Макаренко С.И.

Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки

Монография

С.И. Макаренко

Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки

Монография

Санкт-Петербург
Наукоемкие технологии
2020

УДК 623.61
ББК 68.517
М15

Рецензенты:

Боговик Александр Владимирович, кандидат технических наук, профессор;
Гречишников Евгений Владимирович, доктор технических наук, профессор;
Михайлов Роман Леонидович, кандидат технических наук;
Финько Олег Анатольевич, доктор технических наук, профессор;
Цимбал Владимир Анатольевич, доктор технических наук, профессор.

М15 **Макаренко С.И.**
Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки. Монография. – СПб.: Наукоемкие технологии, 2020. – 337 с.

ISBN 978-5-6044429-5-1

В монографии представлены описательные и формальные модели системы связи специального назначения, функционирующей в условиях дестабилизирующих воздействий и ведения разведки. Данные модели учитывают современное состояние и тенденции развития технологий связи, средств вооружения и способов их применения. В качестве дестабилизирующих воздействий рассмотрены воздействия на систему связи со стороны средств физического (огневого) поражения, средств радиоэлектронного подавления, средств функционального поражения электромагнитным излучением и способов информационно-технического воздействия. В качестве средств разведки рассмотрены средства радио- и радиотехнической, оптико-электронной, компьютерной разведок. Отличительной особенностью разработанных формальных моделей является формализация процесса взаимодействия системы связи, системы дестабилизирующего воздействия и системы разведки в виде информационного конфликта.

Материалы работы предназначены для научных сотрудников, соискателей ученых степеней, военных и технических специалистов, занимающихся вопросами исследования устойчивости, живучести и помехозащищенности систем специальной связи.

Отдельные результаты, представленные в данной монографии, получены в рамках госбюджетной темы НИР СПИИРАН № 0073-2019-0004.

УДК 623.61
ББК 68.517

Напечатано с оригинал-макета, подготовленного автором.

ISBN 978-5-6044429-5-1

© Макаренко С.И., 2020.
© СПб ФИЦ РАН; СПбГЭТУ «ЛЭТИ», 2020.
© Издательство «Наукоемкие технологии», 2020.

С чувством глубокой благодарности посвящаю свою работу моим учителям:

учителю математики гимназии № 25
г. Ставрополя
Юлии Марковне Кудриной;

кандидату технических наук доценту
Александру Васильевичу Кихтенко;

кандидату технических наук профессору
Анатолию Вячеславовичу Баженову;

доктору технических наук профессору
Владимиру Ильичу Владимирову;

доктору технических наук профессору
Александру Григорьевичу Ломако;

доктору военных наук профессору
Юрию Ивановичу Стародубцеву;

доктору технических наук профессору
Валерию Игоревичу Курносову.

С.И. Макаренко

Оглавление

ВВЕДЕНИЕ 10

1. ОПИСАТЕЛЬНАЯ МОДЕЛЬ СИСТЕМЫ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ 20

1.1. Система связи специального назначения: определение, состав, требования 21

1.1.1. Основные термины и определения в области систем связи 21

1.1.2. Характеристика системы связи специального назначения как организационно-технической системы 23

1.1.3. Состав и структура системы связи специального назначения 24

1.1.4. Основные требования, предъявляемые к системе связи специального назначения 27

1.2. Основные тенденции развития систем связи специального назначения на современном этапе 32

1.2.1. Многоэшелонированное построение систем связи специального назначения 33

1.2.2. Использование в системах связи специального назначения канальных и сетевых ресурсов, арендуемых у коммерческих операторов связи 35

1.2.3. Использование в системах связи специального назначения технологий коммутации пакетов и коммерческих протоколов связи 37

1.2.4. Построение систем связи специального назначения в соответствии с концепцией NGN 40

1.2.5. Переход от систем связи к инфокоммуникационным системам специального назначения 47

1.3. Основные протоколы и технологии системы связи специального назначения 50

1.3.1. Базовые технологии физического и канального уровня 51

1.3.2. Базовые протоколы технологии IP 53

1.3.3. Протоколы маршрутизации 54

1.3.4. Протоколы групповой пересылки данных 55

1.3.5. Протоколы повышения устойчивости маршрутизации и доставки пакетов 56

1.3.6. Протоколы и технологии обеспечения качества обслуживания 56

1.3.7. Протоколы безопасности 59

1.3.8. Межсистемные протоколы и интерфейсы 60

1.4. Проблемные вопросы обеспечения устойчивости систем связи специального назначения на современном этапе их развития 63

1.4.1. Проблемные вопросы, обусловленные переходом систем связи специального назначения от технологий коммутации каналов к технологиям коммутации пакетов 64

1.4.2. Проблемные вопросы, обусловленные использованием в системах связи специального назначения канальных и сетевых ресурсов, арендуемых у коммерческих операторов связи 66

1.4.3. Проблемные вопросы, обусловленные построением систем связи специального назначения в соответствии с концепцией NGN 68

1.4.4. Проблемные вопросы управления системой связи специального назначения, построенной в соответствии с концепцией NGN 69

Выводы по первой главе 72

2. ОПИСАТЕЛЬНАЯ МОДЕЛЬ СИСТЕМ И СРЕДСТВ ДЕСТАБИЛИЗИРУЮЩИХ ВОЗДЕЙСТВИЙ 73

2.1. Общие подходы к применению дестабилизирующих воздействий на системы связи в современных вооруженных конфликтах 74

2.2. Описательная модель систем и средств физического поражения 76

2.2.1. Высокоточное оружие 76

2.2.2. Самонаводящееся на излучение оружие 80

2.2.3. Оружие на новых физических принципах 81

2.2.3.1. Гиперзвуковые средства поражения 81

2.2.3.2. Средства кинетического поражения (рельсовые пушки) 82

2.3. Описательная модель систем и средств радиоэлектронной борьбы 84

2.3.1. Средства радиоэлектронного подавления 88

2.3.1.1. Средства радиоэлектронного подавления воздушного базирования 89

2.3.1.2. Средства радиоэлектронного подавления наземного базирования 91

2.3.2. Средства функционального поражения на основе мощного СВЧ электромагнитного излучения 93

2.3.3. Средства функционального поражения на основе лазерного излучения 100

2.3.4. Средства функционального поражения на основе преднамеренного силового электромагнитного воздействия 101

2.4. Описательная модель средств и способов информационно-технических воздействий 105
2.4.1. Общая классификация информационно-технических воздействий и средств их реализации 105
2.4.2. Оборонительные информационно-технические воздействия 110
2.4.3. Обеспечивающие информационно-технические воздействия 111
2.4.4. Атакующие информационно-технические воздействия 111
2.4.4.1. Классификация атакующих информационно-технических воздействий 112
2.4.4.2. Удаленные сетевые атаки 114
2.4.4.3. Компьютерные вирусы 116
2.4.4.4. Программные закладки 117
2.4.4.5. Аппаратные закладки 118
Выводы по второй главе 120
3. ОПИСАТЕЛЬНАЯ МОДЕЛЬ СИСТЕМ И СРЕДСТВ РАЗВЕДКИ 121
3.1. Общие подходы к разведке систем связи специального назначения 121
3.2. Общие сведения о технической разведке 123
3.3. Описательная модель систем и средств радио- и радиотехнической разведки 125
3.3.1. Средства космического базирования 127
3.3.2. Средства воздушного базирования 127
3.3.3. Средства наземного базирования 129
3.4. Описательная модель систем и средств оптико-электронной разведки 130
3.4.1. Средства космического базирования 131
3.4.2. Средства воздушного базирования 131
3.5. Описательная модель средств и способов компьютерной разведки 131
3.5.1. Средства и способы компьютерной разведки 131
3.5.2. Разведка по открытым источникам 135
Выводы по третьей главе 137
4. КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ СИСТЕМЫ СВЯЗИ В УСЛОВИЯХ ДЕСТАБИЛИЗИРУЮЩИХ ВОЗДЕЙСТВИЙ И ВЕДЕНИЯ РАЗВЕДКИ 139
4.1. Общие подходы к представлению системы связи в условиях дестабилизирующих воздействий и ведения разведки в виде информационного конфликта 139

4.2. Описание условий информационного конфликта 141
4.3. Постановка задачи на моделирование 144
4.4. Схема концептуальной модели 148
4.5. Формализация основных аспектов, определяющих выигрыш в информационном конфликте 153
4.6. Способы достижения выигрыша в многоэтапном информационном конфликте 154
4.7. Эффективность управления организационно-технической системой в условиях информационного конфликта 158
4.7.1. Управление организационно-технической системой в условиях информационного конфликта 158
4.7.2. Многоуровневая модель управления организационно-технической системой в условиях информационного конфликта 161
4.7.3. Понятие информационного ущерба 163
4.8. Актуальные направления совершенствования концептуальной модели 165
4.8.1. Модель информационного конфликта между сторонами, состоящими из систем управления и связи, системы разведки и дестабилизирующих воздействий 165
4.8.2. Модель информационного конфликта с координацией конфликтующих систем 167
4.8.3. Модель информационного конфликта в глобальном инфокоммуникационном пространстве с учетом возможностей захвата информационных ресурсов и подыгрыша среды функционирования 168
4.8.4. Модель информационного конфликта с учетом многоуровневого построения системы связи 170
Выводы по четвертой главе 171
5. ДИНАМИЧЕСКАЯ МНОГОУРОВНЕВАЯ МОДЕЛЬ СИСТЕМЫ СВЯЗИ В УСЛОВИЯХ ДЕСТАБИЛИЗИРУЮЩИХ ВОЗДЕЙСТВИЙ И ВЕДЕНИЯ РАЗВЕДКИ 173
5.1. Постановка задачи на моделирование 173
5.2. Динамическая модель протокола системы связи 178
5.2.1. Схема модели 179
5.2.2. Формализация процесса функционирования протокола 181
5.2.3. Формализация критерия эффективного функционирования протокола 183

5.2.4. Формализация канала наблюдения протокола со стороны системы управления связью 184
5.2.5. Формализация канала управления протоколом со стороны системы управления связью 186
5.2.6. Формализация канала разведки протокола со стороны системы дестабилизирующих воздействий 189
5.2.7. Формализация канала воздействия на протокол со стороны системы дестабилизирующих воздействий 190
5.2.8. Итоговые выводы 195
5.3. Динамическая многоуровневая модель системы связи 196
5.3.1. Схема модели 196
5.3.2. Формализация пространственно-распределенной структуры системы связи 201
5.3.3. Формализация процесса функционирования системы связи 202
5.3.4. Формализация показателей качества функционирования системы связи 202
5.3.5. Формализация каналов наблюдения и разведки 207
5.3.6. Формализация системы управления связью и системы дестабилизирующих воздействий 207
5.3.7. Формализация особенностей управления системой связи и воздействия на нее как на многоуровневую систему 208
5.3.8. Итоговые выводы 216
Выводы по пятой главе 216
6. ТОПОЛОГИЧЕСКАЯ МОДЕЛЬ СИСТЕМЫ СВЯЗИ В УСЛОВИЯХ ДЕСТАБИЛИЗИРУЮЩИХ ВОЗДЕЙСТВИЙ И ВЕДЕНИЯ РАЗВЕДКИ 217
6.1. Анализ понятия устойчивости системы связи 217
6.1.1. Системный подход к определению понятия устойчивость 217
6.1.2. Понятие устойчивости, учитывающее особенности функционирования системы связи и дестабилизирующие воздействия на нее 219
6.2. Постановка задачи на моделирование 221
6.3. Обоснование и формализация показателя устойчивости системы связи взаимосвязанного с показателями связности в теории графов 225
6.4. Формализация структурных параметров устойчивости системы связи с учетом дестабилизирующих воздействий различного типа на ее отдельные элементы 230
6.5. Формализация структурных параметров устойчивости системы связи с учетом ведения разведки против ее отдельных элементов 232

6.6. Формализация структурных параметров устойчивости системы связи с учетом требований к качеству обслуживания трафика 236
6.7. Формализация временных параметров устойчивости системы связи с учетом длительности процессов восстановления связи 237
6.8. Итоговая схема оценивания устойчивости на основе топологической модели системы связи 238
Выводы по шестой главе 240
7. ИГРОВАЯ МОДЕЛЬ СИСТЕМЫ СВЯЗИ В УСЛОВИЯХ ДЕСТАБИЛИЗИРУЮЩИХ ВОЗДЕЙСТВИЙ И ВЕДЕНИЯ РАЗВЕДКИ 241
7.1. Постановка задачи на моделирование 241
7.2. Формализация структур системы связи и системы дестабилизирующих воздействий 243
7.3. Формализация показателя качества системы связи 244
7.4. Формализация процесса взаимодействия системы связи и системы дестабилизирующих воздействий в виде игры 245
7.5. Формализация многоэтапного игрового информационного конфликта системы связи 249
7.6. Формализация процесса принятия решений в многоэтапном игровом информационном конфликте 250
Выводы по седьмой главе 254
ЗАКЛЮЧЕНИЕ 255
СПИСОК СОКРАЩЕНИЙ 256
СПИСОК ИСПОЛЬЗУЕМЫХ ОБОЗНАЧЕНИЙ 265
Обозначения, используемые в 4-ой главе 265
Обозначения, используемые в 5-ой главе 265
Обозначения, используемые в 6-ой главе 274
Обозначения, используемые в 7-ой главе 277
ГЛОССАРИЙ ТЕРМИНОВ И ОПРЕДЕЛЕНИЙ 279
ЛИТЕРАТУРА 306

Введение

«Связь – она как воздух. Пока она есть, это воспринимается как само собой разумеющейся, но когда она пропадет, процессы управления стремительно погружаются в пучину хаоса, а командиры становятся бессильными наблюдателями, обреченными безмолвно созерцать свой неминуемо приближающийся бесславный конец…»

Из лекции о роли связи в управлении войсками.

Рубеж XX – XXI веков ознаменовался информационно-технической революцией, которая характеризуется факторами всемирного доступа к глобальному информационному пространству и широким распространением высокопроизводительных средств передачи информации. Достижения информационно-технической революции были использованы для создания новых технологий, внедрение которых позволило в кратчайшие сроки развернуть по всему миру глобальную информационную инфраструктуру, представляющую потребителям принципиально новые сервисы по передаче и обработке информации. Указанные положительные тенденции характерны и для систем связи специального назначения, составляющих технологическую основу систем государственного и военного управления. В этих системах связи с середины 90-ых годов XX века наблюдается устойчивая тенденция к заимствованию коммерческих технологических решений и даже целых стеков протоколов из «гражданской» сферы. Вместе с тем, данные коммерческие технологии не в полной мере отвечают потребностям систем связи специального назначения. Несмотря на то, что такое заимствование действительно обеспечивает существенный прирост пропускной способности сетей и своевременности передачи информационных потоков, а также и расширение диапазона предоставляемых связных услуг, итоговая устойчивость функционирования как отдельных коммерческих технологий, так и всей системы связи, построенной на ее основе, вызывает сомнения.

Информационно-техническая революция привела не только к быстрому развитию систем связи, подобное революционное развитие произошло и в средствах разведки и нападения, ориентированных на нарушение устойчивости систем связи специального назначения. Если ранее в качестве основных средств физического поражения узлов связи рассматривались, прежде всего, огневые средства ракетных войск и артиллерии, а в качестве средств дестабилизирующего воздействия на линии связи – средства радиоэлектронного подавления (РЭП), то с начала XXI века ситуация изменилась. Опыт военных конфликтов показывает, что основным средством поражения в современной войне является высокоточное оружие (ВТО). Именно за счет использования ВТО в ходе нанесения глобального удара в первые минуты начала войны уничтожается до 70-80% инфраструктуры систем государственного и военного управления,

в том числе и объектов систем связи. Традиционными средствами ВТО являются крылатые ракеты воздушного и морского базирования, а также управляемые авиационные бомбы. Вместе с тем, уже сейчас на вооружение поступают принципиально новые средства ВТО – во-первых, гиперзвуковые, а во-вторых, оснащенные боевыми частями, основанными на функциональном поражении электромагнитным излучением (ФП ЭМИ). В области РЭП развитые в военном отношении государства переходят к широкому использованию интегрированных наземно-воздушных территориально-распределенных комплексов РЭП. Отдельно необходимо отметить революционный рост угроз для элементов системы связи со стороны средств информационно-технического воздействия (ИТВ), характеризующихся различными способами их применения. С начала 2000-ых годов информационное пространство стало рассматриваться как отдельная сфера ведения военного противоборства, а осознание важности и значимости ИТВ для борьбы с системами государственного и военного управления, в том числе, путем воздействия на их подсистемы связи, привело к созданию в ведущих технологически развитых странах отдельного рода войск – сил информационных операций, называемых также «кибервойсками».

Аналогичные кардинальные изменения происходят и в средствах разведки, ориентированных на вскрытие параметров системы связи и семантический доступ к передаваемой информации. Если ранее основными средствами разведки систем связи были средства радио- и радиотехнической разведки (РРТР) сухопутных войск и флота, то с начала XXI века ситуация радикально изменилась. При решении задач разведки все большую роль играют средства РРТР воздушного базирования, увеличилась угроза вскрытия местоположения узлов связи средствами воздушной оптико-электронной (ОЭР) и радиолокационной разведки (РЛР) за счет использования интегрированных комплексов мониторинга, размещаемых на беспилотных летательных аппаратах (БПЛА). Существенно возросли возможности космической разведки. Так, современные космические средства РРТР и ОЭР позволяют осуществлять глобальный мониторинг источников радиоизлучения (ИРИ) на всей поверхности Земли, вскрывать режимы работы средств связи, уточнять местоположение и принадлежность пунктов управления (ПУ) и узлов связи в масштабе времени 1,5-2 ч. С середины 1990-ых годов активно развиваются средства и способы компьютерной разведки. По оценкам специалистов, на долю компьютерной разведки сегодня приходится до половины всех разведывательных данных, добываемых о структуре, режимах работы и тенденциях развития систем связи, и эта доля продолжает расти. Рост возможностей компьютерной разведки обусловлен, во-первых, широким распространением сетевых технологий, объединяющих различные силы и средства в единое информационное пространство, в котором функционируют системы военного и государственного управления, а, во-вторых, возможностями компьютерной разведки по ведению глобального мониторинга открытых источников, доступных через сеть Интернет, а также реализация на основе современных интеллектуальных методов обработки «больших данных» процедур комплексирования (формирования) оперативно ценной информации о средствах связи, их местоположении, обслуживающем персонале и т.д. Дополни-

тельным фактором, существенно повышающим эффективность разведывательных мероприятий, является создание единых комплексов сбора и обработки разведывательной информации, например, таких как DCGS (Distributed Common Ground System – автоматизированная система сбора, обработки и распределения разведывательной информации), что позволяет комплексировать информацию от различных источников и формировать более полную и достоверную информацию о состоянии систем связи, местоположении ее объектов и режимах работы.

Целью настоящей работы является, во-первых, формирование новых описательных моделей системы связи специального назначения, систем дестабилизирующего воздействия и разведки, которые бы учитывали их современное состояние и тенденции развития на ближайшую перспективу, а, во-вторых, разработка формальных моделей системы связи, функционирующей в условиях дестабилизирующих воздействий и ведения разведки. Предполагается, что вышеуказанные модели будут использованы научными работниками и разработчиками для формирования новых подходов, способов и технических решений, направленных на повышение устойчивости систем связи специального назначения.

В основу представленных в монографии формальных моделей системы связи положено развитие известных фундаментальных работ П.Н. Барашкова, А.П. Родимова, К.А. Ткаченко, А.М. Чуднова [1], А.В. Боговика, В.В. Игнатова [2, 76], А.В. Паршуткина [3, 4], В.И. Владимирова, И.В. Владимирова [5, 259], Ю.Л. Козирацкого, С.А. Будникова [7], В.Г. Радзиевского, А.А. Сироты [94, 204], Ю.И. Стародубцева [193-195], а также обобщение ранее опубликованных работ автора, основными из которых являются [8-10, 17-19, 166, 192, 408-410, 412]. Отличительной особенностью авторского подхода к разработке формальных моделей является формализация процесса взаимодействия системы связи, системы дестабилизирующего воздействия и системы разведки в виде информационного конфликта. Именно такой подход к формализации моделей системы связи отличает данную монографию от множества других работ, в которых воздействия на систему связи рассматриваются как некие постоянно действующие факторы, снижающие ее устойчивость, живучесть или помехозащищенность, но не учитывающие смену стратегий разведки, нападения и защиты в процессе конфликтного взаимодействия соответствующих систем.

В основу представленных описательных моделей систем и средств дестабилизирующих воздействий, а также систем и средств разведки положены материалы ранее изданных монографий автора [9, 10], посвященных тенденциям развития стратегии военного противоборства, вооружения и военной техники.

В 1-ой главе монографии «Описательная модель системы связи специального назначения» введены основные термины и определения в области специальной связи, дана характеристика сети связи как организационно-технической системы, представлены основные требования, предъявляемые к специальной системе связи. Проведен анализ основных тенденций развития систем связи специального назначения. Показано, что к основным тенденциям относятся: переход к многоэшелонированному построению; широкое использование в

специальных системах связи канальных и сетевых ресурсов, арендуемых у коммерческих операторов связи; массовое использование технологий коммутации пакетов и коммерческих протоколов связи. Представлена описательная характеристика основных протоколов и технологий, используемых в системах связи специального назначения. Проведен анализ проблемных вопросов обеспечения устойчивости систем связи специального назначения на современном этапе их развития. В основу описательной модели, представленной в 1-ой главе, положен материал предыдущих работ автора [10, 18, 19], а также на системное обобщение научных работ [1, 2 21-55, 61, 396, 397], справочных и энциклопедических изданий [56-58, 335, 381, 383, 398].

Во 2-ой главе монографии «Описательная модель систем и средств дестабилизирующих воздействий» представлены общие подходы к дестабилизирующему воздействию на системы связи в современных военных конфликтах. В данной главе представлены описательные модели систем и средств физического поражения, радиоэлектронной борьбы (РЭБ) и ИТВ. В описательной модели систем и средств физического поражения сформированы описания тактико-технических характеристик (ТТХ) типовых средств ВТО, самонаводящегося на излучение оружия (СНИО), перспективных образцов оружия на новых физических принципах – гиперзвукового ВТО и средств кинетического поражения. В описательной модели систем и средств РЭП сформированы описания ТТХ типовых средств наземного и авиационного базирования, средств функционального поражения на основе мощного СВЧ электромагнитного излучения, средств функционального поражения лазерным излучением, средств преднамеренного силового электромагнитного воздействия. В описательной модели средств и способов ИТВ представлена общая классификация ИТВ и средств их реализации, кратко рассмотрены оборонительные и обеспечивающие ИТВ, а также более подробно – атакующие ИТВ: удаленные сетевые атаки, компьютерные вирусы, программные и аппаратные закладки. В основу описательной модели, представленной во 2-ой главе, положен материал ранее изданной монографии автора [9].

В 3-ей главе монографии «Описательная модель систем и средств разведки» представлены общие подходы к разведке систем связи специального назначения. Приведены общие сведения о технической разведке. Представлены описательные модели средств РРТР, ОЭР и компьютерной разведки. В описательной модели средств РРТР сформированы описания ТТХ типовых средств РРТР наземного, воздушного и космического базирования. В описательной модели средств ОЭР сформированы описания ТТХ типовых средств ОЭР воздушного и космического базирования. В описательной модели компьютерной разведки сформированы описания традиционных средств и способов компьютерной разведки, а также проведен анализ возможностей ведения разведки по открытым источникам в сети Интернет за счет использования методов интеллектуальной обработки «больших данных». В основу описательной модели, представленной в 3-ей главе, положен материал ранее изданной монографии автора [9].

В 4-ой главе монографии «Концептуальная модель системы связи в условиях дестабилизирующих воздействий и ведения разведки» сформированы об-

щие подходы к формальному представлению процесса функционирования системы связи в условиях разведки и дестабилизирующих воздействий в виде информационного конфликта организационно-технических систем. Описаны типовые условия информационного конфликта. Представлена обобщенная схема функционирования системы связи в условиях информационного конфликта с системами разведки и дестабилизирующего воздействия. Формализованы основные аспекты, определяющие выигрыш системы связи в информационном конфликте, представлены типовые способы достижения выигрыша в многоэтапном информационном конфликте. Рассмотрена эффективность управления организационно-технической системой, в состав которой входит система связи в условиях информационного конфликта. Представлены актуальные направления совершенствования концептуальной модели. В основу концептуальной модели, представленной в 4-ой главе, положено развитие модели из работы В.И. Владимирова, И.В. Владимирова [5], ранее представленное автором в работах [408, 409], а в основу анализа направлений развития этой модели – работы А.В. Паршуткина [3, 4], В.Г. Радзиевского, А.А. Сироты [94, 204], Ю.Л. Козирацкого, С.А. Будникова [7], Ю.И. Стародубцева [193-195], Р.Л. Михайлова [198, 205-209]. Представленная в 4-ой главе модель ранее была опубликована в цикле работ автора [408, 409, 412].

