронеж: Воронежский институт МВД России, 2005. – № 5 (24). – С. 75–79.

25. Платонов Д. В. Математические модели для оценки эффективности средств интегрированной защиты информации комплексных систем безопасности объектов : дис. канд. техн. наук / Д. В. Платанов. – Воронеж, 2008. – 147 с.

26. Сети радиосвязи специального назначения : учебник / О. И. Бокова [и др.] ; под ред. Н. С. Хохлова. – Воронеж : Воронежский институт МВД России, 2018. – 255 с.

27. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях / В. Ф. Шаньгин. – Москва : ДМК Пресс, 2012. – 592 с.

28. Дунин В. С. Состояние и перспективы развития функциональных подсистем комплексной автоматизированной интеллектуальной системы «Безопасный город» / В. С. Дунин // Общественная безопасность, законность и правопорядок в III тысячелетии : сборник материалов международной научно-практической конференции. – Ч. 3 : Естественные, математические и технические науки. – Воронеж : Воронежский институт МВД России, 2010. – С. 33–40.

29. Дунин В. С. К вопросу о построении модели управления подсистемы защиты информации комплексной автоматизированной интеллектуальной системы «Безопасный город» / В. С. Дунин // Актуальные вопросы эксплуатации систем охраны и защищенных телекоммуникационных си-

стем : сб. материалов всероссийской научно-практической конференции курсантов, слушателей, студентов, адъюнктов и молодых специалистов. – Воронеж : Воронежский институт МВД России, 2011. – С. 91–92.

30. Информационная безопасность открытых систем : учебник для вузов : в 2 т. Т. 1 : Угрозы, уязвимости, атаки и подходы к защите / С. В. Запечников [и др.]. – Москва : Горячая линия–Телеком, 2006. – 536 с.

31. Машкина И. В. Интеллектуальная поддержка принятия решений по управлению защитой информации в критически важных сегментах информационных систем / И. В. Машкина, М. Б. Гузаиров // Приложение к журналу «Информационные технологии». – 2008. – № 7. – С. 32.

32. Национальный стандарт Российской Федерации. Информационная технология. Практические правила управления информационной безопасностью : ГОСТ ИСО/МЭК 17799 – 2005 г.

33. Куликов В. В. Дискретная математика : учебное пособие / В. В. Куликов. – Москва : РИОР, 2007. – 174 с.

34. Дунин В. С. Построение модели интеллектуальной системы управления безопасностью объекта информатизации ОВД на основе нечеткой нейронной продукционной сети / В. С. Дунин, О. И. Бокова, Н. С. Хохлов // Вестник Воронежского института МВД России. – 2011. – № 2. – С. 48–58.

35. Бокова О. И. Оптимальное управление безопасностью территориальных сегментов информационно-телекоммуникационных систем / О. И. Бокова ; под ред. С. В. Скрыля. – Воронеж : Воронежский институт МВД России, 2006. – 153 с.

36. Бурков В. Н. Модели и механизмы управления в самоорганизующихся системах : монография. – Воронеж : Научная книга, 2008. – 300 с.

37. Хохлов Н. С. Распределение ресурса системы связи и управления как задача оптимизации по выбранному критерию / Н. С. Хохлов // Материалы всероссийской конференции «Современные проблемы борьбы с преступностью: информационная безопасность в деятельности органов внутренних дел». – Воронеж : Воронежский институт МВД России, 2005. – С. 21–22.

38. Скрыль С. В. Противодействие угрозам разрушения информации в системах управления и связи как проблема оптимального интегрирования разнородных информационных процессов / С. В. Скрыль, Н. С. Хохлов // Безопасность информационных технологий. – Москва: МИФИ, 2005. – Вып. 2. – С. 57–69.

39. Макаренко С. И. Информационные конфликты – анализ работ и методология исследования / С. И. Макаренко, Р. Л. Михайлов // Системы управления, связи и безопасности. – Санкт-Петербург : Интел Групп, 2016. – № 3. – С. 95–178.