В 5-ой главе монографии «Динамическая многоуровневая модель системы связи в условиях дестабилизирующих воздействий и ведения разведки» представлены: динамическая модель протокола, как основного функционального элемента системы связи; динамическая многоуровневая модель системы связи, состоящая из совокупности отдельных протоколов, декомпозированных по уровням эталонной модели OSI (Open Systems Interconnect). В данных моделях протокол и система связи рассмотрены как объекты управления со стороны двух систем управления, имеющих антагонистические цели функционирования, – системы управления связью и системы управления дестабилизирующими воздействиями. В этих моделях формализованы: входные, внутренние, выходные параметры протокола и системы связи, а также их ресурсы; математические отображения, задающие процесс их функционирования; каналы наблюдения и управления со стороны системы управления связью; каналы разведки и дестабилизирующих воздействий; показатели и критерии качества функционирования отдельного протокола и системы связи в целом. Такое формализованное описание позволяет рассмотреть информационный конфликт, который происходит и развивается в системе связи на всех семи уровнях модели OSI. При этом, в таком рассмотрении информационного конфликта, учитывается тесная функциональная взаимосвязь протоколов между собой, как по горизонтали – в соответствии с задачами отдельного уровня OSI, так и по вертикали – в соответствии с задачами межуровневого взаимодействия. Представленная в данной главе модель системы связи не только позволяет описать противоборство двух сторон – системы связи и системы дестабилизирующих воздействий, но и выявить: внутренние локальные конфликты за ресурсы между различными протоколами внутри системы связи; необходимость координации систем управления связью на различных уровнях OSI; возможности нападающей стороны реализо-

вывать новые типы бескомпроматных воздействий на систему связи основанных на преднамеренном формировании и поддержании в ней локальных конфликтов, нестационарных и переходных процессов, а также неэффективных условий функционирования. В основу динамической многоуровневой модели, представленной в 5-ой главе, положено развитие модели из работы П.Н. Барашкова, А.П. Родимова, К.А. Ткаченко, А.М. Чуднова [1], на основе подхода, предложенного в работах А.В. Паршуткина [3, 4]. При этом в качестве работ, которые частично послужили прототипами общего подхода к моделированию иерархического построения систем связи, относятся работы П.А. Будко [22], К.Е. Легкова [36], И.М. Гуревича [212-216], А.А. Вакуленко, В.И. Шевчука [217], Ю.И. Маевского [218], В.В. Поповского, А.В. Лемешко, О.Ю. Евсеевой [219]. Представленная в 5-ой главе модель ранее была опубликована в работе автора [8].

В 6-ой главе монографии «Топологическая модель системы связи в условиях дестабилизирующих воздействий и ведения разведки» обосновано, что основным свойством системы связи, характеризующим ее способность противостоять дестабилизирующим воздействиям и разведке, является свойство устойчивости. Рассмотрены понятия функциональной и структурной устойчивости системы связи. Показано, что в качестве интегрального показателя устойчивости системы связи можно использовать среднесетевую вероятность устойчивости информационного направления связи (ИНС). Показатель «вероятность устойчивости ИНС» является сверткой структурных параметров устойчивости – показателя структурной связности ИНС, а также временных параметров – коэффициента готовности ИНС. Предложены варианты формализации структурных параметров устойчивости ИНС с учетом различных совокупностей факторов: с учетом дестабилизирующих воздействий различного типа на ее отдельные элементы; с учетом ведения разведки против ее отдельных элементов; с учетом требований к качеству обслуживания трафика в ИНС. Предложен вариант формализации временных параметров устойчивости ИНС, с учетом с длительности процессов восстановления связи в ИНС. Сформирована итоговая схема оценивания устойчивости в топологической модели системы связи. В основу топологической модели, представленной в 6-ой главе, положено развитие подходов к оценке устойчивости системы связи, предложенных в работах А.В. Боговика, В.В. Игнатова [2] и А.Н. Назарова, К.И. Сычева [27]. Представленная в 6-ой главе топологическая модель ранее была опубликована в работе автора [166].

В 7-ой главе монографии «Игровая модель системы связи в условиях дестабилизирующих воздействий и ведения разведки» стратегии нападения и защиты, соответственно системы связи и системы дестабилизирующих воздействий, состоящей из подсистем разведки и нападения, представлены в форме информационного конфликта в формализме теории игр. Показано, что каждая конкретная стратегия нападения и стратегия защиты соответствуют определенной структуре системы связи, а также варианту воздействия средств разведки и нападения. Обосновано, что на основе игры с прямыми или смешанными стратегиями возможно выбрать наиболее вероятные варианты дестабилизирующих

воздействий, а также рациональную структуру системы связи в информационном конфликте. Развивая игровую модель в направлении анализа многоэтапного информационного конфликта, предложена формализация принятия решений противоборствующими сторонами при выборе стратегий на каждом из этапов конфликта. Предложена формализация правила выбора стратегии защиты и соответствующей ей структуры системы связи в виде минимаксного критерия. Данный критерий позволяет осуществить поиск рациональной структуры системы связи как при оперативном (с учетом сложившейся ситуации на этом же этапе информационного конфликта), так и при превентивном (на следующем этапе информационного конфликта, с учетом прогнозируемой стратегии действий противника) принятии решений. Игровая модель ранее была опубликована в работе автора [410]. В основу этой игровой модели положено развитие модели, представленной в работе А.В. Боговика, В.В. Игнатова [2].

Монография не претендует на окончательную верность и полноту изложения всей затронутой проблематики. Данную работу стоит рассматривать, прежде всего, как развитие и дополнение к известным исследованиям процессов взаимодействия системы связи (как сложной информационной организационно-технической системы специального назначения) с системами разведки и дестабилизирующего воздействия, формализованных в виде информационного конфликта. К таким исследованиям стоит отнести работы П.Н. Барашкова, А.П. Родимова, К.А. Ткаченко, А.М. Чуднова [1], А.В. Боговика, В.В. Игнатова [2], А.В. Паршуткина [3, 4], В.И. Владимирова, И.В. Владимирова [5, 226, 259-282], Ю.Л. Козирацкого [7, 255-258], С.А. Будникова [7, 250-255], В.Г. Радзиевского [94, 204], А.А. Сироты [94, 204, 238-242], В.И. Борисова, В.М. Зинчука, А.Е. Лимарева [190, 191], Ю.И. Стародубцева [193-195], Р.Л. Михайлова [198, 205-209], А.Г. Алферова [230, 231], Н.Н. Толстых [230-234], И.О. Толстых [230-232], М.А. Стюгина [235-238], А.А. Бойко [243-250], С.А. Будникова [250-255], В.М. Шацких [260-262], М.А. Коцыняка, А.И. Осадчего, М.М. Коцыняка, О.С. Лауты, В.Е. Дементьева, Д.Ю. Васюкова [266], И.В. Дементьева, Д.Ю. Чаркина [267], Е.А. Жидко [268, 278], С.Н. Разинькова [268], А.В. Бобрусь [269, 270], Л.Е. Мистрова [271-274], Ю.С. Сербулова [273-275], Д.Н. Бирюкова, А.Г. Ломако [276-277], Г.А. Остапенко [282-290]. Также представленный в работе конфликтный подход может быть распространен и на другие исследования в области оценки устойчивости информационных систем, вообще, и систем связи, в частности. К таким исследованиям можно отнести работы А.А. Привалова [152, 291-298], И.И. Чукляева [279-281], М.М. Добрышина [299-307], Е.В. Гречишникова [302-326], Ю.И. Стародубцева [312-320], А.С. Белова [316-333], Р.В. Максимова [361-368], Ю.К. Язова [369-380], С.М. Одоевского, В.И. Калюки [396, 397], а также работы других ученых.

Материал монографии ориентирован на подготовленного читателя, имеющего базовые знания в области вооружения и военной техники, а также владеющего методами теории конфликтов, теории графов, теории игр и теории сложных систем. Работа может быть полезна техническим специалистам, научным работникам, соискателям ученой степени. Автор надеется, что его труд

найдет своего читателя, а для кого-то, возможно, окажется своеобразной отправной точкой в дальнейших исследованиях.

Благодарности

Автор выражает благодарность рецензентам: кандидату технических наук профессору А.В. Боговику, доктору технических наук профессору Е.В. Гречишникову, кандидату технических наук Р.Л. Михайлову, доктору технических наук профессору О.А. Финько, доктору технических наук профессору В.А. Цимбалу за поиск ошибок и неточностей при рецензировании монографии, за ценные предложения, которые способствовали значительному улучшению качества работы, ее полноты и ясности, а также ориентированности на широкого читателя. Также автор благодарит А.С. Мамончикову за кропотливый редакторский труд при подготовке рукописи к изданию.

Необходимо отметить, что на этапе подготовки рукописи, особенно ценными были замечания, высказанные доктором технических наук профессором А.М. Чудновым, а также поддержка данного направления исследований доктором технических наук профессором А.В. Паршуткиным.

Автор благодарит кандидата технических наук профессора А.В. Баженова, кандидата технических наук доцента А.В. Кихтенко, доктора технических наук профессора В.И. Владимирова, доктора технических наук профессора А.Г. Ломако, доктора военных наук профессора Ю.И. Стародубцева, доктора технических наук профессора В.И. Курносова за то, что именно они способствовали становлению автора как ученого, и я безмерно горжусь тем, что имел возможность работать рядом с такими людьми, и особенно – учиться у них.

Выражаю признательность моей супруге и детям за поддержку, понимание и интерес к моим исследованиям.

Многие из моих научных результатов рождались, развивались и корректировались в процессе их неоднократного обсуждения с ближнем научным кругом моих друзей и коллег – с кандидатом технических наук Р.Л. Михайловым, доктором технических наук доцентом Е.А. Новиковым, кандидатом технических наук В.М. Коровиным, доктором технических наук доцентом И.И. Чукляевым, кандидатом технических наук В.Е. Федосеевым. Большое Вам спасибо за многолетнюю дружбу и поддержку как меня, так и моих исследований!

Некоторые отдельные результаты, представленные в монографии, были получены в рамках диссертационных исследований автора на соискание ученой степени доктора технических наук. Автор выражает свою искреннюю благодарность всем тем специалистам, кто на протяжении многих лет помогал моим диссертационным исследованиям, давал ценные советы и оказывал методическую помощь, а особенно – доктору технических наук профессору В.И. Владимирову, доктору технических наук профессору Ю.Л. Козирацкому, кандидату технических наук доценту П.Р. Ляхову, кандидату технических наук доценту С.А. Панову, доктору технических наук доценту С.А. Будникову, доктору технических наук профессору Э.А. Кирсанову, кандидату технических наук доценту А.В. Родионову, доктору технических наук доценту Е.А. Новикову, кандидату технических наук Р.Л. Михайлову, кандидату технических наук К.В. Уша-

нёву, доктору технических наук профессору А.В. Паршуткину, кандидату технических наук доценту В.В. Вознюку, доктору технических наук профессору А.Г. Ломако, доктору технических наук профессору Ю.И. Рыжикову, доктору технических наук профессору А.Д. Хомоненко, доктору технических наук профессору В.А. Смагину, доктору военных наук доценту П.И. Антоновичу, доктору военных наук доценту Е.А. Дербину, доктору технических наук профессору С.Н. Гриняеву, доктору технических наук старшему научному сотруднику А.С. Маркову, доктору технических наук доценту И.И. Чукляеву, доктору технических наук профессору Ю.М. Перунову, доктору технических наук профессору М.Л. Артёмову, доктору технических наук профессору А.И. Куприянову, доктору технических наук профессору В.А. Цимбалу, доктору технических наук профессору В.П. Пашинцеву, доктору технических наук профессору Г.И. Линцу, доктору технических наук профессору Е.В. Гречишникову, доктору технических наук доценту С.С. Семенову, доктору технических наук профессору А.М. Чуднову, доктору технических наук профессору А.Н. Путилину, доктору технических наук профессору В.Г. Анисимову, доктору технических наук профессору И.В. Котенко, докторам технических наук профессорам П.Д. Зегжде и Д.П. Зегжде, доктору технических наук профессору О.А. Финько, доктору технических наук профессору С.М. Климову, доктору технических наук профессору С.А. Юдицкому, члену-корреспонденту РАН Д.А. Новикову. А также тем, кто содействовал в доведении моих многолетних диссертационные исследований до успешной защиты – доктору технических наук профессору А.С. Попову, доктору технических наук профессору В.И. Курносову, доктору военных наук профессору Ю.И. Стародубцеву, доктору технических наук профессору П.А. Будко, доктору технических наук профессору А.В. Кузичкину, доктору технических наук профессору С.А. Петренко, доктору технических наук профессору И.Б. Саенко. Именно этим людям я во многом обязан успешной подготовкой и защитой диссертации на соискание ученой степени доктора наук. Кроме того, считаю своей обязанностью выразить свое признание всем тем специалистам, которые нашли время на экспертный анализ результатов моей дисертации и подготовили положительные отзывы на нее, и в особенности: доктору технических наук профессору Ю.К. Язову, доктору технических наук профессору Б.Г. Тележному, доктору технических наук профессору В.В. Борисову, доктору технических наук профессору О.Н. Маслову, доктору технических наук профессору Т.Р. Газизову, доктору технических наук профессору А.Я. Олейникову, доктору технических наук старшему научному сотруднику А.С. Маркову, доктору технических наук профессору М.В. Буйневичу, доктору технических наук профессору А.А. Зацаринному, кандидату технических наук Е.В. Забегалину, доктору военных наук доценту П.Ю. Хахамову.

Плодотворные исследования в области устойчивости систем специальной связи стали возможными благодаря тем людям, которые помогали, поддерживали, направляли, критиковали и всячески способствовали автору в его исследованиях. Автор выражает благодарность за доброжелательную критику, научную и организационную поддержку, а также за плодотворное общение всем тем, с кем он обсуждал вопросы своих исследований на встречах, семинарах, кон-

ференциях, а также в процессе выполнения совместных НИОКР. Кроме того, автор считает своим долгом поблагодарить всех тех специалистов, которые внесли свой научный и исторический вклад в развитие теории устойчивости систем связи.

Особую признательность хочется выразить тем неординарным людям, с которыми автору посчастливилось совместно служить и работать: коллективу кафедры прикладной информатики и математики Ставропольского филиала МГГУ им М.А. Шолохова; коллективу кафедры эксплуатации и ремонта бортового авиационного радиоэлектронного оборудования (радионавигации и радиосвязи) Ставропольского ВВАИУ им. маршала авиации В.А. Судца; коллективу кафедры радионавигации и радиолокации ВУНЦ ВВС «ВВА им. проф. Н.Е. Жуковского и Ю.А. Гагарина»; коллективу кафедры сетей и систем связи космических комплексов ВКА им. А.Ф. Можайского; коллективам НТЦ-7 и НИО-77 в НИИ «Вектор»; коллективу НТЦ-21 в НИИ «Рубин»; коллективу Корпорации «Интел групп»; коллективу кафедры информационной безопасности СПбГЭТУ «ЛЭТИ» им. В.И. Ульянова (Ленина); коллективу кафедры информационных и вычислительных систем ПГУПС им. Императора Александра I; коллективам лаборатории проблем компьютерной безопасности, а также лаборатории информационных технологий в системном анализе и моделировании СПб ФИЦ РАН. Творческая атмосфера этих коллективов всегда способствовала плодотворной деятельности и определила области научных интересов и направления исследований автора.

Автор будет рад сотрудничеству в рассматриваемой области исследований, а также конструктивным замечаниям и предложениям. Замечания и предложения прошу направлять по адресу: mak-serg@yandex.ru.

С.И. Макаренко

1. Описательная модель системы связи специального назначения

В настоящее время стремительное технологическое развитие, а также внедрение в практику построения систем связи концепции сетей следующего поколения NGN (Next Generation Networks) и концепции глобальной информационной инфраструктуры GII (Global Information Infrastructure), создает предпосылки для коренного изменения архитектуры и принципов построения систем связи специального назначения (СС СН). Так, концепция NGN связана с конвергенцией сетей связи и расширением диапазона предоставляемых связных услуг, а концепция GII – с образованием единого информационного пространства, в котором услуги связи дополнены другими услугами обработки информации, такими как накопление, хранение, обработка и поиск необходимой информации. При этом отличительной особенностью СС СН является то, что, с одной стороны, они традиционно являются наиболее консервативными объектами в отрасли связи, а, с другой стороны, – они должны быть основаны на новейших достижениях этой отрасли, чтобы обеспечивать высокое качество обслуживания специальных абонентов.

Вопросам анализа функционирования СС СН посвящены работы: П.Н. Барашкова, А.П. Родимова, К.А. Ткаченко, А.М. Чуднова [1], А.В. Боговика [2, 54, 61, 76], В.В. Игнатова [2, 76], И.Н. Лялюка [23], П.А. Будко [22-25, 45], Г.И. Линца [26, 45], А.Н. Назарова, К.И. Сычева [27], А.Е. Давыдова [28-31, 335, 381, 398], А.Г. Ермяшина [32, 33], Г.В. Сызранцева [33, 34], В.Г. Иванова [35], К.Е. Легкова [36-42], А.Н. Буренина [40-42, 335], Е.Е. Исакова [43], Р.Л. Михайлова [44, 383], М.А. Шнепс-Шнеппе [46-50], Н.А. Соколова [51-53], В.И. Курнсосова [54, 335, 381, 398], С.П. Воробьева [335, 381, 398], И.Б. Паращука [54, 61], Б.С. Гольдштейна [52, 53], С.М. Одоевского [61, 396, 397], В.В. Ефимова [381, 398], Н.Н. Мошака [398], а также других ученых. Критический анализ проблемных вопросов, связанных с переходом СС СН на новые информационные технологии, представлен в работах М.А. Шнепс-Шнеппе [46-50], Н.А. Соколова [51], В.А. Нетеса [55].

Вместе с тем, в данных работах не в полной мере раскрыты эволюционные процессы развития современных СС СН, не сформулирована описательная модель используемых в СС СН современных протоколов и технологических решений.

В данном разделе представлен авторский вариант описательной модели СС СН, основанной, прежде всего, на предыдущих работах автора [18, 19], а также на системном обобщении вышеуказанных научных работ [1, 2 21-55, 61, 396, 397], материала справочных и энциклопедических изданий в области специальной связи [56-58, 335, 381, 383, 398].

Несмотря на то, что СС СН является системой, реализованной на всех семи уровнях модели OSI (Open System Interconnect), в дальнейшем, при рассмотрении СС СН, основной акцент будет сделан преимущественно на технологиях сетевого и транспортного уровня. Это обусловлено двумя причинами.

Во-первых, технологии физического и канального уровня в различных сетях весьма разнообразны, а их специфика, как правило, обусловлена историческими тенденциями построения тех или иных сетей связи. Поэтому отобразить их в полном объеме в рамках одной описательной модели представляется весьма затруднительным. Во-вторых, современный этап развития СС СН характеризуется процессами конвергенции отдельных сетей. При этом если для отдельных сетей связи, реализуемых в рамках канального уровня, уже существуют частные модели, то для СС СН как интегральной системы, объединяющей множество различных подсистем и подсетей связи, такая модель отсутствует.

1.1. Система связи специального назначения: определение, состав, требования

1.1.1. Основные термины и определения в области систем связи

Для конкретизации понятий, рассматриваемых в данной работе, введем базовые определения.

В настоящее время в нормативно-правовых документах введены следующие термины.

Сеть связи – технологическая система, включающая в себя средства и линии связи и предназначенная для электросвязи или почтовой связи [59].

Электросвязь – любое излучение, передача или прием знаков, сигналов, голосовой информации, письменного текста, изображений, звуков или сообщений любого рода по радиосистеме, проводной, оптической и другим электромагнитным системам [59].

Сеть электросвязи – сеть связи, обеспечивающая электросвязь при помощи электромагнитных систем. Сеть электросвязи состоит из сетей следующих категорий: сети 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. Таким образом, сеть электросвязи фактически представляет собой объединение отдельных категорий сетей, которые классифицируются по их предназначению [59].

Сеть связи специального назначения – сеть связи, предназначенная для нужд органов государственной власти, нужд обороны страны, безопасности государства и обеспечения правопорядка [59].

При этом для обеспечения функционирования сети связи специального назначения могут использоваться как ее собственные ресурсы, так и ресурсы сетей связи общего пользования.

Сеть связи общего пользования – комплекс взаимодействующих сетей связи, обеспечивающих электросвязь, в том числе – трансляцию телеканалов или радиоканалов, предназначенных для возмездного оказания услуг связи любому пользователю. При этом сети связи общего пользования могут иметь присоединение к аналогичным системам связи иностранных государств [59].

Сети связи включают в себя первичные и вторичные сети.

Первичная (*транспортная*) *сеть связи* – совокупность технических средств, комплексов, линий связи и обслуживающего персонала, обеспечивающая потребителей стандартными каналами (трактами) передачи первичных электрических сигналов. Основным видом сервиса, предоставляемого абонентам первичных сетей связи, являются типовые каналы и тракты [2].

Вторичная сеть связи (*сеть абонентского доступа*) – совокупность технических средств и связей между ними, обеспечивающая потребителей различными видами услуг по доставке, хранению и обработке информации. Основным видом сервиса, предоставляемого абонентам вторичных сетей, являются услуги по информационному обмену [2].

Выделенные сети – сети связи, которые организуются в интересах отдельных категорий должностных лиц, пунктов управления (ПУ) и специальных систем управления. К таким выделенным сетям, например, можно отнести сети навигации, государственного опознавания, системы телеметрии в системах технологического управления, сети правительственной связи и др.

Кроме того, в современных отечественных нормативных актах используется термин «информационно-телекоммуникационная сеть». Причем в подавляющем числе документов этот термин ассоциируется с сетью Интернет, а содержание этих документов, прежде всего, ориентировано на использование информационных ресурсов сети Интернет и, в основном, не касается ее технологических особенностей как сети электросвязи.

Информационно-телекоммуникационной сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники [60].

Как видно из вышеуказанных определений, существующие документы делают основной упор на сети, как физико-логические территориально-распределенные структуры, объединяющие узлы и каналы связи. Данный подход соответствует восприятию функций системы связи преимущественно на сетевом уровне, а когда речь идет об услугах связи – на прикладном уровне модели OSI. Трактовка понятия «система связи» является более широким и подразумевает включение в себя не только технических объектов и функций на всех 7-ми уровнях модели OSI, но и организационных структур, осуществляющих проектирование, развертывание, сопряжение со смежными системами (системами управления, навигации, единого времени и т.д.), а также эксплуатацию технических средств связи.

Таким образом, в самом общем, виде термин «система связи» может быть определен следующим образом.

Система связи (СС) – это совокупность распределенных в пространстве взаимосвязанных технических средств и обслуживающего персонала, выполняющих задачи по обеспечению информационного обмена.

Система связи специального назначения (СС СН) – это совокупность распределенных в пространстве взаимосвязанных технических средств и обслуживающего персонала, выполняющих задачи по обеспечению информационного обмена в системах государственного и военного управления, а также в системах управления обеспечением безопасности и правопорядка [2].

Система связи общего пользования (СС ОП) – совокупность распределенных в пространстве взаимосвязанных технических средств и обслуживающего персонала, выполняющих задачи по возмездному оказанию услуг связи любому пользователю.

С точки зрения теории систем СС может быть отнесена к типу ненаправленных управляемых человеко-машинных систем, которая, как правило, функционирует в интересах одной или нескольких систем управления [2].

По отношению к системам связи, довольно часто используют понятие «телекоммуникационная система», которое в большинстве случаев ассоциируется с отдельной первичной (транспортной) сетью, которая соответствует отдельной области маршрутизации в составе системы связи. Таким образом, можно утверждать, что телекоммуникационная система относится к системе связи, как частое к общему.

Телекоммуникационная система (ТКС) – это совокупность связанных линиями связи сетевых узлов, которая основана на единой транспортной технологии и эксплуатируется в соответствии с едиными принципами маршрутизации, адресации и управления, при этом в ее составе имеются граничные узлы, ответственные за допуск трафика в сеть или направление его в другие смежные телекоммуникационные системы.

1.1.2. Характеристика системы связи специального назначения как организационно-технической системы

Анализ особенностей построения и функционирования СС СН был проведен в работах А.В. Боговика, В.В. Игнатова [2], К.Е. Легкова, А.Н. Буренина [40, 41], А.Н. Соколова [51], М.А. Шнепс-Шнеппе [50], С.М. Одоевского [61], С.П. Воробьева, А.Е. Давыдова, В.В. Ефимова, В.И. Курносова [381, 355, 398]. В данном подразделе будут обобщены принципы построения СС СН и основные их особенности относительно СС ОП.

Задачей СС СН, в первую очередь, является доставка информации между распределенными в пространстве органами и пунктами системы управления – органами государственной власти, органами обороны страны, безопасности государства и обеспечения правопорядка.

Одним из основополагающих принципов исследования сложных организационно-технических систем (ОТС) является принцип декомпозиции, при котором исследуемая система разбивается на ряд более простых составляющих, преследующих локальные цели. При этом успешность решения общей задачи исследования, в существенной мере, зависит от того, насколько удачно были выбраны признаки, по которым осуществлена декомпозиция. При решении задач информационного обеспечения органов государственного и военного управления, органов обеспечения безопасности и правопорядка для СС СН такими признаками могут быть [2]:

- тип транспортных средств или протоколов, используемых для доставки информации;
- виды обеспечиваемого для абонентов сервиса и услуг связи;

- типы абонентов;
- способы предоставления абонентов сервиса и услуг связи.

Декомпозиция СС СН по некоторым из указанных признаков приведена на рис. 1.1.

При этом основу современных СС СН как управляемых целенаправленных систем, независимо от их типа и принадлежности, составляют отдельные сети связи (телекоммуникационные системы) и автоматизированные системы управления связью (АСУС).

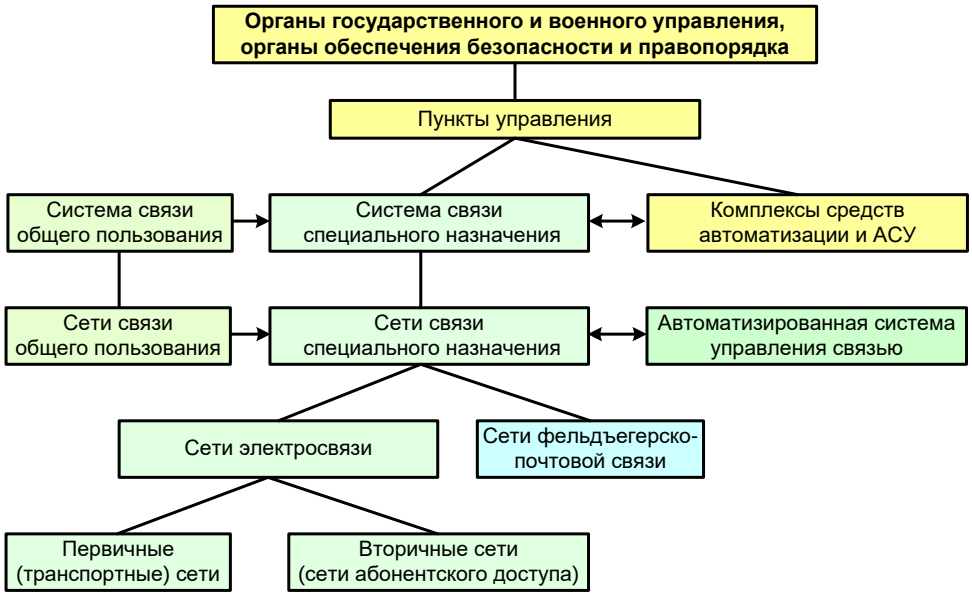

Рис. 1.1. Декомпозиция СС СН [2]

1.1.3. Состав и структура системы связи специального назначения

По транспортным средствам, используемым для доставки информации, в составе СС СН различают [2]:

- *сети фельдъегерско-почтовой связи*, в которых доставка информации (в виде карт, схем, посылок, бандеролей, писем и т.д.) осуществляется специальными курьерами (фельдъегерями) с помощью обычных транспортных средств;
- *сети электросвязи*, в которых доставка информации осуществляется с помощью электрических сигналов и электромагнитных волн.

Каналы и тракты транспортных сетей связи в современных СС СН создаются на базе линий и сетей различных родов связи, входящих в состав первичной (транспортной) сети. При этом под *родом связи* понимается классификационная группировка связи, выделенная по среде распространения сигналов или по применяемым средствам связи.

По видам обеспечиваемого для абонентов сервиса и услуг связи сети электросвязи обычно подразделяют на [2]:

- первичные (транспортные) сети связи;
- вторичные сети связи (сети абонентского доступа).

Классификация элементов сетей первичной и вторичной сетей СС СН представлена на рис. 1.2.

В составе первичных и вторичных сетей СС СН могут быть организованы *выделенные сети*.

Основой построения первичных (транспортных) сетей в составе СС СН в настоящее время являются [2, 13, 62, 381]:

- линии и сети радиосвязи;
- линии и сети спутниковой связи;
- волоконно-оптические линии связи;
- линии радиорелейной и тропосферной связи;
- кабельные линии электрической связи.

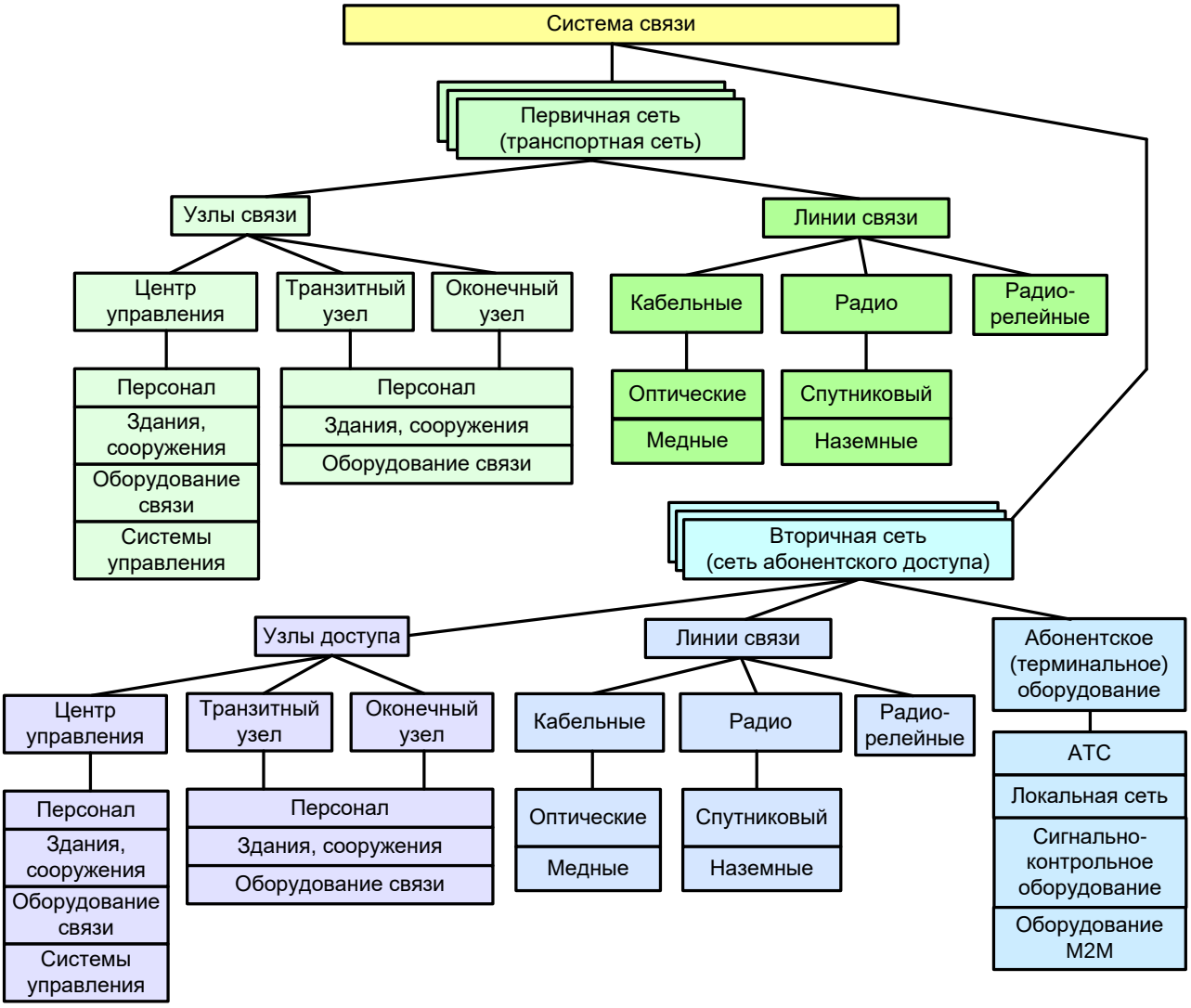

Рис. 1.2. Классификация элементов СС СН [63]

К основным технологиям первичных (транспортных) сетей в составе СС СН можно отнести [2, 13, 62, 381]:

- технологии коммутации каналов – PDH, SDH, OTH;
- технологии коммутации пакетов – IPv4, IPv6;
- технологии коммутации пакетов по виртуальным каналам – X.25, AX.25, Frame Relay, ATM, IP/MPLS, VPN и др.;

- технологии организации, управления и интеграции сетей связи – TMN, ASON/ASTN, NGN, GII и др.;
- специализированные технологии, разработанные для обеспечения связи в условиях преднамеренного воздействия дестабилизирующих факторов на СС СН.

Вторичные сети СС СН обычно подразделяли по видам предоставляемых ими услуг, однако в настоящее время такая классификация устарела.

В соответствии с современными взглядами, вторичные сети можно подразделить по типу [62]:

- локальные сети;
- сети коллективного доступа;
- цифровые линии абонентского доступа;
- оптические линии абонентского доступа;
- сети мобильной или транкинговой связи;
- сети радиодоступа.

В основу более подробной классификации вторичных сетей (сетей абонентского доступа) может быть положена используемая в ней базовая технология сети – рис. 1.3.

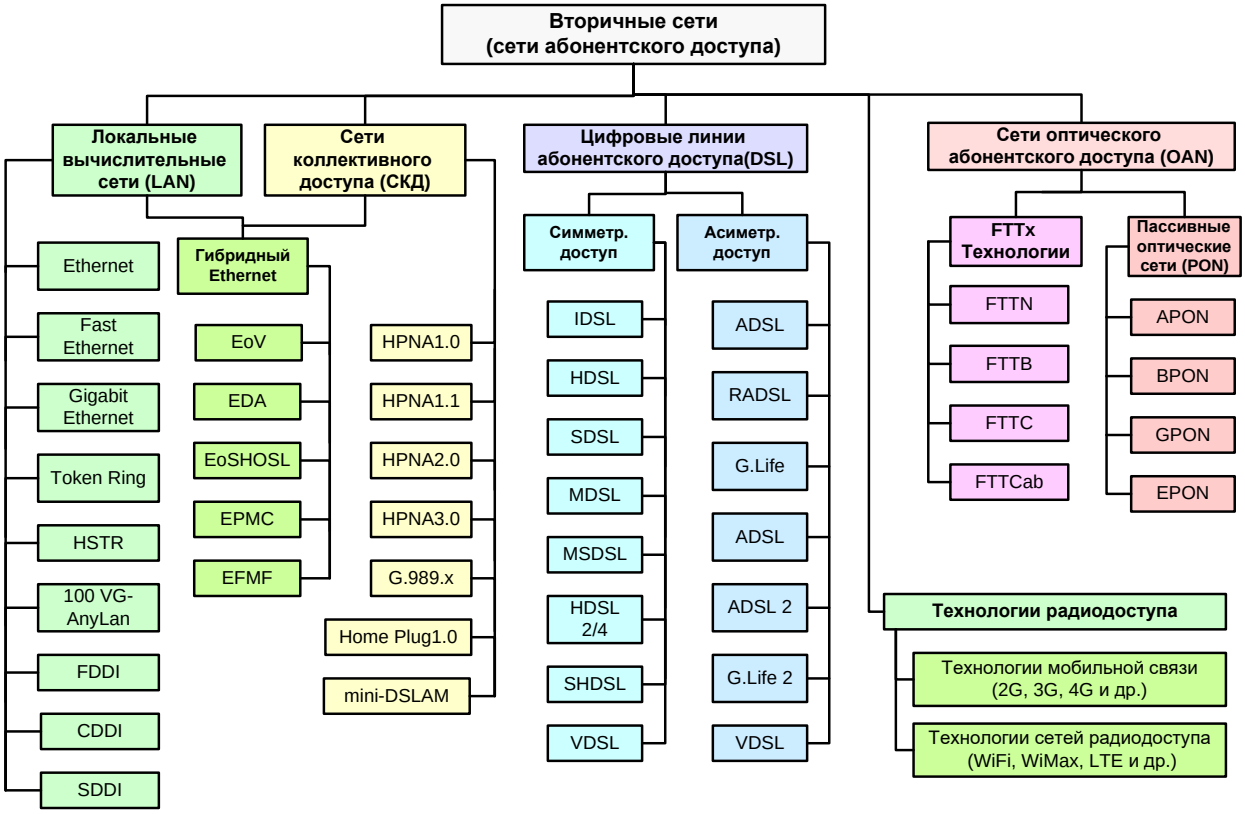

Рис. 1.3. Классификация вторичных сетей СС СН
по используемой технологии связи [62, 381]

По способам предоставления абонентам сервисов и услуг связи в СС СН различают [2]:

- сети с закрепленным ресурсом;
- сети с ресурсом по требованию;
- сети с адаптивным распределением ресурса.

Под ресурсом, как правило, если не указывается иное, понимается пропускная способность сети.

Пропускная способность сети – максимально возможная суммарная скорость передачи сообщений по всем информационным направлениям связи для конкретных условий функционирования. Довольно часто пропускную способность сети оценивают числом типовых каналов на направлениях связи, которые могут быть предоставлены абонентам [2].

При этом под типовым каналом, как правило, понимают *основной цифровой канал* (ОЦК) – цифровой канал связи со скоростью 64 кбит/с, позволяющий передавать оцифрованные с достаточным качеством голосовые сообщения в диапазоне 0,3-3,4 кГц.

Вместе с тем, обеспечение требуемой пропускной способности однозначно связано с определенными затратами других ресурсов – времени, полосы частот, энергии передающих устройств и т.д. В связи с этим можно дать более общее определение ресурсу сети.

Ресурс сети – совокупность канальных, временных, частотных, энергетических и других ресурсов сети связи, затрачиваемых на передачу информации всех абонентов сети [2].

1.1.4. Основные требования, предъявляемые к системе связи специального назначения

Система связи специального назначения функционирует в интересах систем государственного и военного управления, а также систем управления обеспечения безопасности и правопорядка. К данным системам управления предъявляются требования по [2, 381, 335, 398]:

- *устойчивости* – способности органов управления выполнять свои функции в сложной, резко меняющейся обстановке в условиях помех и массированных дестабилизирующих воздействиях противника;
- *непрерывности* – возможности органов управления постоянно взаимодействовать с объектами управления;
- *оперативности* – способности органов управления получать, обрабатывать и преобразовывать информацию, а также формировать управляющие воздействия и доводить их до управляемых объектов в соответствии с темпом изменения текущей ситуации;
- *скрытности* – способности сохранять в тайне информацию о процессах управления, конечной цели и решаемых задачах, имеющихся силах и средствах, а также их возможностях; факт, время и место передачи управляющей информации, ее содержание и принадлежность к конкретным объектам системы управления.

Для обеспечения вышеуказанных требований к управлению, к связи, как к процессу переноса информации между органами и объектами управления, предъявляются требования по [2, 381, 335, 398]:

- *своевременности* – свойству связи, которое характеризует ее способность обеспечивать передачу сообщений или ведение переговоров в заданные сроки;

- *достоверности* – свойству связи, которое характеризует ее способность обеспечивать требуемую точность воспроизведения сообщений в пунктах доставки, а также сохранять эту точность при преобразовании информации;
- *безопасности* – свойству связи, которое характеризует ее способность обеспечить сохранение в тайне содержания передаваемых сообщений и самого факта их передачи.

Соответственно связь, как процесс переноса информации, должна удовлетворять всем этим требованиям, поэтому было введено интегральное понятие «качество связи».

Качество связи – это свойство связи, которое характеризует ее способность обеспечивать своевременную, достоверную и безопасную передачу сообщений.

Для обеспечения указанных требований к связи, в свою очередь СС СН, как организационно-техническая система, должна соответствовать требованиям к определенным ее свойствам. Взаимосвязь этих свойств, требований к связи и требований к системе управления представлена на рис. 1.4. К таким свойствам СС СН относятся [2, 62, 381, 335, 398]:

- *разведзащищенность* – способность системы связи противостоять всем видам разведки;
- *скрытность* – способность системы связи противостоять раскрытию противником факта передачи, содержания передаваемой информации, мест расположения узлов связи, пунктов управления и режимов работы средств связи;
- *криптостойкость* – способность системы связи обеспечивать заданный уровень криптографической защиты и противостоять раскрытию смыслового содержания передаваемой информации;
- *имитостойкость* – способность системы связи противостоять вводу в нее ложной, в том числе и ранее переданной информации и навязыванию ей ложных режимов работы;
- *имитоустойчивость* – способность системы связи обеспечивать требуемый уровень имитостойкости в условиях ввода в нее ложной, в том числе и ранее переданной информации, а также навязыванию ей ложных режимов работы [399-402];
- *управляемость* – способность системы связи изменять свое состояние в заданных пределах при воздействии на нее органов управления связью или средств автоматизации управления, в соответствии с изменениями обстановки;
- *боевая готовность* – способность системы связи в любых условиях обстановки в установленные сроки приступить к выполнению задачи по переносу информации с требуемым качеством;
- *мобильность* – способность системы связи в установленные сроки развертываться, свертываться, изменять структуру и место (район) развертывания в соответствии с реально складывающейся обстановкой;

- *устойчивость* – способность системы связи обеспечивать связь с требуемым качеством в условиях дестабилизирующих воздействий естественного и искусственного характера;
- *живучесть* – способность системы связи обеспечивать связь с требуемым качеством в условиях воздействия на нее обычного и ядерного оружия;

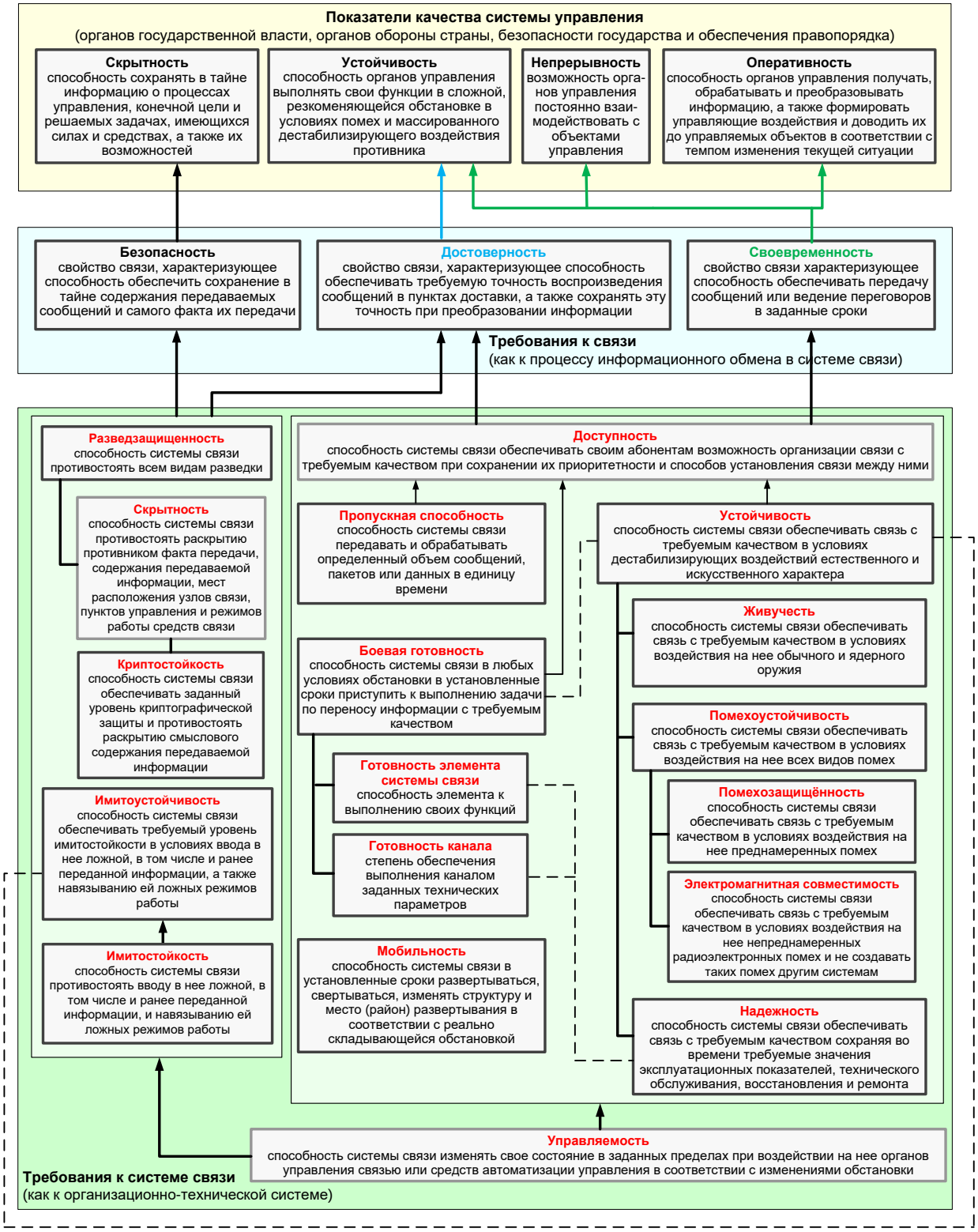

Рис. 1.4. Требования к связи и к СС СН [2, 62]

- *помехоустойчивость* – способность системы связи обеспечивать связь с требуемым качеством в условиях воздействия на нее всех видов помех;
- *помехозащищенность* – способность системы связи обеспечивать связь с требуемым качеством в условиях воздействия на нее преднамеренных помех;
- *электромагнитная совместимость* – способность системы связи обеспечивать связь с требуемым качеством в условиях воздействия на нее непреднамеренных радиоэлектронных помех и не создавать таких помех другим системам;
- *надежность* – способность системы связи обеспечивать связь с требуемым качеством, сохраняя во времени требуемые значения эксплуатационных показателей, технического обслуживания, восстановления и ремонта;
- *доступность* – способность системы связи обеспечивать своим абонентам возможность организации связи с требуемым качеством при сохранении их приоритетности и способов установления связи между ними;
- *пропускная способность* – способность системы связи передавать и обрабатывать определенный объем сообщений, пакетов или данных в единицу времени.

Так как СС СН передает информационные потоки, имеющие прямое отношение к обеспечению обороны и безопасности государства, то, в связи с этим, в СС СН при передаче этих потоков должны обеспечиваться требования по информационной безопасности.

Информационная безопасность – это состояние, при котором обеспечивается конфиденциальность, целостность и доступность информации [64].

Конфиденциальность информации – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на это право [65].

Доступность информации – состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа к информации, могут реализовывать их беспрепятственно [65].

Целостность информации – состояние информации, при котором обеспечивается ее достоверность и полнота [64].

Полнота информации – состав и объем информации достаточный для правильного понимания какого-либо явления или принятия решения.

Достоверность информации – истинность и точность информации в описании какого-либо факта, события или явления.

Структурно-логическая связь между требованиями к СС СН, свойствами информации и категориями информационной безопасности представлены на рис. 1.5.