40. Модели управления конфликтами и рисками [Текст]: Монография. / С. А. Баркалов [и др.] ; под ред. Д. А. Новикова. – Воронеж : Научная книга, 2008. – 495 с.

41. О подходах реализации централизованной системы управления информационной безопасностью АСУ военного и специального назначения / Ю. В. Бородакий [и др.] // Вопросы кибербезопасности. – Москва : НПО «Эшелон», 2014. – № 2(3). – С. 2–8.

42. Паршуткин А. В. Концептуальная модель взаимодействия конфликтующих информационных и телекоммуникационных систем / А. В. Паршуткин // Вопросы кибербезопасности. – Москва : Эшелон, 2014. – № 5(8). – С. 2–6.

43. Хохлов Н. С. Современные информационные технологии как основа системы радиосвязи МВД России / Н. С. Хохлов, С. Н. Ляшенко // Охрана, безопасность, связь – Воронеж : Воронежский институт МВД России, 2017. – №1. – С. 12-19.

44. Канавин С. В.Разработка мультисервисной сети связи специального назначения : учебно-практическое пособие / С. В. Канавин, Д. А. Жайворонок, Н. С. Хохлов. – Воронеж : Воронежский институт МВД России, 2018. – 79 с.

45. Канавин С. В. Перспективы применения систем мобильного широкополосного доступа в сетях подвижной радиосвязи на основе стандартов MOBILE WIMAX и LTE / С. В. Канавин, А. С. Лукьянов // Моделирование, оптимизация и информационные технологии. – Воронеж : Воронежский институт высоких технологий, 2016. – № 2. – С. 6–10.

46. Назаров А. Н. Модели и методы расчета показателей качества функционирования узлового оборудования и структурно-сетевых параметров сетей связи следующего поколения / А. Н. Назаров, К. И. Сычев. – Красноярск : Поликом, 2010. – 389 с.

47. Канавин С. В. Организация оперативных сетей радиосвязи на основе ROIP технологий / С. В. Канавин, С. Н. Ляшенко, О. И. Бокова // Актуальные проблемы деятельности подразделений УИС : сборник материалов всероссийской научно-практической конференции. – Воронеж : Воронежский институт ФСИН России, 2015. – С. 118–120.

48. Фоменко Г. И. Симбиоз прошлого и будущего эффективно работает в настоящем / Г. И. Фоменко // Информационные технологии, связь и защита информации МВД России – Москва : Информационный мост, 2016. – С. 90–93.

49. Хохлов Н. С. Методы декомпозиции систем связи специального назначения для реализации алгоритмов оценки эффективности их функционирования в условиях конфликтного существования / Н. С. Хохлов, С. Н. Ляшенко // Общественная безопасность, законность и правопорядок в III тысячелетии – Воронеж : Воронежский институт МВД России, 2016. – № 1. – С. 185-188.

50. Бокова О. И. Показатели оценки эффективности региональных компьютерных систем в условиях противодействия угрозам информационной безопасности / О. И. Бокова, С. В. Скрыль // Труды всероссийской конференции «Интеллектуализация управления в социальных и экономических системах» Российская академия естественных наук им. В. И. Вернадского. – Воронеж : Воронежский государственный технический университет, 2006. – С. 77–78.

51. Овчинский А. С. Информация и оперативно-розыскная деятельность: монография / А. С. Овчинский. – Москва : ИНФРА-М, 2002. – 97 с.

52. Батищев Р. В. К вопросу о решении проблем обеспечения безопас-ности информационных систем / Р. В. Батищев, О. Д. Морева, С. Л. Подвальный // Информация и безопасность. – 2005. – Вып. 1. – С. 122-129.

53. Ажмухамедов И. М. Решение задач обеспечения информационной безопасности на основе системного анализа и нечеткого когнитивного моделирования : монография / И. М. Ажмухамедов. – Астрахань, 2012. – 344 с.