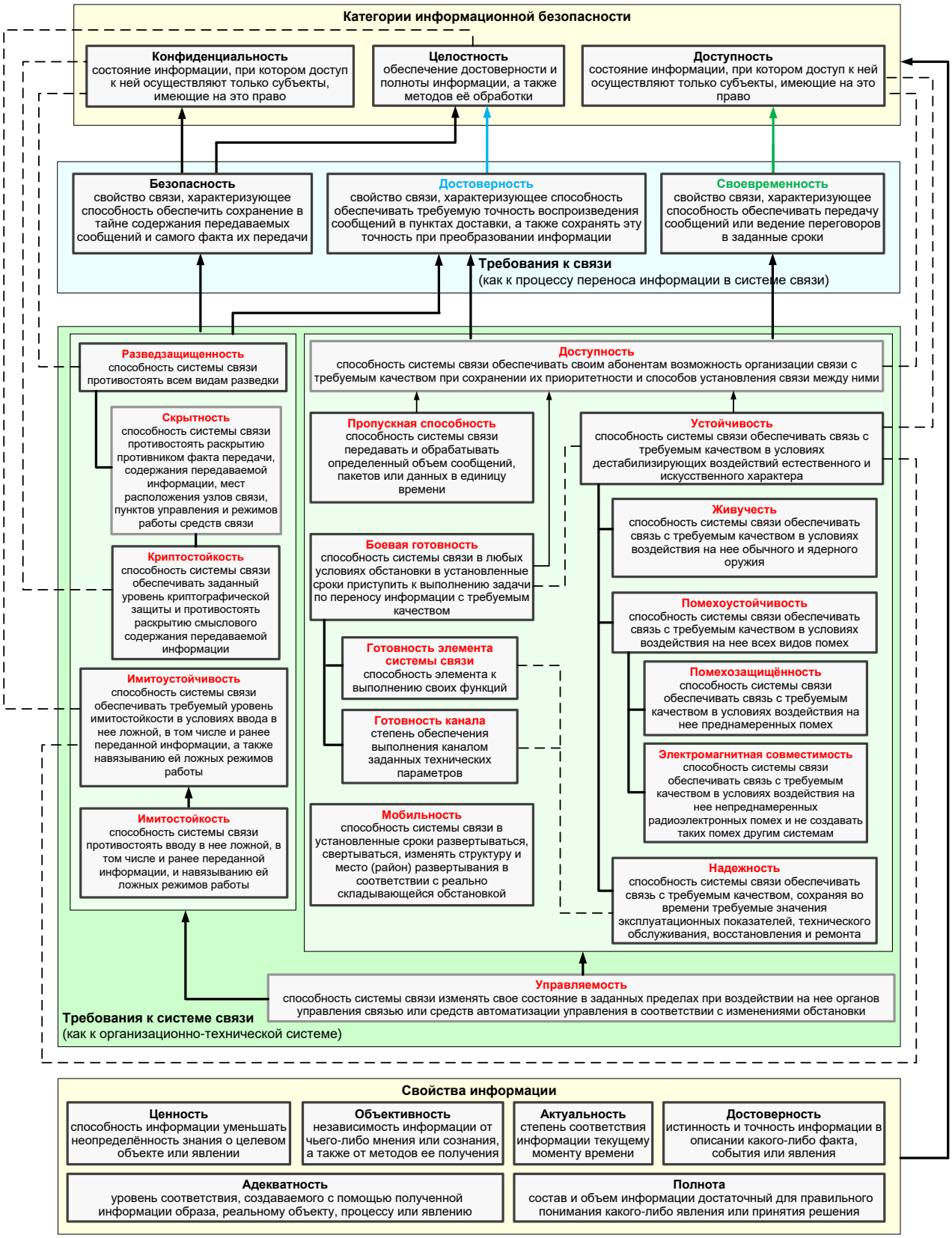

Рис. 1.5. Связь категорий информационной безопасности со свойствами информации и с требованиями, предъявляемыми к СС СН

Основной особенностью СС СН, которая отличает ее от СС ОП, является то, что СС СН ориентирована на функционирование как в мирное, так и в военное время, в условиях воздействия противника, а также различного рода деста-

билизирующих факторов. В связи с этим для СС СН особенное значение приобретает свойство ее устойчивости.

В стандарте [66] даны следующие определения.

Устойчивость сети электросвязи – способность сети электросвязи выполнять свои функции при выходе из строя части ее элементов в результате воздействия дестабилизирующих факторов.

Дестабилизирующий фактор – воздействие на сеть электросвязи, источником которых является физический или технологический процесс внутреннего или внешнего характера, приводящее к выходу из строя элементов сети.

Таким образом, понятие «фактор», в соответствии со стандартом [66], семантически соответствует понятию «воздействие». Уточняя, что основной функцией СС СН является обеспечение требуемого качества связи, а также разделяя дестабилизирующие факторы на естественные и искусственные, можно дать следующее определение.

Устойчивость системы связи – это ее способность обеспечивать требуемое качество связи в условиях воздействия дестабилизирующих факторов естественного и искусственного характера.

1.2. Основные тенденции развития систем связи специального назначения на современном этапе

Анализ работ в области построения СС СН, обеспечивающих информационный обмен в вооруженных силах (ВС) США и НАТО, а также работ в области развития отечественных СС СН [10, 18, 19, 21, 27-30, 32-35, 46-49, 56-58, 61, 381] позволил выявить следующие тенденции развития СС СН:

- переход от сопряжения отдельных СС СН, в различных органах государственного и военного управления к единой СС СН, основанной на многоэшелонированном принципе построения (как правило, СС СН включает в свой состав космический, воздушный, наземный и морской эшелоны);
- широкая интеграция в состав СС СН сегментов СС ОП и коммерческих ТКС;
- активное замещение в СС СН технологий коммутации каналов на технологии коммутации пакетов;
- массовое использование коммерческих протоколов и технологий в составе СС СН, прежде всего, протоколов IP (Internet Protocol) и MPLS (MultiProtocol label Switching);
- конвергенция отдельных сетей и систем связи в единое информационное пространство на основе концепции NGN;
- широкое использование спутниковых систем связи (ССС) в качестве основы, обеспечивающей глобальную связность СС СН и глобальную управляемость во всех звеньях управления, особенно в военное время, при этом в состав СС СН могут включаться ССС гражданских операторов спутниковой связи из состава СС ОП;

- использование в сетях СС СН тактического звена технологий адаптивных мобильных радиосетей Mesh/MANET-сетей (Mobile Ad hoc Network);
- использование методов обработки «больших данных», а также облачных и Grid-технологий для организации распределенного хранения и обработки больших массивов данных.

Рассмотрим основные из этих тенденций более подробно.

1.2.1. Многоэшелонированное построение систем связи специального назначения

Современные СС СН, как правило, декомпозируются на четыре эшелона (рис. 1.6) [35]:

- наземный эшелон (стационарный и полевой (мобильный) сегменты);
- воздушный эшелон (воздушный и наземный сегменты);
- морской эшелон (морской и наземный сегменты);
- космический (космический и наземный сегменты).

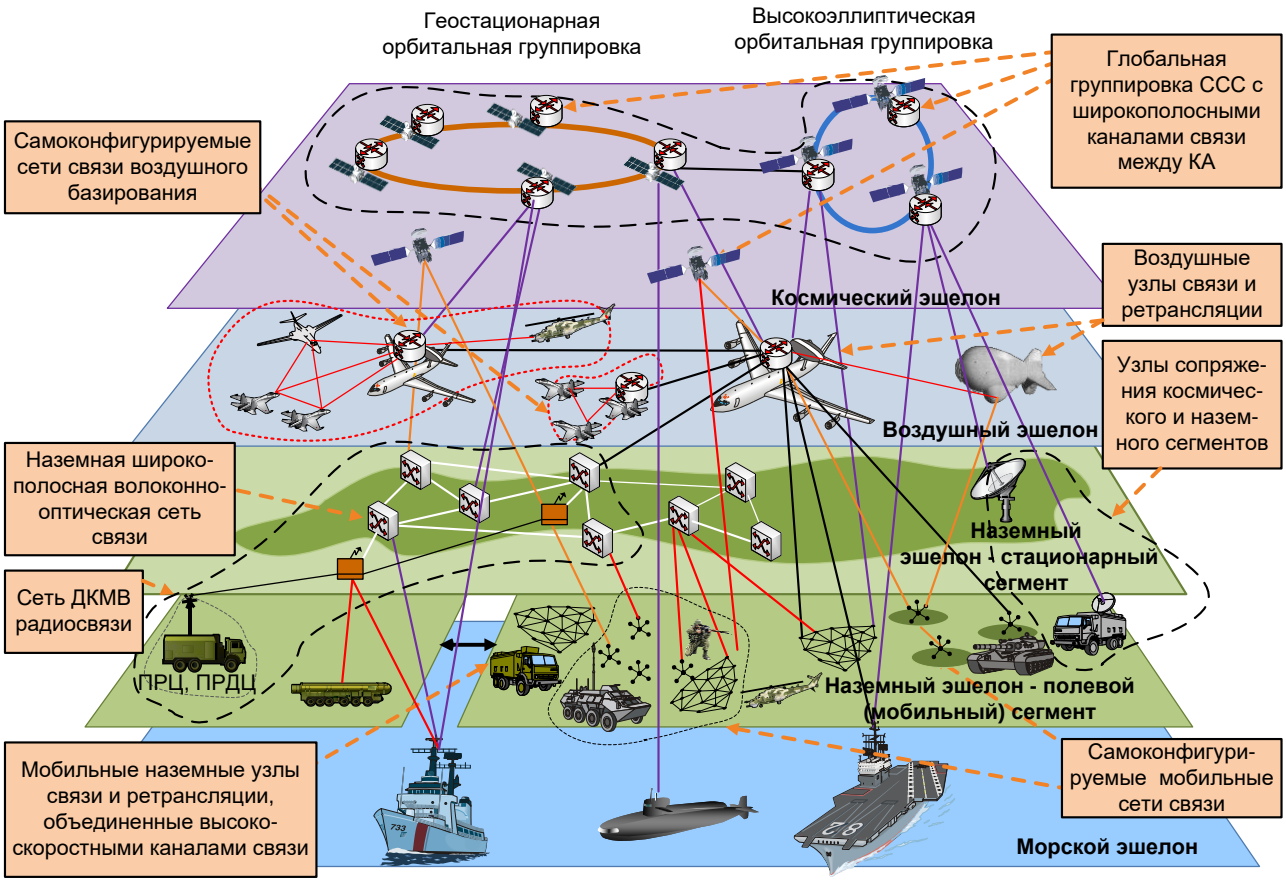

Рис. 1.6. Многоэшелонированное построение СС СН [35]

Наземный эшелон СС СН использует сетевые, унифицированные технические и программно-аппаратные решения со стандартной номенклатурой типовых каналов связи. Наземный эшелон является взаимоувязанной совокупностью стационарных и подвижных узлов и линий связи различных родов. Он представляет организационно-техническое объединение средств и комплексов

связи, выполняющих задачи по образованию, маршрутизации и коммутации каналов связи в интересах системы государственного и военного управления. Узлы и линии связи наземного эшелона, кроме того, обеспечивают взаимодействие между техническими средствами других эшелонов.

Наземный эшелон включает в себя:

- стационарный сегмент;
- полевой (мобильный) сегмент;
- автоматизированную систему управления связью.

Стационарный сегмент наземного эшелона представляет собой цифровую стационарную транспортную сеть в составе СС СН. Стационарный сегмент наземного эшелона базируется на основе территориально-распределенных транспортных сетей из состава СС СН, а также на основе арендованных линий связи СС ОП. В качестве основной физической среды передачи стационарного компонента наземного эшелона, как правило, используются волоконно-оптические линии связи (ВОЛС).

Полевой (мобильный) сегмент наземного эшелона СС СН представляет собой совокупность самостоятельных, но организационно и технически взаимоувязанных ТКС, объединяющихся по звеньям управления:

- в полевую (мобильную) сеть связи стратегического звена управления;
- в полевые (мобильные) сети связи оперативного звена управления;
- в полевые (мобильные) сети связи тактического звена управления.

Полевой сегмент СС СН базируется на общих принципах построения самоорганизующихся мультисервисных сетей с максимально возможным использованием унифицированных цифровых средств и комплексов связи. Предполагается, что структура полевого (мобильного) сегмента наземного эшелона СС СН является инвариантной по отношению к структуре системы государственного и военного управления. В состав узлов связи полевого (мобильного) сегмента входит типовой набор радиорелейных, тропосферных, проводных и спутниковых средств связи, комплексы автоматизации связи, аппаратные электропитания и т.д.

Воздушный эшелон СС СН строится на основе средств воздушной и наземной связи и ретрансляторов на летно-подъемных средствах различного назначения. Воздушный эшелон СС СН включает в себя:

- наземный сегмент;
- воздушный сегмент;
- автоматизированную систему управления связью с элементами наземного и воздушного базирования.

К воздушному сегменту относится транспортная сеть, включающая в себя бортовые комплексы связи, которыми оснащаются ретрансляторы транспортной сети воздушного эшелона, воздушные ПУ, летательные аппараты, различных видов авиации, а также средства связи для сопряжения отдельных сетей других эшелонов, базирующихся на летно-подъемных средствах (самолеты, вертолеты, дирижабли, аэростаты, беспилотные летательные аппараты, и т.д.).

К наземному сегменту воздушного эшелона относятся комплексы связи, размещаемые на наземных стационарных и подвижных узлах связи, а также средства сопряжения с транспортной сетью наземного эшелона.

Технической основой воздушного эшелона являются комплексы радиосвязи КВ и УКВ диапазонов, а также средства спутниковой связи.

Морской эшелон СС СН представляет организационно-техническое объединение стационарных и мобильных узлов связи, радиоцентров, радиостанций, автоматизированных комплексов связи подводных лодок, кораблей, летательных аппаратов, соединенных линиями различных родов связи. Для организации радиосвязи используются различные диапазоны радиоволн (СНЧ, СДВ, ДВ, СВ, КВ, УКВ), а также каналы спутниковой связи. Морской эшелон включает в себя:

- морской сегмент;
- наземный сегмент;
- автоматизированную систему управления связью.

Морской сегмент, как правило, состоит из средств связи и автоматизации, размещаемых на подводных лодках и кораблях, а при организации сетей для ретрансляции сигналов используются радиоретрансляторы на летно-подъемных средствах и ССС.

Космический эшелон СС СН развертывается на основе ССС, образованных линиями спутниковой связи и узлами сети – земными станциями и космическими аппаратами связи. Космический эшелон СС СН включает в себя:

- космический сегмент;
- наземный сегмент;

Космический эшелон СС СН предназначен для обеспечения глобальной связности СС СН в стратегическом и оперативно-тактическом звеньях управления, правительственной связи и специальной связи. При этом структура космического эшелона СС СН инвариантна по отношению к структуре системы государственного и военного управления. Технологии, применяемые в сетях космического эшелона, обеспечивают интеграцию различных видов трафика, устойчивое и глобальное взаимодействие комплексов и средств, на стационарных, полевых и подвижных узлах связи различных звеньев управления для стационарного наземного, полевого (мобильного) наземного, воздушного и морского эшелонов с целью обеспечения возможности обмена всеми видами информации между всеми абонентами во всех эшелонах СС СН.

1.2.2. Использование в системах связи специального назначения канальных и сетевых ресурсов, арендуемых у коммерческих операторов связи

Анализ современных СС СН, а также перспектив их развития, представленных в работах [10, 18, 19, 21, 27-30, 32-35, 46-49, 56-58, 61, 381, 335, 398], позволяет сформулировать следующие основные тенденции технологического построения СС СН:

- переход от иерархического принципа построения СС СН, когда ее структура жестко увязывается со структурой организационной подчиненности абонентов к децентрализовано-сетевой структуре, которая не

зависит от системы подчиненности абонентов и, в большей степени, соответствует современным требованиям к сетецентрическим системам государственного и военного управления;
- отказ от построения СС СН на основе выделенной сетевой инфраструктуры и переход к построению СС СН на основе гибридного подхода, когда отдельные сегменты СС ОП национальных и региональных операторов связи, а также сегменты глобальных сетей используются в качестве элементов транспортной инфраструктуры СС СН;
- максимальное широкое использование для построения СС СН подходов, протоколов и технологий, применяемых в гражданской сфере связи и телекоммуникаций.

Данные тенденции подтверждаются общими принципами построения СС СН как для ВС РФ, так и для ВС США.

Стационарные и мобильные узлы, на основе которых разворачиваются компоненты перспективных СС СН, привязываются к единой транспортной сети СС СН, основу которой составляют ВОЛС, а использование ССС обеспечивает глобальность информационного обмена и связность отдельных сетевых ВОЛС-сегментов. При этом, при недостатке собственных ресурсов СС СН, как правило, необходимые канальные ресурсы из СС ОП арендуются у региональных и национальных операторов связи. Основным подходом к организации такой аренды, является использование низкоуровневых ресурсов сети операторов связи, к которым можно отнести [28-30]:
- выделенные каналы связи для передачи потоков E1-E4, STM-n;
- оптические волокна в волоконно-оптическом кабеле;
- отдельные длины волн (в составе ВОЛС с технологией WDM);
- радиоресурсы коммерческих ССС;
- виртуальные и логические соединения на канальном уровне, реализуемые, например, с использованием базовых услуг канального уровня сети передачи данных VLAN, L2 VPN;
- виртуальные частные сети и туннели канального (технологии VLAN, MPLS L2 VPN, VPLS, L2TP, L2TP и др.) и сетевого уровня (технологии IP VPN, MPLS L3 VPN, IPSec и др.).

Необходимо отметить, что используемые структурно-технологические решения по сопряжению транспортных сетей из состава СС СН с сетями в составе СС ОП гражданских операторов связи обеспечивают связность на сетевом уровне, как правило, за счет использования единых протокольных решений на основе протоколов IPv4 и IPv6. В целях обеспечения безопасности при сопряжении СС СН с СС ОП используются решения, обеспечивающие изоляцию адресных пространств отдельных сетей в составе СС СН и передаваемых потоков трафика от тех сегментов и потоков, которые обслуживаются в СС ОП гражданскими операторами связи.

Ряд экспертов считает, что в настоящее время развертывание отдельной телекоммуникационной инфраструктуры СС СН является экономически нецелесообразным, и что современные и перспективные СС СН активно используют и будут использовать ресурсы гражданских операторов СС ОП национального

и регионального масштаба. Однако, при таком пути развития СС СН, на нее существенное влияние будут оказывать технологии, на основе которых строятся и модернизируются сети гражданских операторов связи [28-30].

Таким образом, из самого факта сопряжения СС СН и СС ОП следует два важных вывода:

1) технологии связи СС СН должны быть «обратно совместимыми» с технологиями, используемыми в гражданских СС ОП, для обеспечения использования ресурса СС ОП в интересах СС СН;
2) сквозное сопряжение СС СН с СС ОП, а также последней с гражданскими СС ОП других государств, делает СС СН потенциально уязвимой для преднамеренных дестабилизирующих воздействий, организуемых через СС ОП других государств.

Эти выводы определяют следующие современные тенденции развития СС СН:

1) мировой тенденцией является использование для построения перспективных СС СН современных «гражданских технологий», широко используемых в СС ОП, а не разработка специализированных технологических решений;
2) использование в СС СН «гражданских технологий», одновременно с их фактической интеграцией через общие сегменты СС ОП в мировое информационное пространство, существенно расширяет спектр уязвимостей СС СН, которые могут быть использованы противником при реализации преднамеренных дестабилизирующих воздействий.

1.2.3. Использование в системах связи специального назначения технологий коммутации пакетов и коммерческих протоколов связи

В настоящий момент в мире происходит активное замещение специализированных технологий связи на открытые коммуникационные технологии, которые являются общими как для гражданских СС ОП, так и для СС СН. Например, в органах государственного и военного управления США и НАТО эксплуатируется большое количество СС СН, используемых различными ведомствами и базирующихся на использовании как специализированных военных, так и коммерческих телекоммуникационных ресурсов.

Принципиальным изменением, которое происходит в области построения транспортных сетей СС СН является переход к пакетной коммутации, при необходимости обеспечения устойчивого и мультисервисного обслуживания специальных абонентов. При этом в качестве базовых технологий в транспортных сетях доступа широко используются технологии коммутации пакетов IPv4 и IPv6, а также технология коммутации по меткам MPLS, которые начинают вытеснять такие технологии транспортных сетей как PDH, SDH и ATM [27-30, 46-49].

Анализ работ [10, 18, 19, 21, 27-30, 32-35, 46-49, 56-58, 61], посвященных возможным вариантам технологического построения перспективных СС СН,

позволил сформировать основные принципы и технологии, используемые в них для организации связи.

Транспортная сеть СС СН представляет собой совокупность множества объединенных между собой пакетных ТКС, выполняющих задачи по доставке пакетов от абонента-источника к абоненту-потребителю.

Перспективные СС СН, как правило, строятся на основе ТКС, использующих IP протоколы, кроме того, в них так же могут использоваться сети на основе технологий MPLS и MPLS-TE (для сетей на основе ресурсов ВОЛС и радиорелейной связи), технологии ATM, протоколов DVB-S/DVB-S2 (для ССС), протоколов на основе открытых стандартов STANAG (для сетей ДКМВ радиосвязи). Для обеспечения работы по каналам низкого качества, в большинстве случаев, в СС СН сохранено использование протоколов X.25 (для проводных аналоговых каналов с вероятностью ошибки 10^{-3}), AX.25 и FX.25 (для аналоговых радиоканалов с вероятностью ошибки 10^{-2} и $5 \cdot 10^{-2}$) [56-58].

Таким образом, в транспортной сети СС СН используются следующие протокольные решения [21, 29, 43]:

- IP/MPLS, самостоятельно или поверх PDH/SDH/OTH/ATM/Gigabit Ethernet – для построения проводного транспортного сегмента;
- X.25 – для обеспечения работы по проводным аналоговым каналам и каналам связи низкого качества;
- AX.25 и FX.25 – для обеспечения работы по аналоговым радиоканалам и каналам связи низкого качества в условиях мирного времени, а также для построения мобильной (полевой) транспортной сети СС СН в условиях военного времени;
- протоколы семейства DVB (DVB-S/DVB-S2/DVB-RSC) – для организации спутниковых каналов связи.

Применение пакетных технологий на основе протоколов IP/MPLS позволяет обеспечить организацию связи в транспортной сети СС СН на сетевых принципах, которые ранее были недоступны для ТКС на основе технологий коммутации каналов PDH/SDH/OTH. Это позволяет обеспечить в СС СН следующие эффекты [29]:

- возможность взаимодействия каждого абонента с каждым (по схемам «point-to-point» и «multipoint-to-multipoint») в любой момент времени при условии эффективного использования сетевых ресурсов;
- эффект повышения устойчивости транспортной сети и улучшения качества обслуживания (QoS – Quality of Service), несмотря на возможное использование разных операторов связи, в условиях выхода из строя большинства узлов связи, за счет оперативной организации обходных маршрутов в статическом и динамическом режимах.

Обобщенная структурная схема сети СС СН приведена на рис. 1.8.

Объединение отдельных ТКС организуется путем обмена маршрутной информацией, необходимой для правильного выбора маршрута доведения пакетов с учетом отказов и возможной перегрузки сетевых элементов. Для СС СН, состоящей из большого числа ТКС и подсетей с высоким числом взаимных связей, используются динамические протоколы маршрутизации. При обмене

маршрутной информацией между ТКС и сетями в СС СН, как правило, используется маршрутный протокол BGP4 [56-58].

В ТКС и в сетях, входящих в состав СС СН, используются известные модели и механизмы обеспечения качества обслуживания (IntServ, DiffServ), применяемые в пакетных сетях, с целью обеспечения требуемых показателей QoS. С целью исключения случаев перегрузки трафиком в состав каждой ТКС включаются граничные маршрутизаторы. Передаваемый трафик квотируется путем соглашения между абонентами и службой администрирования как ТКС, так и всей СС СН в целом. При превышении квот трафик сбрасывается, либо доводится без гарантий по соблюдению требуемых показателей качества обслуживания в режиме «Best Effort».

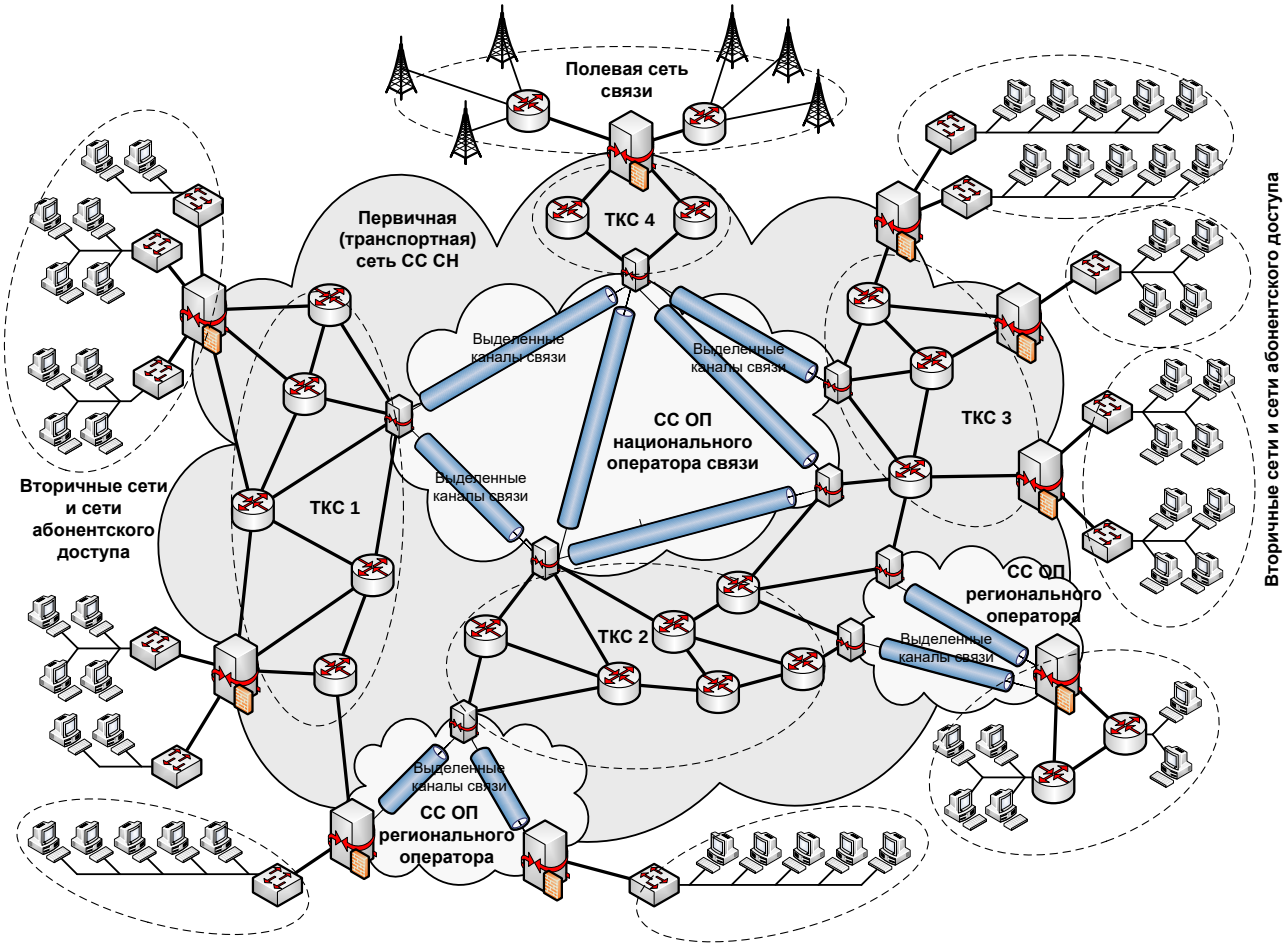

Рис. 1.7. Обобщенная структурная схема СС СН

Таким образом, транспортная сеть СС СН строится с использованием единых подходов и архитектуры, технологий и средств передачи, защиты данных и управления в части как стационарного, так и мобильного (полевого) сегмента:

- стационарный сегмент транспортной сети СС СН строится с использованием ТКС, основанных на технологии пакетной коммутации IP/MPLS с встроенными функциями динамической маршрутизации, а также с использованием ТКС, основанных на технологиях коммутации каналов PDH/SDH/OTH с каналами типа E1-E4, STM-n, OTU-n. При

этом данные ТКС могут являться как сегментами самой СС СН, так и сегментами СС ОП региональных и национальных операторов связи;
- мобильный (полевой) сегмент СС СН строится с использованием ТКС, основанных на преимущественном использовании пакетных технологий IP/X.25/AX.25 (FX.25);
- унаследованное оборудование СС СН сопрягается с новыми средствами связи и современными ТКС через модули сопряжения, которые инкапсулируют трафик унаследованных средств связи в пакетный трафик, что позволяет обеспечить единый подход к транспортировке всех видов информации с использованием пакетной коммутации.

Вышеуказанные подходы к построению транспортной сети СС СН позволяют:

- использовать единую технологию коммутации пакетов для передачи информации как по проводным (оптическим, медным и др.) и беспроводным (радиорелейным, тропосферным, спутниковым, широкополосного радиодоступа, КВ/УКВ и иным) аналоговым и цифровым каналам связи СС СН, так и по каналам связи СС ОП региональных и национальных операторов связи, включая глобальную сеть Интернет;
- осуществлять оперативное динамическое управление ресурсами СС СН, в том числе адаптивную перемаршрутизацию потоков трафика с учетом динамики изменения структуры транспортной сети СС СН в результате дестабилизирующих воздействий;
- обеспечить согласованное взаимодействие отдельных ТКС, сетей и унаследованных средств связи, входящих в транспортную сеть СС СН, и в итоге – объединить их в единое инфотелекоммуникационное пространство;
- получить ряд технологических преимуществ от внедрения в состав СС СН новых ТКС, основанных на новейших коммерческих технологиях из гражданской отрасли связи.

1.2.4. Построение систем связи специального назначения в соответствии с концепцией NGN

Анализ работ в области глобальных перспектив развития СС СН [27-30, 32-35, 46-49] позволяет сделать вывод об эволюционном развитии СС СН в направлении перехода к концепции NGN. В частности, в данном направлении эволюционируют СС СН США, в которых уже реализованы концептуальные решения по объединению в единое информационное пространство разнородных сетей и систем связи, а также переход к персонализированным услугам связи для каждого абонента, вне зависимости от его географического местонахождения [50]. Обзор основных технологических решений концепции NGN представлен в более ранней работе автора [20], а возможности по использованию концепции NGN для построения СС СН в достаточно полном виде представлены в работе А.Н. Назарова и К.И. Сычева [27].

Базовым принципом построения сети связи следующего поколения является строгое разделение функций переноса и коммутации информационных по-

токов, а также управления вызовами и услугами. При этом, в соответствии с рекомендацией МСЭ-Т Y.2011, базовая архитектура сети NGN может быть представлена четырьмя функциональными уровнями [27]:

1) уровнем приложений и услуг;
2) уровнем коммутации услуг;
3) уровнем транспорта, включающего функции управления сетевыми ресурсами и уровень доступа;
4) уровнем управления сетью.

Для построения сети NGN необходимо, в дальнейшем, реализовать каждый из этих уровней в виде соответствующего набора элементов сети NGN (рис. 1.8). При этом на различных функциональных уровнях сети могут использоваться различные технологии и протоколы.

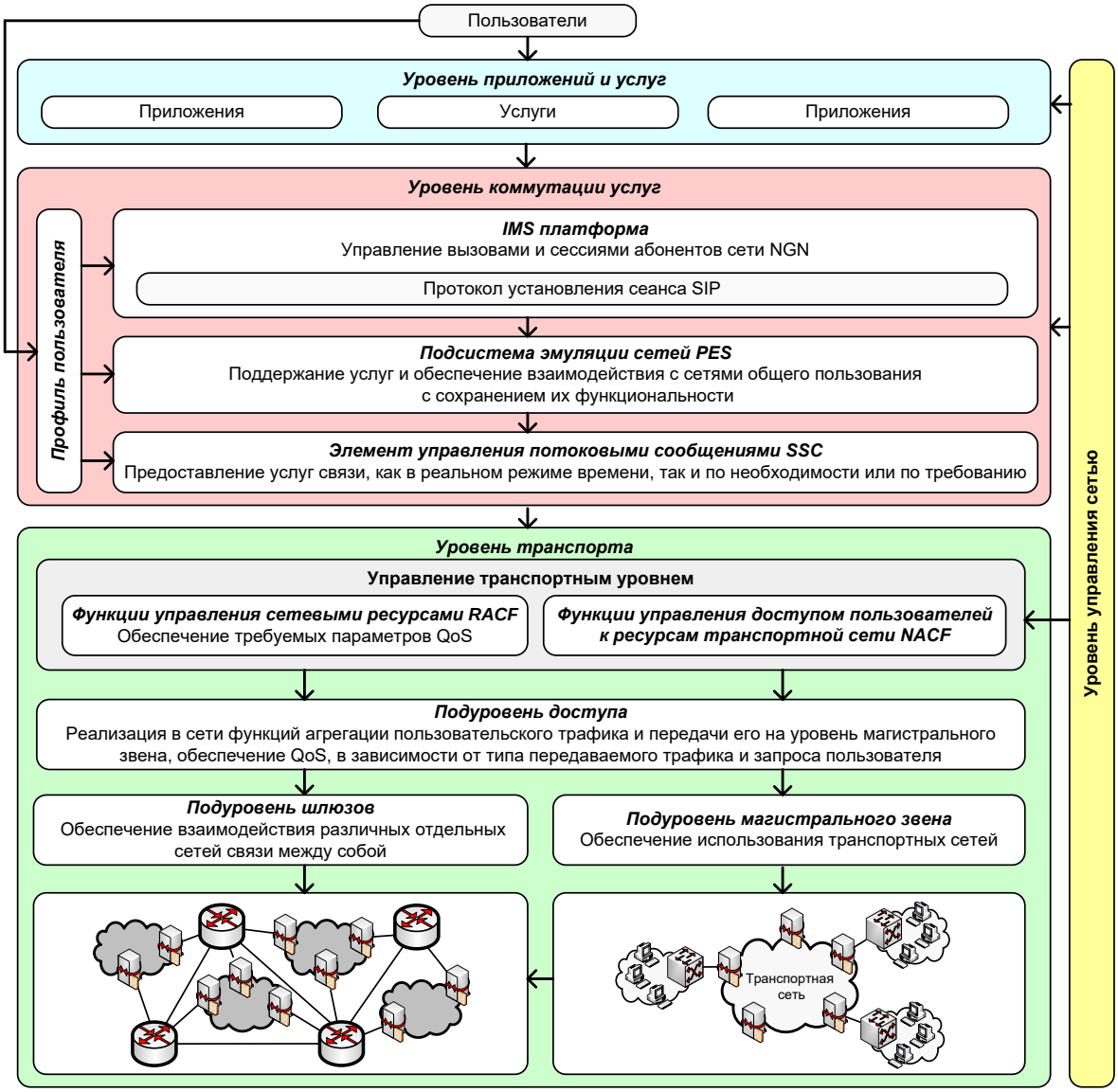

Рис. 1.8. Схема основных уровней сети NGN [20]

Уровень приложений и услуг выполняет функции управления логикой предоставления услуг и функционирования приложений и представляет собой

распределенную вычислительную среду, обеспечивающую следующие потребности пользователей [20]:

- предоставление инфокоммуникационных услуг;
- управление услугами;
- создание и внедрение новых услуг;
- взаимодействие различных услуг.

Уровень коммутации услуг позволяет реализовать специфику услуг и применять одну и ту же логику оказания услуги, вне зависимости от типа транспортной сети (IP, ATM, FR и т.п.) и способа доступа к ней. Наличие этого уровня также позволяет вводить в сети новые услуги без вмешательства в функционирование других уровней. В основе этого уровня лежит взаимодействие с центральными элементами сети NGN – элементами уровня коммутации (IMS, PES и SSC), которое осуществляется по стандартным интерфейсам ANI (Access Network Interface) для доступа в сеть. Данный уровень может включать множество независимых подсистем («сетей услуг»), базирующихся на различных технологиях, имеющих своих абонентов и использующих свои, внутренние системы адресации [20].

Фактически, на данном уровне обеспечивается решение основных задач по установлению соединений и предоставлению услуг в сети NGN.

Основными функциями, которые обеспечиваются на уровне коммутации услуг, являются [20]:

- регистрация пользователей (аутентификация и авторизация) для предоставления им доступа к определенным услугам NGN;
- управление сессиями, вызовами (установление, разрыв и поддержание соединений);
- управление коммутацией и передачей, обработка данных сигнализации, маршрутизация вызовов и управление информационными потоками;
- управление ресурсами сети, включая шлюзы и маршрутизаторы, установленные на транспортном уровне сети NGN.

Транспортный уровень сети NGN обеспечивает выполнение функций коммутации и «прозрачной» передачи информации пользователя. Данные функции образуются двумя подгруппами [20]:

- функции управления сетевыми ресурсами (RACF – Resource and Admission Control Functions), обеспечивающие реализацию в сети заданных параметров QoS. Сюда входит резервирование требуемых сетевых ресурсов, управление доступом к ресурсам транспортной сети, управление ресурсами шлюзов и т.д.;
- функции, реализуемые на основе информации авторизации пользователей, соглашений об уровне обслуживания SLA, приоритета предоставляемой услуги, а также доступных сетевых ресурсов на транспортной сети и сети доступа.

Транспортный уровень включает в себя ряд функциональных подуровней [20]:

- подуровень доступа. На данном уровне реализуются функции агрегации абонентского трафика, которые зависят от типа передаваемого

трафика и запросов пользователя, а также обеспечение QoS трафика и передача его на уровень магистрального звена;
- подуровень магистрального звена. Магистральное звено в виде отдельного ТКС должно обеспечивать передачу агрегированного пользовательского трафика в соответствии с требованиями по QoS. На данном уровне применяются те же механизмы по управлению QoS, что и на уровне доступа;
- подуровень шлюза. Данный уровень обеспечивает возможность взаимодействия различных ТКС, построенных на основе различных технологий, а также взаимодействие с другими сетями NGN.

Технологической основой построения транспортного уровня является транспортная сеть NGN, строящаяся на основе технологий коммутации каналов PDH/SDH/OTH и, преимущественно, коммутации пакетов IP, ATM, MPLS. В дальнейшем планируется, что связка протоколов IP/MPLS и технология построения виртуальных сетей VPN будут базовыми для транспортного уровня NGN. Данные технологии способны обеспечивать управление и мониторинг качества всех уровней магистрального звена: сетевого, канального и физического. Это обеспечивает возможность предоставления абонентам сети услуг с заданным качеством.

Уровень управления сетью обеспечивает функции управления и соответствует системе управления сетью NGN. В задачи данного уровня входят: мониторинг и управление инфраструктурой и ресурсами сети, поддержание в сети заданных параметров качества, а также ряда параметров, характеризующих работу сети в целом [20].

Система управления должна обеспечивать [20]:
- управление процедурами устранения ошибок и сбоев;
- управление процедурами конфигурации;
- управление автоматизированной системой расчетов;
- управление сетевыми характеристиками;
- управление безопасностью.

Основу сети NGN составляет мультипротокольная ТКС (рис. 1.9), как правило, на основе технологий ATM, IP, MPLS, которая предоставляет услуги переноса данных и реализует функции транспортного уровня и уровня управления вызовами. Целью построения транспортной сети NGN является переход от отдельных сетей предыдущего поколения, предназначенных для отдельных групп пользователей или услуг (телефония, данные и др.) к интегрированной сети с гарантированным качеством обслуживания.

В состав интегрированной транспортной сети NGN могут входить [27]:
1) транзитные узлы, выполняющие функции переноса и коммутации;
2) оконечные и граничные узлы, обеспечивающие доступ абонентов;
3) контроллеры сигнализации или контроллеры медиашлюзов (Media Gateway Controller, MGC/Softswitch), выполняющие функции обработки информации сигнализации, управления вызовами (запросами) и соединениями, а также управления транспортной сетью NGN;

4) шлюзы, осуществляющие подключение сетей связи предыдущих поколений:
   - медиашлюз или транспортный шлюз MG (Media Gateway), предназначенный для преобразования речевой информации в IP-пакеты или ATM-ячейки и их маршрутизации;
   - сигнальный шлюз SG (Signalling Gateway), предназначенный для ретрансляции и преобразования данных сигнализации;
   - транкинговый шлюз TG (Trunking Gateway), выполняющий функции транспортного и сигнального шлюзов;
   - шлюз доступа AG (Access Gateway), выполняющий функции транспортного и сигнального шлюзов при подключении по интерфейсу V.5;
   - резидентный шлюз доступа RAG (Residential Access Gateway), предназначенный для подключения пользователей телефонных сетей и сетей ISDN;

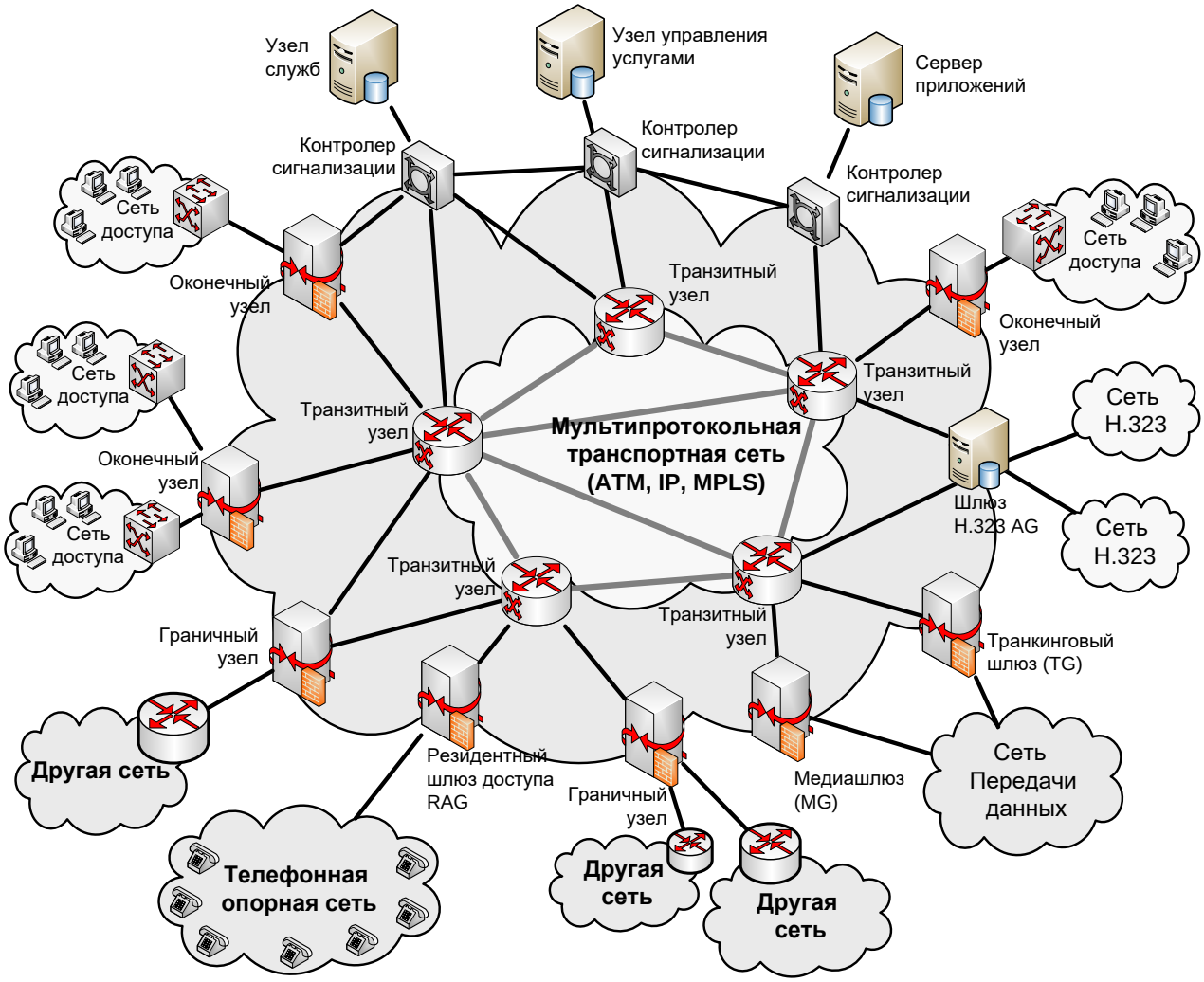

Рис. 1.9. Мультипротокольная транспортная сеть NGN [20]

5) пограничный контроллер соединений SBC (Session Border Controller), обеспечивающий сопряжение оборудования нескольких производителей и выполняющий функции шлюза сигнализации и медиа-шлюза, контроля за установлением соединений CAC (Call Admission Control), управления QoS, а также концентрации голосового и сигнального трафика;
6) сетевые устройства на основе стандарта H.323 для предоставления узкополосных аудио и видео услуг в комбинированных коммутируемых и пакетных сетях:
   - шлюз H.323 AG (Access Gateway), предназначенный для преобразования медиа-потоков между коммутируемыми и пакетными сетями;
   - шлюз-привратник (Gatekeeper H.323), предназначенный для преобразования адресации (IP, телефонных номеров) между коммутируемыми и пакетными сетями, а также управления полосой пропускания;
   - блок многоточечного управления MCU (Multipoint Control Unit), предназначенный для обеспечения соединений «точка-точка», «многоточка-многоточка», а также конференц-связи.

Концепция NGN предполагает создание регионального и магистрального сегментов сети. При этом на региональном уровне должно обеспечиваться подключение пользователей и предоставление им транспортных услуг, а также взаимодействие с аналогичными региональными транспортными сетями. На магистральном уровне должно обеспечиваться предоставление услуг переноса конвергентного трафика для взаимодействия региональных сетей, а также передача трафика всех существующих сетей [27].

Модель звена транспортной сети NGN представлена на рис. 1.10. При этом в данной модели для реализации любых сетевых услуг в различных ТКС предполагается использование именно IP-технологии.

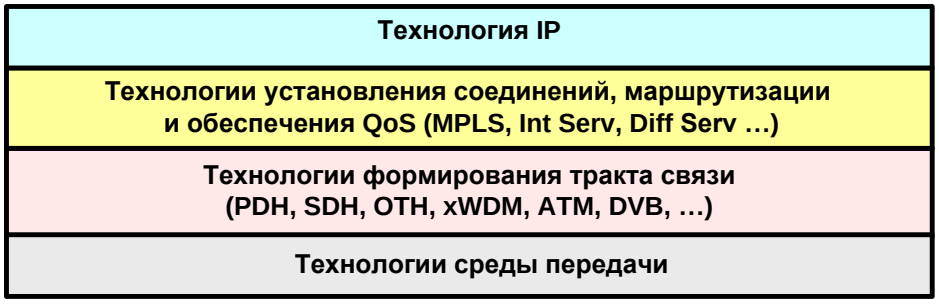

Рис. 1.10. Модель звена транспортной сети NGN [27]

При организации сети NGN основные функции уровня транспорта реализуются протоколами сетевого и транспортного уровня модели OSI. Именно эти протоколы выполняют в ТКС NGN функции маршрутизации, установления и разрыва соединений, а также обеспечения QoS трафика.

На транспортном уровне OSI в сети NGN для обеспечения QoS передаваемых потоков трафика могут использоваться как известные технологии обеспе-

чения QoS, основанные на моделях IntServ и DiffServ, так и механизмы, встроенные в транспортные технологии канального уровня – ATM, MPLS, SDH, DVB и др.

На сетевом уровне OSI для маршрутизации в сети NGN на основе IP могут использоваться протоколы без установления соединения, такие как OSPF, IS-IS, RIP и др. Однако, для маршрутизации потоков трафика в мультипротокольном ядре ТКС NGN на основе ATM и IP/MPLS используется протокол маршрутизации с установлением соединения PNNI.

На канальном уровне ТКС NGN выполняются функции формирования цифровых трактов связи на основе технологий PDH, SDH, WDM, Ethernet (Gigabit Ethernet/10-Gigabit Ethernet), ATM, DVB-S/S2/RSC и др.

Физический уровень, как среда передачи сигналов, реализуется на основе волоконно-оптических, радиорелейных и спутниковых линий связи [27].

В соответствии с вышесказанным, при построении сетей NGN обеспечиваются следующие сочетания транспортных технологий [27]:

- IP/ATM/SDH/ВОЛС, радиорелейные, спутниковые линии связи;
- IP/ATM/ВОЛС, радиорелейные, спутниковые линии связи;
- IP/SDH/ВОЛС, радиорелейные, спутниковые линии связи;
- IP/ВОЛС;
- IP/MPLS/ВОЛС, радиорелейные, спутниковые линии связи.