54. Завгородний В. И. Комплексная защита информации в компьютерных системах : учебное пособие / В. И. Завгородний. – Москва : Логос. – 2001. – 264 с.

55. Александров Е. А. Основы теории эвристических решений / Е. А. Александров. – Москва : Советское радио, 1975. – 256 с.

56. Новиков Д. А. Теория управления организационными системами: учебно-методическое пособие / Д. А. Новиков. – Москва : МПСИ, 2005. – 584 с.

57. Калинин В. Н. Теория систем и оптимального управления. Ч. II / В. Н. Калинин, Б. А. Резников, Е. И. Варакин. – Москва : Министерство обороны СССР, 1987. – 589 с.

58. Комплексные системы защиты информации предприятия: учебное пособие / В. Т. Еременко [и др.]. – Орел : Орловский государственный университет имени И. С. Тургеньева», 2016. – 116 с.

59. Месарович М. Теория иерархических многоуровневых систем / М. Месарович, Д. Мако, И. Такахара. – Москва : Мир, 1973. – 344 с.

60. Лазарев И. А. Композиционное проектирование сложных агрегативных систем / И. А. Лазарев. – Москва : Радио и связь, 1986. – 312 с.

61. Язов Ю. К. Организация защиты информации в информационных системах от несанкционированного доступа : монография / Ю. К. Язов, С. В. Соловьев. – Воронеж : Кварта, 2018. – 588 с.

62. Ларичев О. И. Наука и искусство принятия решений / О. И. Ларичев. – Москва : Наука, 1979. – 200 с.

63. Заде Л. А. Понятие лингвистической переменной и его применение к принятию приближенных решений / Л. А. Заде. – Москва : Мир, 1976. – 168 с.

64. Поспелов Д. А. Логико-лингвистические модели в системах управления / Д. А. Поспелов. – Москва : Энергия, 1981. – 231 с.

65. Поспелов Д. А. Ситуационное управление: теория и практика / Д. А. Поспелов. – Москва : Наука, 1986. – 284 с.

66. Строгалев В. П. Имитационное моделирование : учебное пособие / В. П. Строгалев, И. О. Толкачева. – Москва : МГТУ им Н. Э. Баумана, 2018. – 430 с.

67. Зарубин В. С. Математические модели прикладной механики: учебное пособие / В. С. Зарубин, Г. Н. Кувыркин, И. В. Толкачева. – Москва : МГТУ им Н.Э. Баумана, 2016. – 300 с.

68. Лазарев И. А. Информация и безопасность. Композиционная технология информационного моделирования сложных объектов принятия решений. / И. А. Лазарев. – Москва : Московский городской центр НТИ, 1997. – 336 с.

69. Моделирование информационных операций и атак в сфере государственного и муниципального управления / В. Г. Кулаков [и др.]. – Воронеж : Воронежский институт МВД России, 2004. – 144 с.

70. Зыков А. А. Теория конечных графов / А. А. Зыков. – Новосибирск : Наука, 1969. – 543 с.

71. Татт У. Теория графов: пер. с англ. / У. Татт. – Москва : Мир, 1988. – 424 с.

72. Советов Б. Я. Моделирование систем : учеб. для вузов / Б. Я. Советов, С. А. Яковлев – 3-е изд., перераб. и доп. – Москва : Высшая школа, 2001. – 343 с.

73. Бусленко Н. П. Моделирование сложных систем / Н. П. Бусленко. – Москва : Наука, 1978. – 400 с.

74. Вентцель Е. С. Исследование операций / Е. С. Вентцель – Москва : Советское радио, 1972. – 552 с.

75. La Vigne N. G. Using Public Surveillance Systems for Crime Control and Prevention: A Practical Guide for Law Enforcement and Their Municipal Partners Washington. / N. G. La Vigne [et al.]. – D.C. : Urban institute Justice Policy Center, 2011. – 60 p.

76. Ariel B. Police Body Cameras in Large Police Departments // Journal of Criminal Law and Criminology. – Chicago : Northwestern University School of Law, 2016. – P. 729–768.

77. Кустов А. М. Проблемы применения видеозаписи при расследовании преступлений против личности / А. М. Кустов, А. М. Кокорев // Труды академии управления МВД России. – 2018. – Москва : Академия управления МВД России, 2018. – С. 73-77.

78. Смахин Е. В. Применение систем видеофиксации в раскрытии и расследовании преступлений / Е. В. Смахин, С. В. Щербич // Алтайский юридический вестник – 2017. – Барнаул : Барнаульский юридический институт МВД России, 2017. – С. 137–141.

79. Муленков Д. В. Видеозапись как один из способов фиксации криминалистически значимой информации. / Д. В. Муленков, О. Н. Лазаренко // Вестник Московского университета МВД России. – Москва : Московский университет МВД России, 2017. – С. 107–110.

80. Защита информации в каналах связи методом формирования маскирующих сигналоподобных помех. Вестник Поволжского государственного технологического университета. Серия: Радиотехнические и инфокоммуникационные системы. / Н. С. Хохлов [и др.]. – Йошкар-Ола : Поволжский государственный технологический университет, 2018. – № 4. – С. 6–14.

81. Егоров Н. П. Новая структура портативных цифровых видеолиний. / Н. П. Егоров // Материалы VII международной научно-практической

конференции «INTERMATIC – 2009». – Москва : МИРЭА. – Ч. 4. – С. 186-189.

82. Канавин С. В. Анализ состояния и перспективы развития систем видеонаблюдения на основе беспроводных технологий 4G. / С. В. Канавин, А. С. Лукьянов // Вестник Воронежского института высоких технологий. – 2017. – № 4. – С. 73–75.

83. Родионов А. Ю. Комплексный анализ помехоустойчивости многочастотных сигналов COFDM с частотной модуляцией. / А. Ю. Родионов, С. Г. Стаценко // Вестник Воронежского государственного университета. – Воронеж : Воронежский государственный университет, 2007.– № 1. – С. 33–35.

84. Хохлов Н. С. Типовые модели деструктивных широкополосных и сверхширокополосных сигналов, воздействующих на системы связи специального назначения. Вестник Воронежского института МВД России / Н. С. Хохлов, С. В. Канавин, И. В. Гилев. – Воронеж : Воронежский институт МВД России, 2018. – № 1. – С. 91–101.

85. Методика количественной оценки влияния радиопомех и сигнала радиоэлектронных средств на показатели радиоэлектронной защиты. / Н. С. Хохлов, С. Н. [и др.]. // Вестник Поволжского государственного технологического университета. Серия: Радиотехнические и инфокоммуникационные системы. – Йошкар-Ола : Поволжский государственный технологический университет, 2019.– № 1. – С. 22–30.

86. Гилев И. В. Моделирование системы мобильного широкополосного доступа стандарта WIMAX в условиях многолучевого распространения сигнала. / И. В. Гилев, С. В. Канавин // Вестник Воронежского института МВД России, 2019. – № 2. – С. 181–191.

87. Макаренко С. И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века : Монография / С. И. Макаренко. – Санкт Петербург : Наукоемкие технологии, 2017. – 546 с.

88. Шерстобитов Р. С. Маскирование интегрированных сетей связи ведомственного назначения. / Р. С. Шерстобитов, С. Р. Шарифуллин, Р. В. Максимов // Системы управления, связи и безопасности. – 2018. – № 4. – С. 136–175.

89. Вовчук Д. А. Моделирование системы передачи цифровой информации с помощью хаотического маскирования. / Д. А. Вовчук // Технологический аудит и резервы производства.– 2013. – №5. – С. 55-57.

90. Дворянкин С. В. Сепарация и маскировка речевых сообщений в многоканальных системах конфиденциальной голосовой связи / С. В. Дворянкин, А. А. Мишуков. – Москва : Спецтехника и связь, 2011. – № 1. – С. 40–47.