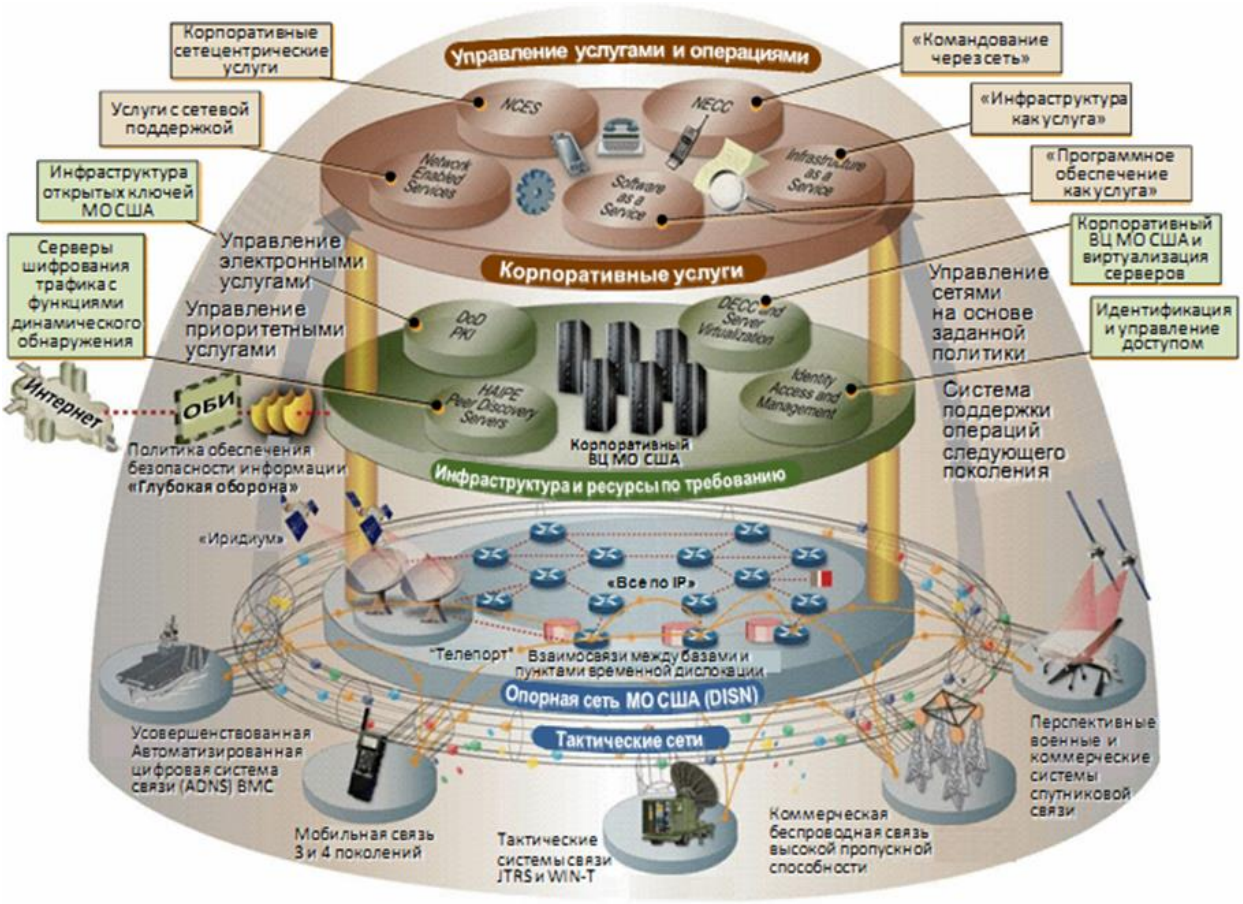

Рис. 1.11. Общая структура информационного пространства на основе GIG [68]

Для построения высокоскоростных сетей NGN могут применяться технологии цифровых транспортных иерархий нового поколения OTN/OTH, а также технологии автоматически коммутируемых транспортных сетей ASON/ASTN, которые будут обеспечивать более высокую эффективность использования сетевых ресурсов при передаче разнородного трафика. В перспективе, построение транспортной сети СС СН на основе NGN будет эволюционировать к однородной конвергентной структуре на базе связки протоколов IP/MPLS – концепция «все по IP» (рис. 1.11). При этом данная транспортная сеть будет включать два логических подуровня: сетевой и сервисный [27].

Сетевой логический подуровень включает [27]:

- транспортную сеть IP/MPLS, выполняющую функции канального, сетевого и транспортных уровней модели OSI;
- пограничный интеллектуальный слой (шлюзы MG, SG, MGC), предназначенный для агрегации, преобразования и передачи трафика по IP/MPLS сети;
- слой с функциями доступа к транспортной сети.

В свою очередь сервисный подуровень включает различные платформы приложений (в том числе IMS) и серверы приложений.

Данный подход обеспечит дальнейшее повышение эффективности использования сетевых ресурсов при внедрении NGN за счёт объединения различных ТКС фиксированной и мобильной связи в составе СС СН в единую транспортную сеть IP/MPLS, поддерживающую широкий спектр технологий доступа.

1.2.5. Переход от систем связи к инфокоммуникационным системам специального назначения

Дальнейшее развитие концепции NGN в практике построения СС СН привело к эволюционной миграции от СС СН к инфокоммуникационным системам (ИКС) специального назначения. Ключевым в таком переходе является развитие на основе концепции NGN информационных услуг, связанных не только с передачей информации, но и с ее сбором, обработкой, хранением, а также поиском и представлением пользователям по их запросам. Переход от СС СН на основе NGN к инфокоммуникационным системам связан с развитием АСУ связью и интеграцией в них существующего научно-технического задела в области управления ресурсами связи в СС ОП (прежде всего, стандартов концепции TMN), виртуализации сетевых и вычислительных ресурсов, а также использования новых технологических решений по обеспечению устойчивости такой системы в условиях преднамеренных дестабилизирующих воздействий.

Основные принципы формирования инфокоммуникационных систем подробно рассмотрены в работах К.Е. Легкова [36-42] и А.Н. Буренина [40-42].

Инфокоммуникационная система специального назначения (ИКС СН) – информационная система, обеспечивающая предоставление набора как связных, так и информационных услуг с гибкими возможностями по управлению ими и их персонализации, и предназначенная для нужд органов государственной вла-

сти, обороны страны, безопасности государства и обеспечения правопорядка [37].

Главное отличие ИКС СН от СС СН на основе NGN – это дополнительное предоставление пользователям и техническим средствам помимо услуг связи еще и других информационных услуг, связанных со сбором, обработкой, хранением, поиском и представлением информации. Предоставление этих услуг унифицировано и осуществляется соответствующими программно-аппаратными комплексами услуг, которые поддерживают широкий спектр ТКС в составе ИКС СН. Тем самым, обеспечивается предоставление всем пользователям полного спектра услуг, связанных как с обменом информацией, так и с ее накоплением, хранением и обработкой [37].

Как правило, различные ИКС СН существенно отличаются друг от друга потребностями в ресурсах, объемом, структурой, возможностями, реальной пропускной способностью, а также безопасностью и устойчивостью [37].

Создаваемые в настоящее время ИКС СН следуют концепции NGN. Основой архитектурного построения ИКС СН являются: транспортная сеть (как правило, двухуровневая), сети доступа, узлы информационных служб, узлы телекоммуникационных служб, узлы управления услугами [37].

В современных ИКС СН двухуровневая транспортная сеть связи, входящая в их состав, с соответствии с концепцией NGN является мультипротокольной и обеспечивает перенос разных видов информации с использованием различных протоколов передачи (PDH, SDH, ATM, FR, IP/MPLS и др.), т.е. реализует универсальную услугу связи, которая заключается в бесшовной передаче информации пользователей между отдельными ТКС в составе ИКС без какого-либо анализа или обработки ее содержания [37].

Средства ИКС СН помимо услуги связи предоставляют также информационные услуги, основанные на обработке и анализе информации пользователей. В рамках ИКС СН информационные услуги характеризуются транзакциями, которые осуществляются при запросе/активизации услуги. При этом сервис предоставления информационной услуги основан на том, что соответствующие услуги связи для информационных транзакций оказываются с заданным качеством. Пользователи могут воспользоваться информационными услугами ИКС СН напрямую или с помощью пользовательских приложений. При этом компоненты пользовательских услуг обычно объединяются в пакеты, чтобы создать для конкретного пользователя требуемую сложную услугу или предоставить доступ к нескольким приложениям. Спектр информационных и связных услуг, которые обычно обеспечиваются в рамках современных ИКС СН, достаточно широк. При этом он может динамически меняться вместе с изменением доступных ресурсов [37].

В целом, ИКС СН составляет совокупность баз данных (БД), средств обработки информации, взаимодействующих ТКС и множество терминалов пользователей. При этом доступ к информационным ресурсам ИКС СН реализуется посредством услуг нового типа – инфокоммуникационных услуг. Предполагается, что именно они будут преобладать в перспективных ИКС СН уже в ближайшем будущем [37].

К основным технологическим особенностям, отличающим инфокоммуникационные услуги от услуг связи, можно отнести следующие [37]:

- инфокоммуникационные услуги оказываются на прикладном уровне модели OSI, в то время как услуги связи предыдущего поколения предоставляются на транспортном и сетевом уровнях OSI;
- стандартизация инфокоммуникационных услуг ведется на основе стандартов OSE/RM (Open System Environment / Reference Model) и ISO/IEC TR 14252, которые существенно расширяют и дополняют модель OSI в части детализации прикладного уровня [38];
- большинство инфокоммуникационных услуг предполагает наличие клиентской и серверной частей, при этом клиентская часть реализуется оборудованием пользователя, а серверная – на специальном выделенном узле ИКС, называемом узлом служб;
- инфокоммуникационные услуги, как правило, предполагают передачу мультимедийной информации, которая характеризуется высокими скоростями передачи и асимметричностью входящего и исходящего информационных потоков;
- для предоставления инфокоммуникационных услуг, зачастую, необходимы сложные многоточечные топологические конфигурации сетевых соединений;
- для инфокоммуникационных услуг характерно разнообразие прикладных протоколов и возможностей по управлению услугами со стороны пользователя;
- для идентификации пользователей инфокоммуникационных услуг, как правило, используется дополнительная адресация в рамках данной инфокоммуникационной услуги.

Обобщенная информационная архитектура перспективной ИКС СН представлена на рис. 1.12.

Особенностью интеграции сервиса оказания информационных услуг пользователям в ИКС СН является то, что существенно возрастет роль систем управления как услугами, так и сетью. Для реализации функций управления создаются службы MNS (Network Management System), которые обеспечивают рациональные режимы функционирования сетей, распределенное планирование, управление и контроль сетевых элементов и ресурсов. Функции службы MNS описываются специальной моделью (рекомендации МСЭ-Т серии X.700, стандарт ISO 7498-4), которая определяет функции управления, виды услуг сетевой службы, предоставляемые для управления, а также структуру управляющей информации и протоколы, определяющие ее транспортировку по сети [39].

В соответствии с моделью ISO 7498-4, управление сетью обеспечивается через локальное управление всеми элементами, входящими в сеть. Модель ISO 7498-4 охватывает следующие основные функции управления [39]:

- базовые протоколы технологии IP;
- маршрутные протоколы;
- протоколы групповой рассылки;
- протоколы повышения устойчивости маршрутизации;

- протоколы и технологии обеспечения качества обслуживания;
- протоколы обеспечения безопасности.

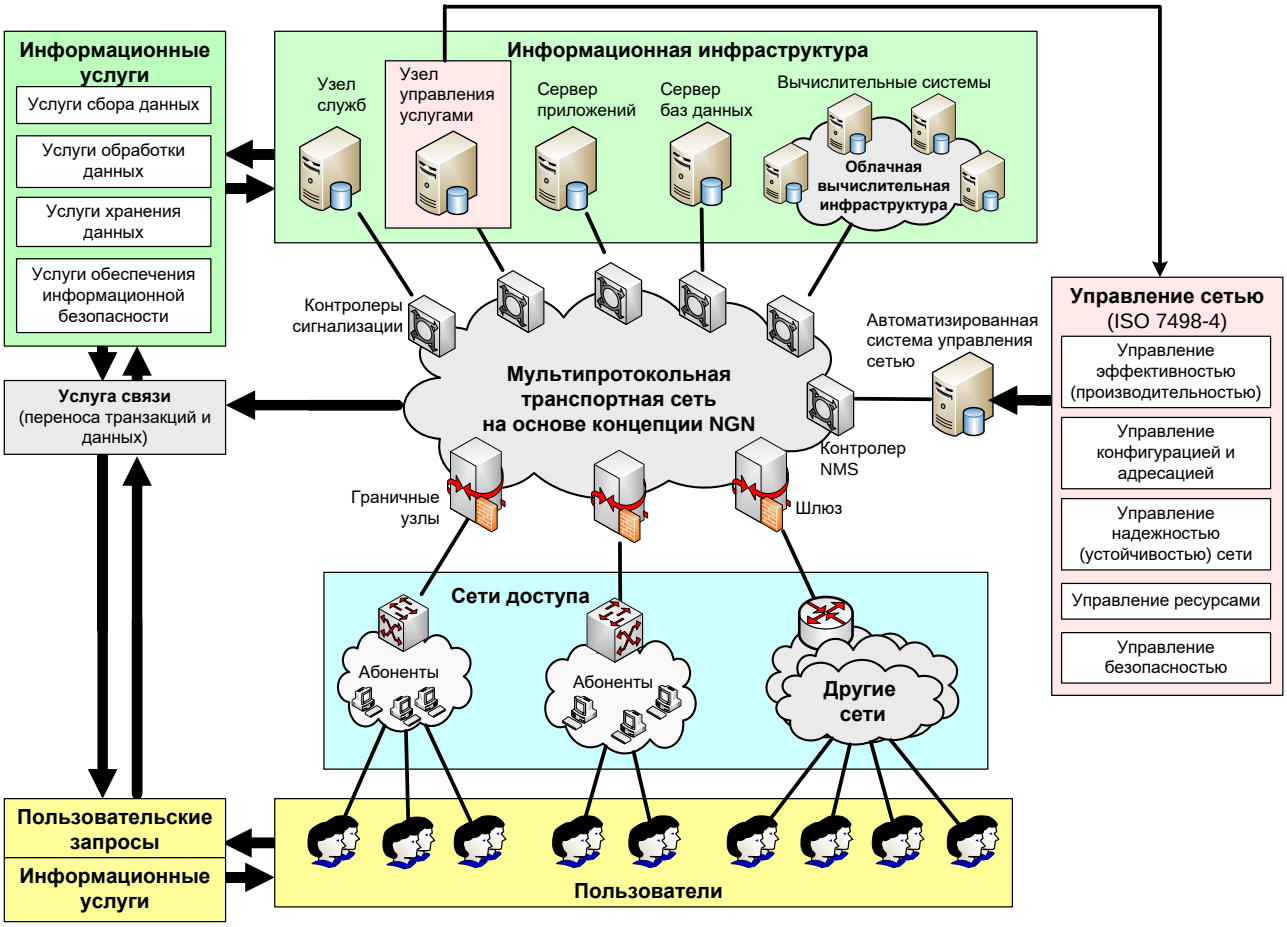

Рис. 1.12. Обобщенная архитектура перспективной ИКС СН

Подробные сведения о реализации процессов управления в сети в соответствии с моделью ISO 7498-4, а также о современных протоколах мониторинга и управления сетью представлены в работе [39].

1.3. Основные протоколы и технологии системы связи специального назначения

Как было показано выше, одной из основных тенденций развития СС СН является массовое использование в составе СС СН коммерческих протоколов и технологий. Опишем технологии функционирования СС СН и взаимодействие отдельных ТКС в ней более подробно.

При описании технологии СС СН целесообразно протоколы и технологии разбить на несколько основных групп:

- технологии физического и канального уровня;
- базовые протоколы технологии IP;
- протоколы маршрутизации;
- протоколы и механизмы поддержки качества обслуживания;
- протоколы групповой пересылки данных;

- протоколы повышения устойчивости маршрутизации и доставки пакетов;
- протоколы обеспечения безопасности.

Ниже рассмотрены особенности реализации и функционирования протоколов этих основных групп в ТКС входящих в состав СС СН, в соответствии с их применением в коммерческих СС ОП, как это представлено в работах [35, 61, 69, 71-74, 381].

1.3.1. Базовые технологии физического и канального уровня

Технологии канального и физического уровня существенно меняются в зависимости от используемой физической среды передачи, рода связи, технологий отдельных ТКС, а также рассматриваемого эшелона СС СН.

Для стационарных ТКС в составе наземного эшелона СС СН можно указать приблизительные типовые варианты использования физических сред, сигналов, информационного и помехоустойчивого кодирования, протоколов доступа к среде передачи для базовых транспортных технологий: PDH, SDH, OTH и Gigabit Ethernet (см. таблица 1.1) [13, 70-73, 336-337, 381].

Таблица 1.1 – Типовые технологии физического и канального уровня, используемые в стационарных ТКС наземного эшелона СС СН [70-73, 336-337]

Технология	Физическая среда	Используемые сигналы	Линейное кодирование	Помехоустойчивое кодирование	Технология доступа / мультиплексирования
PDH (E1)	Радио (ТРРЛ)	2FSK, 4FSK	По стандарту G.703	код Витерби, FEC, PC, БЧХ	TDM, FDM
PDH (E1…E4)	Радио (РРЛ)	BPSK, QPSK, 8PSK, 2FSK, 4FSK, 4QAM…1024QAM	По стандарту G.703	код Витерби, FEC, PC, БЧХ	TDM, FDM, CDMA, OFDM, COFDM
PDH (E1…E4)	Проводные линии связи (UTP, STP)	PCM (по стандарту G.703)	AMI, B8ZS, B6ZS, HDB3, CMI (по стандарту G.703)	FEC	TDM
SDH (STM-1)	Проводные линии связи (UTP, STP)	PCM (по стандарту G.703)	CMI	BPI	TDM
SDH (STM-1, STM-4)	Радио (РРЛ)	BPSK, QPSK, 8PSK, 2FSK, 4FSK, 4QAM…1024QAM	NRZ	код Витерби, FEC, BPI	TDM, OFDM, COFDM
SDH (STM-1…STM-256)	ВОЛС (SMF, MMF)	PCM	NRZ	BPI	TDM, WDM, CWDM, DWDM, HDWDM
OTH	ВОЛС (SMF, MMF)	PCM	–	FEC, PC	TDM, WDM, CWDM, DWDM, HDWDM
Gigabit Ethernet	ВОЛС (SMF, MMF)	PCM	NRZ	CRC	CSMA/CD, MPCP, EoT, PON

Особенностью стационарных ТКС наземного эшелона СС СН является то, что подавляющая их часть развернута на физической инфраструктуре ВОЛС, использующих различные варианты WDM-уплотнения оптических каналов. В случае отсутствия физической инфраструктуры на основе ВОЛС, узлы связи подключаются к ТКС с использованием технологий РРЛ (в некоторых случаях – ТРРЛ).

Для сетей авиационной радиосвязи в составе воздушного эшелона СС СН сложно указать какие-то конкретные стеки протоколов или варианты типовых технологических решений. Это связано с тем, что авиационное радиосвязное оборудование в гораздо меньшей степени стандартизировано на физическом и канальном уровнях по сравнению с оборудованием стационарных ТКС наземного эшелона СС СН. Вместе с тем, на физическом и канальном уровне в воздушном эшелоне уже получили широкое распространение отдельные технологии, которые учитываются в «режиме обратной совместимости» в новых радиосредствах авиационного базирования. Типовые технологии физического и канального уровня, широко используемые в авиационных радиосетях воздушного эшелона СС СН, представлены в таблице 1.2. Дополнительные сведения о технологических решениях в области авиационной радиосвязи, представлены в работах [92, 338-354].

Таблица 1.2 – Типовые технологии физического и канального уровня, используемые в радиосетях воздушного эшелона СС СН [92, 338-354]

Классы излучений	Используемые сигналы	Линейное кодирование*	Помехоустойчивое кодирование	Технология доступа / мультиплексирования
A1, A3, A3E, F1, F1B, F3, J3E, H3E, G1B, G3E, R3E, J7D, ППРЧ	ASK, 2FSK, 4FSK, BPSK, QPSK, 8PSK, *n*-QAM	AMI, B8ZS, B6ZS, HDB3, CMI, NRZ, NRZI	Витерби, РС, БЧХ	TDM, FDM, CSMA/CA, MF-TDM

Примечание:
*Определяется производителем оборудования.

Технологии спутниковой связи космического эшелона СС СН, преимущественно основаны на известных стандартах VSAT, DVB-S/S2, DVB-RSC. Дополнительной особенностью радиосредств ССС в составе СС СН является активное применение широкополосных сигналов (ШПС) с большой базой, а также режима ППРЧ в интересах повышения помехоустойчивости связи в космическом эшелоне. Типовые технологии физического и канального уровня, используемые в радиосетях космического эшелона СС СН, представлены в таблице 1.3.

Более полные сведения о технологиях физического и канального уровня космического эшелона СС СН представлены в работах [355-360, 382, 383].

Таблица 1.3 – Типовые технологии физического и канального уровня, используемые в радиосетях космического эшелона СС СН [355-360, 382, 383]

Технологии связи	Используемые сигналы	Линейное кодирование*	Помехоустойчивое кодирование	Технология доступа / мультиплексирования
DVB-S/S2, DVB-RSC, VSAT, iDirect	BPSK, QPSK, OQPSK, 8PSK, FSK, GMSK, 16QAM, TCM, 16APSK, 32APSK, ШПС, ППРЧ	AMI, B8ZS, B6ZS, HDB3, CMI, NRZ, NRZI	код Витерби, код Галея, РС, БЧХ, LDCP	TDMA, FDMA, MF-TDMA, DAMA, Aloha, S-Aloha, R-Aloha

Примечание:
*Определяется производителем оборудования.

1.3.2. Базовые протоколы технологии IP

К базовым протоколам технологии IP относятся, как собственно протоколы IPv4 или IPv6, так и протоколы, обеспечивающие их функционирование – Internet Control Message Protocol (ICMP), Address Resolution Protocol (ARP), Dynamic Host Configuration Protocol (DHCP). Эти базовые протоколы, как правило, поддерживаются всеми устройствами сетевого уровня.

Протоколы IPv4 или IPv6 определяют ряд основополагающих параметров и механизмов сетевого уровня. К ним относятся [70]:

- формат IP-пакета;
- сетевая адресация;
- фрагментация дейтаграммы на составные части;
- защита дейтаграммы от зацикливания;
- адрес протокола транспортного уровня, которому предназначена дейтаграмма.

Протокол ICMP используется для передачи сообщений об ошибках и о других исключительных ситуациях, возникших при передаче трафика, например, если запрашиваемая услуга связи недоступна, или маршрутизатор не отвечает. ICMP является отдельным протоколом для IPv4 и встроенным в IPv6 [70].

Протокол ARP используется для получения адреса канального уровня MAC по известному адресу IP. Протокол ARP является отдельным для IPv4 и встроенным в IPv6 [70].

Протокол DHCP используется для динамической настройки параметров узлов сети, в частности, для получения динамического адреса узла. При отсылке данных DHCP использует сервис транспортного уровня UDP [70].

В СС СН, построенных в соответствии с концепцией NGN на основе технологии IP/MPLS, к базовым протоколам также нужно отнести протокол MPLS. Этот протокол обеспечивает создание виртуальных каналов в IP-сети, присвоение IP-пакетам специализированных меток и последующую передачу их по виртуальным каналам с использованием технологии быстрой коммутации по меткам. Кроме указанных функций, протокол MPLS поддерживает механизмы оптимизации и управления трафиком для обеспечения высокого QoS.

1.3.3. Протоколы маршрутизации

К протоколам маршрутизации в СС СН относят протоколы обмена служебной информацией, обеспечивающие построение сетевыми устройствами таблиц маршрутизации, которые в дальнейшем используются для поиска кратчайших путей передачи трафика между узлами сети.

Различают статическую и динамическую маршрутизацию. Статическая маршрутизация в СС СН используется маршрутизаторами в сетях доступа для тех случаев, когда имеется единственный маршрут доставки пакетов. Кроме того, она используется для работы в сетях на основе технологий коммутации каналов (таких как PDH, SDH, OTH), где из-за наличия постоянных соединений функционирование протоколов динамической маршрутизации невозможно. Во всех остальных случаях, как правило, в СС СН используется динамическая маршрутизация [56-58].

Протоколы динамической маршрутизации функционально разделяются на [70]:

- протоколы «внутреннего шлюза» (Interior Getaway Protocol – IGP);
- протоколы «наружного шлюза» (Exterior Getaway Protocols – EGP).

Протоколы IGP используются внутри отдельных ТКС, которые с точки зрения сетевого уровня являются автономными системами (областями) маршрутизации в составе СС СН. Основная задача протоколов IGP – автоматическое объединение маршрутизаторов, принадлежащих одной области и связанных каналами связи, в единую сеть. Маршрутизаторы рассылают и используют полученную служебную информацию для построения таблиц маршрутизации с заданным критерием эффективности. Протоколы IGP характеризуются полным представлением структуры сети, принадлежащей конкретной ТКС.

К протоколам группы IGP относятся следующие протоколы [70]:

- протоколы на основе оценки состояния каналов (OSPF, IS-IS и др.);
- дистанционно-векторные протоколы (RIP, RIPng, IGRP, EIGRP и др.).

В ТКС на основе IP наибольшее распространение получили протоколы RIP, RIPng (для IPv6) и OSPF. В составе ТКС, которые построены на оборудовании компании Cisco, могут использоваться протоколы IGRP или EIGRP. В ТКС на основе технологии IP/MPLS используется протокол установления и поддержания соединений PNNI, в котором поиск кратчайших путей реализован через протокол OSPF. В дальнейшем, после установления соединений, передача IP трафика в них производится путем назначения меток и быстрой коммутации по ним на основе протокола MPLS.

В качестве протоколов IGP также используют сервисные протоколы, обеспечивающие перенос сообщений об изменении топологии сетей от сторонних областей маршрутизации между граничными устройствами своей области маршрутизации. К данным протоколам относятся: IBGP, MP BGP [70].

Протоколы EGP используются при обмене маршрутной информацией между отдельными ТКС внутри СС СН, а также между ТКС отдельного функционального назначения или между ТКС различных уровней государственного или военного управления. Они обеспечивают перенос в СС СН сообщений об

изменении топологии сетей отдельных ТКС, а также обмен информацией о достижимости ТКС из других автономных областей маршрутизации. Их задача – автоматическое информирование о достижимых сетях через межсетевой интерфейс. Протоколы EGP еще называют протоколами маршрутизации на основе политик, так как они позволяют определить условия использования сервисов доступа и осуществлять перенос трафика через транзитные ТКС внутри СС СН. К широко распространенным протоколам EGP относятся протоколы группы BGP (Border Gateway Protocol): IBGP, BGP4 и EBGP, при этом наибольшее распространение в СС СН получил протокол BGP4. Протоколы межсетевого взаимодействия ТКС внутри СС СН из группы EGP-протоколов и протокол DNS являются основными протоколами, обеспечивающими объединение отдельных ТКС в единую СС СН (это справедливо как для СС СН и СС ОП, так и для глобальной сети Интернет, в целом) [70].

1.3.4. Протоколы групповой пересылки данных

К протоколам групповой пересылки (multicast) относятся протоколы, обеспечивающие эффективную доставку данных по принципам «от одного – ко многим» и «от многих – ко многим» между абонентами СС СН, объединенными в группу. Здесь под эффективностью понимают минимизацию трафика, или числа пакетов, которые должны дублировать маршрутизаторы при передаче их через сеть. К данным протоколам в СС СН относятся [56-58, 70]:

- протокол IGMP (Internet Group Management Protocol) – протокол управления групповой передачей данных в сетях, основанных на протоколе IP, и сходный по принципам функционирования с протоколом ICMP. Этот протокол используется маршрутизаторами для объединения сетевых устройств в группы;
- семейство протоколов PIM (Protocol Independent Multicast) – использует данные функционирующих в IP сети протоколов маршрутизации для построения путей, проведения групповой рассылки пакетов и многоадресной маршрутизации. Довольно часто протоколы семейства PIM используются совместно с протоколом DVMRP;
- протокол дистанционно-векторной многоадресной маршрутизации DVMRP (Distance Vector Multicast Routing Protocol) – предназначен для маршрутизации пакетов внутри автономных областей маршрутизации в IP сетях при групповой рассылке сообщений;
- протокол MARS (Multicast Address Resolution Server) – сервер разрешения широковещательных адресов, предназначенный для организации соединений «точка-группа».

Наиболее важными для служебных целей маршрутизации в СС СН являются протоколы семейства PIM (PIM-DM, PIM-SM, PIM-SSM). Они позволяют строить множество кратчайших путей от источника к множеству получателей с определением места каждого маршрутизатора в составе пути и дублированием рассылки пакетов другим маршрутизаторам или группе абонентов, являющихся получателями.

1.3.5. Протоколы повышения устойчивости маршрутизации и доставки пакетов

К данной группе относят протоколы, которые обеспечивают повышение устойчивости функционирования базовых протоколов СС СН. В своем большинстве эти протоколы призваны обеспечить устойчивость маршрутизации в условиях резко меняющейся интенсивности трафика – его так называемой «пульсации».

К протоколам повышения устойчивости маршрутизации и доставки пакетов можно отнести [56-58]:

- протоколы группы STP (Spanning Tree Protocol): RSTP, PVSTP, MSTP, которые позволяют обнаруживать петли в транспортных сетях на основе технологии Ethernet, блокировать их, а в случае отказа каналов сети – использовать эти петли для формирования резервных направлений связи;
- протокол IP-Trunk, служащий для объединения отдельных IP-соединений на сетевом уровне со сходными требованиями к QoS в магистрали соединений (так называемые «транки»);
- протокол резервирования сетевых ресурсов RSVP (Resource ReSerVation Protocol), который позволяет резервировать сетевые ресурсы маршрутизаторов для обеспечения QoS в соответствии с моделью IntServ;
- протоколы технологий CES (Circuit Emulation Service) TDMoIP и TDMoP, использующиеся для обеспечения эмуляции типовых каналов цифровой иерархии PDH и SDH при передаче трафика через пакетные сети;
- протоколы виртуализации маршрутизаторов HSRP (Hot Standby Router Protocol) и VRRP (Virtual Router Redundancy Protocol), предназначенные для повышения надежности основного маршрутизатора сети (маршрутизатора по умолчанию) путем объединения группы маршрутизаторов в один виртуальный маршрутизатор и назначения им общего IP-адреса;
- протокол резервирования маршрутизаторов в территориально распределенных сетях E-Trunk, который обеспечивает резервирование и обмен служебной информацией между граничными маршрутизаторами ТКС, а при выходе из строя одного из них – перенаправление трафика на другой граничный маршрутизатор.

1.3.6. Протоколы и технологии обеспечения качества обслуживания

Для обеспечения требуемого качества обслуживания трафика на сетевом и транспортном уровнях СС СН используются стандартные архитектуры обеспечения QoS.

К основным архитектурам обеспечения QoS в СС СН относятся [74]:

- *обслуживание с максимальными усилиями, но без гарантий* (Best Effort) – архитектура, использующая механизм выделения дополнительной пропускной способности без использования «тонких» способов управления трафиком;
- *интегрированное обслуживание* (IntServ – Integrated Service) – архитектура, использующая протокол RSVP для резервирования сетевых ресурсов в каналах и в узлах сети на этапе установления соединения, после чего обеспечивающая QoS во всем соединении путем контроля соблюдения QoS во всех промежуточных элементах сети;
- *дифференцированное обслуживание* (DiffServ – Differentiated Service) – архитектура, использующая классификацию трафика по классам обслуживания CoS (Class of Service) на границе сети, определение требуемого QoS для каждого класса обслуживания с последующим распределением сетевых ресурсов сети с целью гарантировать QoS допущенного в сеть трафика. Данная архитектура поддерживает управление формированием трафика (классификация пакетов, маркировка, управление интенсивностью и др.) и управление политикой обслуживания (распределение сетевых ресурсов, приоритетность отбрасывания пакетов и т.д.).

Основной архитектурой обеспечения качества обслуживания в СС СН, как правило, является DiffServ. Для обеспечения высокой эффективности архитектуры DiffServ ее должны поддерживать все сетевые устройства СС СН.

Архитектура DiffServ поддерживает три базовых класса обслуживания трафика [74]:

- трафик «реального времени» (Real Time – RT);
- приоритетный трафик (Priority – P);
- неприоритетный трафик (Non priority – NP).

Для трафика класса RT поддерживается четыре приоритета абонентов, для классов P, NP – по три приоритета абонентов.

Зачастую производители оборудования для СС СН вводят собственные маркировки классов обслуживания, учитывающие особенности передачи трафика специальных абонентов (сообщения различной степени важности, уровень подчиненности абонента, условия мирного/военного времени и т.д.), однако при этом, как правило, берутся за основу классы обслуживания, принятые в технологиях DiffServ для MPLS.

Сетевые устройства, поддерживающие DiffServ, используют различные входные/выходные очереди для трафика различных классов обслуживания, а также основанные на этих классах приоритетные механизмы обслуживания очередей CQ (Class based Queuing) [74]:

- механизмы предотвращения перегрузок очередей;
- механизмы управления очередями;
- механизмы ограничения скорости.

К наиболее распространенным механизмам предотвращения перегрузок очередей относятся [74]:

- раннее обнаружение перегрузок в очередях – RED (Random Early Detection);
- взвешенное раннее обнаружение перегрузок в очередях – WRED (Weighted Random Early Detection);
- адаптивное раннее обнаружение перегрузок в очередях – ARED (Adaptive Random Early Detection);
- многоуровневое раннее обнаружение перегрузок в очередях – MRED (Multilevel Random Early Detection);
- сброс пакетов в конце очереди (Tail Drop);
- случайный сброс пакетов (Random Drop);
- отказ в приеме пакетов, переполняющих очередь (Drop Front on Full) и др.

К наиболее распространенным механизмам управления очередями относятся [74]:

- «первый пришел – первый обслужился» – FIFO (First In – First Out);
- приоритетное обслуживание в очереди – PQ (Priority Queuing);
- настраиваемые очереди – CQ (Custom Queuing);
- справедливое обслуживание в очереди – FQ (Fair Queuing);
- взвешенное справедливое обслуживание в очереди – WFQ (Weighted Fair Queuing);
- взвешенное справедливое обслуживание в очереди на основе классов – CBWFQ (Class-Based Weighted Fair Queuing);
- приоритетное взвешенное справедливое обслуживание в очереди на основе классов (PQ-CBWFQ – Priority Class-Based Weighted Fair Queuing), обеспечивающее низкую задержку обслуживания очереди – LLQ (Low Latency Queuing);
- круговой циклический алгоритм обслуживания очереди – RR (Robin Round);
- взвешенный круговой циклический алгоритм обслуживания очереди – WRR (Weighted Robin Round);
- дефицитный взвешенный круговой циклический алгоритм обслуживания очереди – DWRR (Deficit Weighted Robin Round) и др.

К механизмам ограничения скорости относятся [74]:

- технологии ограничения трафика (Traffic Policing) – отбрасывает пакеты, создающие перегрузку;
- технологии выравнивания трафика (Traffic Shaping) – помещает пакеты, создающие перегрузку, в буфер и обслуживает их при снижении нагрузки;

При реализации обоих этих технологий могут использоваться алгоритмы:

- алгоритм «дырявого ведра» (Leaky Bucket) – основан на том, что независимо от количества трафика, поступающего в буфер, выборка трафика из буфера ведется с постоянной скоростью (по аналогии с дырявым ведром);

- алгоритм «маркерного ведра» (Token Bucket) – основан на том, что выборка трафика из буфера регулируется виртуальными маркерами, каждый из которых соответствует передаче определенного объема трафика.

Граничные маршрутизаторы в каждой автономной области маршрутизации (т.е. в каждой ТКС в составе СС СН) должны поддерживать классификацию трафика (Traffic Classification), а также сопоставление интенсивности поступающего трафика и достаточности доступных сетевых ресурсов для его обслуживания. При этом при передаче трафика СС СН через сегменты СС ОП, в граничных маршрутизаторах трафик может перемаркироваться. Вариантом такой перемаркировки может быть [381]:

- RT (Real Time) – трафик, критичный к задержкам и джиттеру;
- BC (Business Critical) – трафик, критичный к полосе пропускания;
- BE (Best Effort) – трафик терпимый к потерям и задержкам.

Для контроля перегрузок и выполнения ограничений по интенсивности и структуре трафика в своей области маршрутизации (в отдельной ТКС) граничные маршрутизаторы должны использовать вышеуказанные механизмы предотвращения перегрузок и управления очередями, а также механизмы ограничения скорости поступления трафика. При невозможности обслуживания трафика в конкретной области маршрутизации (в отдельной ТКС в составе СС СН) поступающий трафик либо сбрасывается, либо дополнительно буферизируется с пометкой «Best Effort». Данная пометка означает, что трафик будет обслужен без гарантий обеспечения требований к QoS, но с максимальными усилиями со стороны сетевых устройств по его соблюдению. Для технологии MPLS трафик IP инкапсулируется, а класс MPLS маркируется заново [74].

В СС СН модель DiffServ может быть реализована совместно с моделями «Best Effort» и IntServ, коорые в этом случае дополняют друг друга. Например, в отсутствие трафика определенного класса, в отведенной ему полосе обслуживания может передаваться трафик «Best Effort». В сетях с ограниченными ресурсами дополнительно могут реализоваться функции RSVP протокола, позволяющие выборочно зарезервировать сетевые ресурсы под соединение для специальных абонентов с высоким приоритетом. Функционал RSVP запросов относится к модели IntServ [74].

1.3.7. Протоколы безопасности

Для СС СН определены следующие функции безопасности [75]:

- аутентификация (обеспечивает аутентификацию абонентов и пользователей по общению, а также аутентификацию источника данных в СС СН);
- управление доступом (позволяет ограничить режимы взаимодействия сетей и обеспечить сокрытие информации о структуре и особенностях построения как отдельных ТКС, так и СС СН в целом, путем фильтрации пакетов и сообщений на сетевом, транспортном и прикладном уровнях модели OSI по соответствующим группам служебных атрибутов, извлекаемых из этих сообщений);

- конфиденциальность и целостность трафика в режимах как с установлением соединения, так и без него (достигается криптографической защитой данных на физическом, канальном, сетевом, транспортном и прикладном уровнях модели OSI);
- целостность соединений с обеспечением и без обеспечения возможности их восстановления (позволяет обнаруживать изменения данных, передаваемых в рамках уже установленных соединений);
- безотказность или защита от отказа источника или получателя сообщений (основано на использовании криптографических протоколов, которые обеспечивают надежные гарантии отправки и доставки сообщений для их источника/получателя).

К протоколам СС СН, которые обеспечивают эти функции безопасности, относятся [42, 56-58, 75]:

- протоколы формирования защищенных соединений (PPP – на канальном уровне, IPsec – на сетевом, AH, ESP – на транспортном, PPTP – на сеансовом, SSL, TLS – на представительном, S/MIME – на прикладном);
- протоколы фильтрации IP-адресов (IP-filtering) и протоколы доступа на основе списков (ACL-lists), реализованные в маршрутизаторах и в межсетевых экранах;
- протоколы авторизации при обмене динамической маршрутной информацией между маршрутизаторами (например, такие как: IS-IS authorization и EBGP authorization);
- протоколы виртуальных каналов и сетей VPN;
- технологии формирования анонимных защищенных сетей на основе «луковой» и «чесночной» маршрутизации.

Кроме того, в состав СС СН, как правило, включаются специализированные закрытые протоколы шифрования, управления ключевой информацией, электронной цифровой подписи, авторизации, а также другие протоколы и технологии, направленные на обеспечение информационной безопасности в СС СН. Более развернутое описание защищаемых ресурсов и требований к протоколам безопасности с учетом специфики СС СН представлено в работе [42].

1.3.8. Межсистемные протоколы и интерфейсы

Обобщая вышеуказанное, на основе анализа работ [27-30, 35, 56-58, 74], возможно сформулировать перечень основных протоколов и интерфейсов, которые будут заимствованы из сферы связи гражданского назначения для использования в составе СС СН.

К таким коммерческим протоколам, получившим широкое распространение в СС СН, относятся следующие.

1) Базовые протоколы СС СН, обеспечивающие передачу данных в сетях:

- IPv4;
- IPv6;
- MPLS;
- ICMP;

- ARP;
- DHCP.

2) Протоколы маршрутизации:

а) для внутрисетевой маршрутизации (IGP):

- RIP;
- OSPF, OSPF-TE;
- IS-IS;
- PNNI;
- IGRP (EIGRP) – в оборудовании компании Cisco;

б) для межсетевой маршрутизации (EGP):

- BGP 4;
- EBGP.

3) Протоколы групповой рассылки:

- IGMP;
- PIM (PIM-DM, PIM-SM, PIM-SSM);
- DVMRP.

4) Протоколы повышения устойчивости маршрутизации:

- STP, RSTP, PVSTP, MSTP;
- IP-trank, E-trank;
- RSVP;
- TDMoIP, TDMoP;
- HSRP, VRRP.

5) Протоколы и технологии обеспечения качества обслуживания трафика:

а) архитектуры обеспечения качества обслуживания:

- DiffServ;
- IntServ;
- Best Effort;

б) механизмы предотвращения перегрузок в очередях DiffServ:

- RED, WRED, ARED, MRED;
- сброс пакетов в конце очереди (Tail Drop);
- случайный сброс пакетов (Random Drop);
- отказ в приеме пакетов, переполняющих очередь (Drop Front on Full);

в) механизмы управления очередями DiffServ:

- FIFO;
- PQ;
- CQ;
- FQ, WFQ, CBWFQ;
- LLQ;
- RR, WRR, DWRR;

г) механизмы ограничения скорости DiffServ:

- ограничение трафика (Traffic Policing);
- выравнивание трафика (Traffic Shaping);

д) механизмы ограничения скорости IntServ:

- RSVP.

6) Протоколы обеспечения безопасности:

- технологии формирования защищенных каналов (PPP, IPsec, AH, ESP, PPTP, SSL, TLS, S/MIME);
- IP-фильтрация и листы доступа ACL;
- авторизация при обмене маршрутнй информацией;
- технологии «луковой» и «чесночной» маршрутизации;
- другие специализированные протоколы.

К интерфейсам ТКС в составе СС СН, которые также широко заимствуются из сферы гражданской связи, относятся следующие.

1) На физическом уровне модели OSI.

а) консольные порты:

- RS-232;
- USB;

б) интерфейсы пакетной сети:

- Ethernet 100 BASE-SX (FX) – многомодовые и одномодовые ВОЛС;
- Ethernet 100 BASE-TX, IEEE 802.3u;
- Ethernet 1000 BASE-T;
- Ethernet 1000 BASE-LX (LX10, SX, EX, ZX) – многомодовые и одномодовые ВОЛС;
- E1 G.703/G704, E2, E3, E4;
- STM-1, STM-4, STM-16, STM-64, STM-256;
- OTU1, OTU2, OTU3, OTU4;
- интерфейсы систем связи предыдущих поколений;

в) протоколы управления:

- SNMP v.3;
- XML;
- SSH;
- Telnet;
- CLI;
- FTP, TFTP.

2) На канальном уровне модели OSI:

- IEEE 802.3 (Ethernet);
- PPP, MP-PPP;
- кадры Jumbo;
- авторизация и аутентификация (PAP/CHAP, 802.1X, RADIUS);
- L2 VPN;
- резервирование (LAG);
- Ethernet OAM;
- QoS DiffServ;
- STP, RSTP, PVSTP, MSTP.

3) На сетевом уровне модели OSI:

- IPv4, IPv6;
- MPLS;
- BGP4;

- балансировка трафика IP;
- многоадресные протоколы (PIM, DVMRP);
- авторизация и аутентификация (RADIUS).

4) На транспортном уровне модели OSI:

а) обеспечение качества обслуживания средствами IntServ:

- RSVP;

б) обеспечение качества обслуживания средствами DiffServ:

- выравнивание трафика (Shaping Traffic) на входящих и исходящих интерфейсах;
- регулирование трафика на исходящих интерфейсах (буферирование LLQ, WFQ, CB WFQ, WRED и т.д.);
- управление доступом (контроль доступа на базе адресов IP, портов TCP/UDP, полей TOS/DSCP и т.д.);
- как «прозрачный» перенос полей ToS и DSCP, так и их переопределение;
- ICMP;
- резервирование VRRP.

1.4. Проблемные вопросы обеспечения устойчивости систем связи специального назначения на современном этапе их развития

Анализ тенденций развития СС СН, проведенный на основе работ [10, 18, 19, 21, 27-30, 32-35, 46-49, 56-58, 61], показал, что модернизация СС СН, в первую очередь, направлена на замену устаревших технологий новыми, в интересах достижения более высокой пропускной способности и повышения набора услуг связи, предоставляемых абонентам. При этом для решения задач повышения пропускной способности СС СН используются наработанные подходы и технологии из сферы коммерческой связи. Вместе с тем, при выборе протокольно-технологического базиса СС СН следует руководствоваться не только необходимостью кардинального повышения пропускной способности и расширения спектра услуг связи, но и специфическими требованиями, предъявляемыми к СС СН, а именно по устойчивости функционирования в мирное время, угрожаемый период и военное время. Последнее обуславливает целый ряд дополнительных требований, вытекающих из необходимости обеспечивать своевременный, скрытный и достоверный обмен информацией между пунктами управления и абонентами СС СН в условиях ведения противником разведки, радиоэлектронной борьбы (РЭБ) и информационного противоборства (ИПб).

Можно выделить четыре основных вида преднамеренных дестабилизирующих воздействий, которые потенциально будут иметь место при функционировании СС СН в угрожаемый период и в военное время:

1) воздействия на узловое оборудование и проводные линии связи СС СН обычным оружием;
2) воздействия на радиоканалы и радиосети в составе СС СН средствами радиоэлектронного подавления (РЭП), воздействия на узловое обору-

дование СС СН средствами функционального поражения электромагнитным излучением (ФП ЭМИ);

3) информационно-технические воздействия (ИТВ) на узловое телекоммуникационное оборудование и на протоколы связи СС СН;
4) информационно-психологические воздействия (ИПВ) на пользователей и обслуживающий персонал СС СН.

Вышеуказанные воздействия определяют особые требования к формированию технологической основы СС СН, которые не всегда соблюдаются в условиях перехода сетей СС СН к пакетной коммутации, активному заимствованию коммерческих протоколов связи, а также использованию в качестве сегментов СС СН незащищенных подсетей СС СП.

Рассмотрим более подробно возникающие проблемные вопросы, связанные с текущими тенденциями развития СС СН.

1.4.1. Проблемные вопросы, обусловленные переходом систем связи специального назначения от технологий коммутации каналов к технологиям коммутации пакетов

Дестабилизирующие воздействия на объекты физического уровня путем применения высокоточного оружия (ВТО), средств РЭП и ИТВ будут отображаться на сетевом уровне OSI в виде следующих эффектов [3, 24]:

- снижение качества каналов;
- снижение скоростей информационного обмена;
- возникновение одиночных и групповых ошибок приема;
- сбои тактовой синхронизации функционирующего в синхронном режиме оборудования, приводящие к потере данных;
- перерывы в связи;
- сбой или выход из строя телекоммуникационного оборудования сетевых узлов;
- сбой или некорректное функционирование протоколов связи в сети.

Анализ, проведенный в работах [21, 29, 43], показал, что, например, ВС США при построении своей СС СН исходят из того, что в военное время при массированном применении средств РЭП единственным видом связи может остаться передача данных в КВ-диапазоне. Однако, информационный обмен по КВ-радиоканалу в режиме пакетной коммутации возможен только с применением протоколов AX.25/FX.25 (так как вероятность ошибочного приема бита в канале может достигать значений $10^{-3} – 10^{-2}$, а в отдельных случаях и $5 \cdot 10^{-2}$), в то время как протоколы IP предусматривают работу только по каналам связи среднего качества и выше.

Широко используемые в транспортных сетях технологии коммутации каналов, такие как PDH и SDH, так же не способны обеспечить устойчивость связи. Так, сети PDH, ввиду отсутствия возможностей по развитой маршрутизации информационных потоков не способны обеспечить должной оперативности реконфигурации сети. Сети SDH, несмотря на развитый методический аппарат построения устойчивых топологических решений на основе колец и схем резервирования каналов, в результате дестабилизирующего воздействия против-

ника подвержены недопустимо частым сбоям синхронизации, приводящим к необратимой потере данных.

Недостатки сетей PDH/SDH/OTH следуют из самого принципа их псевдостатического построения, когда проистекающие в них процессы статичны и фактически не позволяют реконфигурировать транспортную сеть в режиме реального времени. Использование технологии автоматически коммутируемых транспортных сетей ASON/ASTN, применительно к существующим сетям PDH/SDH/OTH, лишь частично решает вопросы обеспечения структурной устойчивости. По сути, технология ASON/ASTN предоставляет только сервис автоматической реконфигурации PDH/SDH/OTH сетей, не решая при этом задачи повышения оперативности управления ресурсами сетей.

Однако и пакетные транспортные сети эффективны только при условии, что они поддерживают динамическое равновесие при обеспечении QoS абонентов и приспосабливаются к быстро изменяющимся условиям. Так, в сетях с использованием пакетных технологий IP/MPLS длительность процессов перемаршрутизации находится в секундном диапазоне [82], что на порядки превышает аналогичные показатели для SDH-сетей, в которых гарантированная длительность переключения на резервную конфигурацию обеспечивается механизмами физического уровня и составляет 50 мс.

Кроме того, сама возможность маршрутизации, порождает специфическую уязвимость пакетных сетей, источником которой являются сбои в протоколах маршрутизации [55, 77]. При этом в силу особенностей работы протоколов маршрутизации подобные нарушения могут распространяться по сети лавинообразно. Именно на это обстоятельство обращает внимание в своем отчете [78] проблемная группа по NGN Консультативного комитета по связи для национальной безопасности при Президенте США. Рекомендация МСЭ-Т G.1000 [79] также указывает, что использование сетей и служб на основе IP выдвигает целый ряд проблем, таких как отсутствие апробированных, надежных и масштабируемых технологий для решения целого ряда задач, в частности, быстрого восстановления связности на сетевом уровне после серьезных сбоев.