91. Канавин С. В. Применение алгоритма оптимальной обработки сигналов для защиты информации в каналах связи с зашумлением / С. В. Канавин, С. Н. Панычев, В. Б. Авдеев // Вестник Воронежского института ФСИН России. – 2012. – № 1. – С. 14–18.

92. Формирование оптимальной имитационной помехи для подавления несанкционированных сеансов связи. / С. Н. Панычев [и др.]. // Вестник Воронежского института ФСИН России, 2013. – №1. – С. 26-31.

93. Канавин С. В. Оптимизация передачи и приема информации в каналах связи с зашумлением. / С. В. Канавин, С. Н. Панычев // Вестник Воронежского государственного технического университета, 2011. – Т.7. – №10. – С. 26–31.

94. Павлов И. И. Энергетическая эффективность усилителя в моногармоническом режиме (Классы А, В, С). / И. И. Павлов, Д. Ю. Старыш // World science: problems and innovations, 2017. – Т.1. – С. 26–30.

95. Методика и результаты тестирования модели канала с аддитивными и мультипликативными помехами. / Ю. Ф. Сургутов[и др.]. // Математические структуры и моделирование. – Омск : Омский государственный университет имени Ф. М. Достоевского, 2016. – № 2. – С. 60–65.

96. Дубовский В. В. Оценка пропускной способности канала с аддитивными и мультипликативными помехами для сигнальной конструкции на основе фазовой манипуляции. / В. В. Дубовский, С. И. Отрох, М. С. Попова. // Проблемы инфокоммуникаций. – Минск : Белорусская государственная академия связи, 2017. – Т.2 (2).– №10. – С. 88–94.

97. Хохлов Н. С. Использование многосекторной антенной системы MIMO как элемента комплекса средств противодействия деструктивным электромагнитным воздействиям. / Н. С. Хохлов, И. В. Гилев, С. В. Канавин. // Вестник Воронежского института МВД России, 2019. – № 4. – С. 126–136.

98. Мельников В. П. Информационная безопасность: учебник / В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева ; под ред. В. П. Мельникова. – 2-е изд., перераб. и доп. – Москва : КНОРУС, 2018. – 372 с.

99. Экспериментальное исследование и моделирование квадратурного фазового модулятора с аналоговыми функциональными преобразователями модулирующего напряжения в режиме импульсно-шумового модулирующего воздействия / С. А. Шерстюков [и др.]. // Вестник Воронежского государственного технического университета, 2010. – Т. 6. – № 6. – С. 136-141.

100. Шерстюков С. А. Теория и применение квадратурных формирователей радиосигналов с угловой модуляцией: Монография / С. А. Шерстюков, Н. С. Хохлов, С. С. Никулин – Воронеж: «Научная книга», 2009 – 144 с.

101. Квадратурные формирователи радиосигналов : монография / под ред. П. А. Попова. – Воронеж : Воронежский институт МВД России, 2001. – 176 с.

102. Панычев С. Н. Нелинейные радиоизмерения и контроль характеристик изделий военной электроники : монография / С. Н. Панычев. – Воронеж : Военный институт радиоэлектроники, 2004. – 178 с.

103. Авдеев В. Б. Энтропийно-вероятностный фильтр для обнаружения шумоподобных сигналов / В. Б. Авдеев, С. Н. Панычев, Д. В. Сенькевич // Информационно- измерительные и управляющие системы. – Москва : Радиотехника, 2007. – Т. 5. – №6. – С. 3–8.

104. Макаренко С. А. Помехозащищенность систем связи с псевдослучайной перестройкой рабочей частоты : монография / С. А. Макаренко, М. С. Иванов, С. А. Попов. – Санкт Петербург : Свое издательство, 2013. – 166 с.

105. Способ противодействия деструктивным электромагнитным воздействиям, основанный на дополнительной модуляции с применением вейвлет-преобразования / И. В. Гилев[и др.]. Моделирование, оптимизация и информационные технологии – Воронеж : Воронежский институт высоких технологий, 2020. – №2. – С. 1–11.

106. Канавин С. В. Модель комплекса противодействия угрозам информационной безопасности в сетях связи специального назначения: Моделирование, оптимизация и информационные технологии / О. И. Бокова, Д. А. Жайворонок, С. В. Канавин, Н. С. Хохлов. – Воронеж : Воронежский институт высоких технологии, 2020. – № 2. – С. 1–14.

107. Рыбокитов А. Е. Методический подход к оценке рисков нарушения информационной безопасности в самоорганизующихся мобильных сетях на основе аппарата нечеткой логики / Н. С. Хохлов, С. В. Канавин, А.

Е. Рыбокитов // Вестник Воронежского института МВД России, – 2018. – № 4. – С. 84–92.

108. Рыбокитов А. Е. Логико-лингвистическая нечеткая модель для оценки рисков нарушения информационной безопасности в самоорганизующихся сетях связи и управление ими. / Н. С. Хохлов, С. В. Канавин, А. Е. Рыбокитов // Вестник Воронежского института МВД России. – Воронеж: Воронежский институт МВД России, – 2019. – № 2. – С. 144–154.

109. Khokhlov N. Modeling Information Security Infringements in Mobile Self Organizing Network of Communication Using Fuzzy Logic and Theory of Graphs Bulletin of the Lipetsk State Technical University / N. Khokhlov, S. Kanavin, A. Rybokitov // 1st International Conference on Control Systems, Mathematical Modelling, Automation and Energy Efficiency (SUMMA). – Lipetsk, 2019. – p. 407–410. – DOI: 10.1109/SUMMA48161.2019.8947572.

110. Хохлов Н. С. Особенности построения мобильных радиосетей специального назначения с использованием технологии самоорганизации сети / Н. С. Хохлов, С. В. Канавин, С. Н. Ляшенко // Охрана, безопасность, связь 2017. – Воронеж : Воронежский институт МВД России, 2018. – Т. 2. №3 (3). – С. 81–86.

111. Хохлов Н. С. Методы управления рисками в беспроводных мобильных сетях. Общественная безопасность, законность и правопорядок в III тысячелетии / Н. С. Хохлов, С. В. Канавин, А. Е. Рыбокитов. – Воронеж : Воронежский институт МВД России, 2018. – Т.4. – С. 255–259.

112. Хохлов Н. С. Анализ рисков в управлении информационной безопасностью самоорганизующихся мобильных беспроводных сетей специального назначения. / Н. С. Хохлов, С. В. Канавин, А. Е. Рыбокитов // Охрана, безопасность, связь 2017. – Воронеж : Воронежский институт МВД России, 2018. – Т. 2. – № 3 (3). – С. 109–113.

113. Дмитриев А. С. Динамический хаос: новые носители информации для систем связи / А. С. Дмитриев, А. И. Панас. – Москва : Издательство Физико-математической литературы, 2002. – 252 с.

Научное издание

Хохлов Николай Степанович,
доктор технических наук, профессор;
Бокова Оксана Игоревна,
доктор технических наук, профессор;
Канавин Сергей Владимирович,
кандидат технических наук;
Гилев Игорь Владимирович

МЕТОДЫ И МОДЕЛИ ФОРМИРОВАНИЯ КОМПЛЕКСА СРЕДСТВ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕТЯХ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Монография

Редактор Н. Ф. Палихова
Компьютерная верстка С. В. Канавин

Подписано в печать 08.12.2020. Формат 60×84 $^{1}/_{16}$
Усл. печ. л. 10,23
Бумага офсетная. Гарнитура Таймс Новая. Печать офсетная.
Тираж 50 экз. Заказ № 201.

Воронежский институт МВД России
394065, Воронеж, просп. Патриотов, 53

Типография Воронежского института МВД России
394065, Воронеж, просп. Патриотов, 53

176