Еще одной проблемой пакетных сетей является широкий диапазон значений джиттера времени передачи пакетов. Даже если отправитель посылает пакеты в сеть через равные интервалы времени, получатель может получать их через промежутки времени, отличающиеся на десятки миллисекунд. Это происходит из-за того, что задержки передачи отдельных пакетов существенно зависят от загруженности маршрутизаторов и каналов связи, от структуры пакетного трафика, а также от длины маршрута, состоящего из разного числа промежуточных приемо-передач. Корректировку джиттера отдельных пакетов, который образуется из-за разности во времени передачи отдельных пакетов по сети, приходится производить в оконечном оборудовании данных. При этом сети PDH/SDH/OTH являются детерминированными – задержка распространения сигнала в них мала и постоянна, синхросигнал передается вместе с данными, а на джиттер наложены строгие ограничения, что позволяет добиться передачи информации в режиме времени, близком к реальному. Так, для этих сетей изменения задержки должны лежать в пределах от 40 нс до 18 мкс, в то время как

в пакетных сетях, где данные передаются с использованием таких протоколов как IP и MPLS, изменения задержки передачи пакетов могут составлять десятки миллисекунд [29].

В работе [29] указывается, что проблема джиттера пакетов якобы решается путем использования технологий CES (Circuit Emulation Service) для передачи потоков E1, E3 и STM-1 через пакетные сети при сохранении высоких требований к синхронизации. Технология CES основана на алгоритмах адаптации и инкапсуляции трафика сетей PDH и SDH в пакеты и последующей его передачи через пакетную сеть (технология TDMoIP или TDMoP). Однако, технология CES, решая проблемы обеспечения передачи потоков PDH и SDH, а также обеспечивая синхронизацию этих сетей через пакетные сети, не гарантирует постоянный уровень джиттера передачи пакетов, в которые инкапсулируются потоки E1, E3 и STM-1.

Проблемой пакетных сетей также являются гигантские пульсации трафика. Если коэффициент пульсации телефонного трафика имеет значения от 5 до 15, то при передаче данных данный коэффициент составляет значения сотни тысяч [80]. Однако, технологии PDH/SDH/OTH в моменты роста трафика вообще не способны динамически предоставить большую полосу пропускания, а в моменты спада не в состоянии использовать свободную полосу.

1.4.2. Проблемные вопросы, обусловленные использованием в системах связи специального назначения канальных и сетевых ресурсов, арендуемых у коммерческих операторов связи

Как показано в работах [10, 35] одной из основных тенденций развития СС СН является использование ресурсов СС ОП. В результате, СС СН начинает критически зависеть от ресурсов СС ОП, особенно в период нарастания военной угрозы и в военное время.

В соответствии с оценками результатов учений, проводимых министерством обороны (МО) США с целью выяснения потребности ВС в телекоммуникационных услугах в случае одновременного участия ВС США в вооруженных конфликтах высокой интенсивности на двух театрах военных действий (ТВД), суммарная пропускная способность линий связи, включая ССС, принадлежащие МО США, а также арендуемых коммерческих линий дальней связи как космических, так и наземных (подводных), должна составлять не менее 50 Гбит/с. При этом ежегодный прирост потребностей МО США в среднем прогнозируется на уровне 15%. По другим оценкам, потребность МО США в телекоммуникационных услугах в 2010 г. для обслуживания двух ТВД достигала 100 Гбит/с. Основной объем передаваемой информации приходится на данные тактической разведки (изображения, видео и данные для планирования боевых действий), которые составят около 57% от всего объема трафика. Следующий основной потребитель телекоммуникационных ресурсов на ТВД – АСУ войсками и оружием, на долю которых приходится около 31% трафика. Обмен информацией с высшим военно-политическим руководством государства составляет 4%, а на информацию боевого обеспечения приходится 3%. Обмен

информацией с системами управления и оповещения стратегического звена составит 1%, прочий объем трафика – 4%. На долю ТВД будет приходиться около 48% от общего объема трафика, циркулирующего в ВС США. Трафик с ТВД на континентальную часть США составит 35%, а передача информации с территории США на ТВД – около 17% [10].

Однако распределение потоков информации в значительной степени зависит от условий и характера ведения боевых действий. Для США, которые рассматривают, прежде всего, конфликты на удаленных ТВД, существенно возрастает значение ССС. Анализ распределения используемых линий связи для информационного обеспечения абонентов (таблица 1.4) показывает, что именно на них придется основная нагрузка при передаче информации.

Таблица 1.4 – Вклад отдельных родов связи (по объемам передаваемой информации) в управление на удаленных ТВД [68]

Спутниковая связь	более 50-60%
Радиорелейная связь	до 18-22%
Тропосферная связь	до 12%
КВ-, УКВ-радиосвязь	до 5-6%

Требования к пропускной способности спутниковых линий связи в случае участия ВС США одновременно в двух вооруженных конфликтах на разных ТВД по состоянию, например, на 2010 г., составляла 4 Гбит/с.

Таким образом, большая часть трафика ВС США при участии в конфликтах на удаленных ТВД будет приходиться на арендуемые системы незащищенной широкополосной спутниковой связи [33].

Оценки для ВС РФ, выполненные в работе [35], показывают, что для обеспечения функционирования СС СН группировки войск на ТВД при максимальном использовании каналов стационарной СС ОП (в качестве которой выступает единая система электросвязи (ЕСЭ) РФ) необходимо использование 30 стационарных узлов связи территориальной бригады связи и более 700 узлов связи операторов ЕСЭ РФ (количество узлов связи зависит от размера территории военного округа), из которых выделяется более 700 потоков Е1. При этом собственная транспортная сеть СС СН обеспечивает пропускную способность до 200 Мбит/с, а ЕСЭ РФ – 1600 Мбит/с. В ходе проведения операции скорость арендуемых цифровых трактов может достигать 4 Гбит/с. Ввиду того, что узлы СС ОП обладают низкой живучестью, дополнительно развертывается полевая сеть связи, обеспечивающая пропускную способность до 300 Мбит/с. В результате, зависимость СС СН от арендуемого ресурса СС ОП составляет [35]:

- по возможностям привязки на местности до 96%;
- по пропускной способности до 96% (после развертывания полевой сети связи – до 95%).

Итоговая зависимость СС СН ВС РФ от арендуемого ресурса транспортных сетей СС ОП составляет:

- до развертывания полевой системы связи около 72%;
- после развертывания полевой системы связи до 60%.

В случае реализации противником воздействий по объектам СС ОП, системы управления войсками могут потерять возможность передавать до 60% информации.

Таким образом, СС ОП из вспомогательного компонента СС СН превращается в ее основополагающую, но наименее устойчивую часть. При этом, информационное обеспечение ведения боевых действий на ТВД становится критически зависимым от арендованного ресурса коммерческих ССС для ВС США и арендованных ресурсов ЕСЭ РФ – для ВС РФ.

Использование в качестве сегментов СС СН арендуемых каналов и сетей СС ОП, а также массовое использование в СС СН коммерческих протоколов связи делает СС СН уязвимой к атакам средств РЭП и ИТВ. Эти атаки (особенно атаки ИТВ) могут проводиться на СС СН через сетевые сегменты, общие с СС ОП, так как СС ОП, как правило, подключены к глобальной информационно-телекоммуникационной сети Интернет. При этом, как показано выше, среди коммерческих сетевых протоколов, основанных как на коммутации каналов (PDH/SDH/OTH, ASON/ASTN), так и коммутации пакетов (IP, IP/MPLS), и широко используемых в СС СН, не отработаны механизмы защиты от воздействий ИТВ и РЭП, а также механизмы быстрого восстановления сети после сбоев.

1.4.3. Проблемные вопросы, обусловленные построением систем связи специального назначения в соответствии с концепцией NGN

Одной из основных проблем при построении СС СН, в соответствии с концепцией NGN, является устойчивость сетевой инфраструктуры. При этом, как отмечается в работе [55], обеспечение устойчивости в сетях NGN является более сложной задачей, чем обеспечение устойчивости сетей предыдущего поколения, основанных на коммутации пакетов или каналов.

Во-первых, в основе сетей NGN лежат IP-сети. В связи с этим все проблемные вопросы, связанные с недостаточно быстрым восстановлением этих сетей, рассмотренные выше, являются актуальными и для сетей NGN.

Во-вторых, для сетей предыдущего поколения, основанных на коммутации каналов, основной нормируемой составляющей надежности является готовность узла, требование к которой задавалось в виде $K_Г$=0,99999 [81]. При переходе к NGN вместо традиционного узла коммутации используется гибкий коммутатор (softswitch). Возникает комплекс из большого числа отдельных устройств (контроллеров, шлюзов, серверов). Все они имеют высокую надежность: значение коэффициента готовности каждого из них, как обычно заявляют производители, составляет все те же «пять девяток». Однако для выполнения функций узла коммутации необходима совместная работа нескольких таких устройств, поэтому результирующая надежность будет равняться произведению их коэффициентов готовности, т. е. в итоге она оказывается более низкой [55].

В-третьих, еще более важным фактором, негативно влияющим на устойчивость сетей NGN, является централизация управления процессами обслуживания вызовов. Критическим элементом сети NGN становится контроллер

шлюзов или сервер вызовов (softswitch в узком понимании этого термина). При этом, один такой контроллер или сервер управляет многими шлюзами, поэтому его отказ может привести к прекращению работы сети на большой территории. Подобная ситуация негативно влияет на устойчивость сети. Неслучайно ведущие производители оборудования NGN предусматривают возможность резервирования контроллеров шлюзов, в том числе с географическим разнесением. Однако многие операторы связи подобное резервирование при проектировании своих сетей не используют из соображений экономии [55].

1.4.4. Проблемные вопросы управления системой связи специального назначения, построенной в соответствии с концепцией NGN

Вышеуказанные проблемы обеспечения устойчивости СС СН в условиях дестабилизирующих воздействий при ограничениях на качество обслуживания специальных абонентов предъявляют жесткие требования к системе управления связью. Несмотря на то, что концепция NGN предусматривает стандартные подходы к управлению услугами и средствами связи, она не рассматривает условия перманентных дестабилизирующих воздействий как повседневные условия функционирования сети. Таким образом, переход СС СН к концепции NGN требует существенной доработки принципов и подходов NGN в части управления связью применительно к СС СН. Исследование этой тематики проводилось в работах К.Е. Легкова [36-41], А.Н. Буренина [40, 41], Н.А. Соколова [51], А.Е. Давыдова [31].

Система управления связью является важнейшей подсистемой СС СН. В настоящее время практически во всех современных СС СН и СС ОП развитых стран развернуты центры управления связью с той или иной степенью автоматизации, выполняющие необходимые функции, связанные с мониторингом, контролем состояния и изменением конфигурации удаленных сетевых устройств. Большинство этих систем управления строится по иерархическому принципу, позволяющему обеспечивать более гибкое, эффективное и оперативное управление за счет сегментирования СС СН на более мелкие элементы – региональные и местные сети, а также отдельные ТКС. При этом разработка систем централизованного управления связью является довольно сложной наукоемкой задачей, в рамках которой необходимо объединить разнотипное оборудование различных производителей, которое имеет различный функционал, принципы и возможности управления [31].

Необходимо отметить, что в этом смысле задачи управления, решаемые в СС СН и в СС ОП, идентичны и в равной степени актуальны. Однако существенные различия в подходах и методах решения задач управления проявляются в уровне наблюдаемости, управляемости, а также в своевременности принятия решений применительно к СС СН. Это обусловлено большим количеством специальных требований, предъявляемых к СС СН по сравнению с СС ОП, таких как устойчивость, боевая готовность, мобильность, управляемость, разведзащищенность и др. Степень выполнения этих специфичных тре-

бований зависит от подходов к управлению связью, которые, в свою очередь, определяются жесткими требованиями к оперативности управления [31].

Оперативность управления определяет время реакции системы связи на различные виды изменений, вносимых в состав, конфигурацию или режимы функционирования СС СН. В свою очередь характеристики оперативности управления во многом определяются, с одной стороны, уровнем автоматизации процессов управления связью, а с другой – принципами организации управления, закладываемыми при разработке телекоммуникационного оборудования [31].

Так, недостаточный уровень автоматизации процессов управления некоторых СС СН уже сегодня стал их ключевой проблемой, решить которую можно только путем перехода от повсеместно применяемого принципа управления отдельно взятым сетевым элементом, предложенного ведущими производителями телекоммуникационного оборудования, к принципу единого сетевого управления, который рассматривает СС СН как совокупность различных сетевых ресурсов. Такое изменение принципов управления обусловлено не только необходимостью выполнения жестких требований по оперативности управления и автоматизацией связных процессов, но и изменениями самих телекоммуникационных технологий [31].

В большинстве работ под управлением связью понимается настройка оборудования первичной сети с последующим наложением на транспортную сеть различного рода услуг связи. В условиях, когда перечень услуг исчисляется единицами, такой подход подразумевает лишь выделение абоненту номерной емкости и определенного сетевого ресурса. При переходе СС СН к концепции NGN резко увеличивается номенклатура предоставляемых услуг связи и их персонализация. В результате, ведущее значение приобретает не настройка отдельных средств связи, а именно персонализация услуг, в зависимости от которых формируется сначала телекоммуникационная инфраструктура СС СН, а затем на ее основе формируется единый пул сетевых ресурсов, который должен использоваться с высокой эффективностью, а также с учетом условий дестабилизирующего воздействия на элементы телекоммуникационной инфраструктуры [31].

Вместе с тем, использование в составе СС СН сегментов СС ОП и коммерческого оборудования связи не позволяет в полной мере реализовать указанные подходы к управлению связью. Разработчики СС СН вынуждены использовать подходы к управлению, принятые ведущими производителями коммерческого сетевого оборудования, ввиду их широкого использования в составе СС СН. В основу управления коммерческим сетевым оборудованием, согласно современным стандартам по NMS, среди прочего включается [39]:

- управление неисправностями;
- управление конфигурацией;
- управление ресурсами.

Как правило, эти функции управления реализуются в отношении одного или группы однотипных устройств в соответствии с моделью «агент – сервер». При этом управление осуществляется с помощью ввода соответствующих ко-

манд вручную или с помощью графического интерфейса пользователя и предполагает наличие сервисной инженерной службы, которая в случае отказа или сбоя средства связи диагностирует и конфигурирует его удаленно [31].

Условия функционирования СС СН характеризуются динамическим воздействием преднамеренных дестабилизирующих факторов, выходом из строя элементов СС СН вследствие их огневого или радиоэлектронного поражения, динамическим переходом на дополнительные каналы связи, подключением дополнительных сетевых ресурсов в условиях блокировки имеющимися средствами ИТВ. Такие условия функционирования вступают в противоречие с поэлементным автоматизированным управлением СС СН. В таких условиях никакая сервисно-инженерная служба не сможет обеспечить требуемый уровень оперативности и эффективности управления. То есть такой подход противоречит современным требованиям к управлению, так как [31]:

- не отвечает требованиям управляемости, оперативности, мобильности и боевой готовности;
- требует содержания многочисленной сервисно-инженерной службы;
- не отвечает критериям обеспечения информационной безопасности;
- «размывает» функционал и зоны ответственности при предоставлении услуг связи специализированным абонентам (оператор СС СН должен осуществлять полное наблюдение и управление сетью, в то время как сегменты СС ОП в составе СС СН оказываются ограниченно наблюдаемыми и недоступными для управления).

Одним из путей решения задачи создания автоматический системы управления связью СС СН, предложенным в работе [31], является создание единой базы сетевых ресурсов СС СН и автоматической системы управления этими ресурсами. При этом подразумевается, что база сетевых ресурсов и система управления ими будут размещаться в доверенной зоне СС СН и частично реплицироваться в территориальные центры управления отдельных ТКС. Единая база сетевых ресурсов будет содержать агрегированную информацию обо всех сетевых элементах и их конфигурации, в том числе [31]:

- сетевые адреса и параметры;
- профили безопасности и межсетевых экранов (на основе политики безопасности как для уровня должностных лиц, так и для устройств и сетей);
- параметры протоколов обеспечения качества обслуживания, приоритетной обработки трафика и выделения полос пропускания;
- параметры протоколов маршрутизации и протоколов обеспечения функционирования виртуальных наложенных сетей;
- временные параметры и критерии блокировки и разблокировки пользователей, устройств и сетей;
- частоты и режимы работы радиосредств;
- документацию под соответствующую конфигурацию сети и др.

Создание такой базы сетевых ресурсов является одной из подзадач управления связью и осуществляется либо заранее, либо в режиме реального времени при наличии автоматической системы управления связью. Впослед-

ствии, каждый сетевой элемент СС СН получает только необходимую ему информацию. При таком централизованном подходе к управлению СС СН конфигурации всех сетевых элементов будут семантически согласованы и централизованно оттестированы на корректность введения тех или иных настроек, во избежание конфликтных ситуаций и ошибок, связанных с человеческим фактором, целенаправленными действиями внутреннего нарушителя и др. [31].

Таким образом, задача разработки системы управления связью для СС СН является актуальной научной и технической задачей. При этом, принципы и технологии управления, используемые для СС ОП, не приемлемы для управления СС СН ввиду того, что последние функционируют в условиях перманентных дестабилизирующих воздействий. Одним из вариантов решения задачи управления СС СН является создание единой базы сетевых ресурсов СС СН и автоматической системы управления этими ресурсами.

Выводы по первой главе

Система связи специального назначения – это система связи, функционирующая в интересах государственной и военной систем управления. В условиях перехода этих систем управления к сетецентрическим принципам построения, развитие СС СН идет по пути кардинального наращивания пропускной способности и количества связных и информационных услуг, оказываемых пользователям. При этом анализ развития СС СН позволяет выявить следующие основные тенденции по ее технологическому построению:

- переход от иерархического принципа построения СС СН к децентрализованой сетевой структуре, которая в большей степени соответствует современным требованиям к системам государственного и военного управления, а также условиям ведения боевых действий, характеризующимся высокой динамикой развития и мобильностью ее участников;
- отказ от построения СС СН на основе отдельной связной инфраструктуры и переход к построению СС СН на основе гибридного подхода, когда отдельные сегменты СС ОП национальных и региональных операторов связи, а также сегменты глобальных сетей используются в качестве элементов транспортной инфраструктуры СС СН;
- отказ от использования в СС СН закрытых и специализированных протоколов связи и максимально широкое использование для построения элементов СС СН коммерческих протоколов и технологий, применяемых в гражданской сфере связи и телекоммуникаций.

Использование в качестве сегментов СС СН арендуемых каналов и сетей СС ОП, а также массовое использование в СС СН коммерческих протоколов связи делает СС СН уязвимой к атакам средств РЭП и ИТВ. Эти атаки (особенно атаки ИТВ) могут проводиться на СС СН через сетевые сегменты, общие с СС ОП, так как СС ОП, как правило, подключены к глобальной информационно-телекоммуникационной сети Интернет. При этом, среди коммерческих сетевых протоколов, которые широко используются в СС СН, не отработаны механизмы защиты от воздействий ИТВ и РЭП, а также механизмы быстрого восстановления после сбоев.

2. Описательная модель систем и средств дестабилизирующих воздействий

Система связи специального назначения в процессе своего функционирования подвергается дестабилизирующим воздействиям, направленным на снижение ее устойчивости. Анализ работ [10, 63] позволил предложить классификацию дестабилизирующих воздействий на СС СН, представленную на рис. 2.1. При этом необходимо отметить, что естественные и искусственные непреднамеренные дестабилизирующие воздействия на СС СН характерны для мирного времени. В военное время и в угрожаемый период эти воздействия дополняются преднамеренными искусственными дестабилизирующими воздействиями.

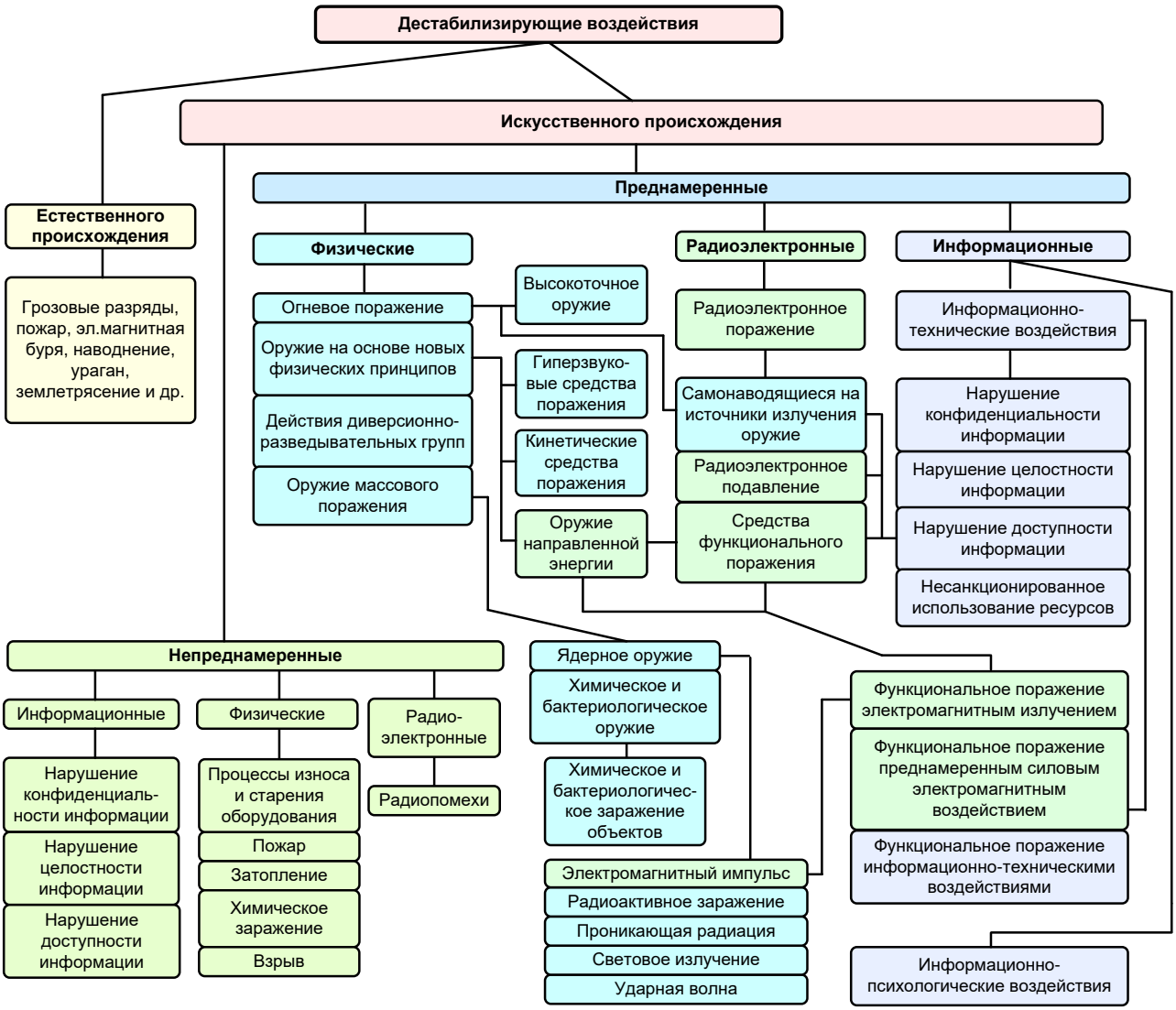

Рис. 2.1. Классификация дестабилизирующих воздействий

Анализ военных конфликтов рубежа XX-XXI веков, проведенный в работе [10], позволил выявить три основных типа основных преднамеренных дестабилизирующих воздействий, влияющих на СС СН:

1) физическое поражение элементов СС СН обычным оружием, а также оружием на новых физических принципах (рельсотроны, гиперзвуковые средства поражения);
2) воздействие на элементы СС СН средств РЭП, а также оружия на новых физических принципах, основанного на функциональном поражении электромагнитным излучением (средства создания мощных электромагнитных импульсов, излучатели направленной энергии, генераторы мощного электрического тока, лазерное оружие);
3) воздействие на элементы СС СН средств и способов ИТВ.

На основе анализа тенденций развития соответствующих средств и комплексов, а также перспективных разработок потенциального противника, далее сформированы описательные модели вышеуказанных дестабилизирующих факторов. При этом, данные модели, основанные на обобщении сведений из открытых источников, носят информационный характер и не претендуют на высокую точность и полноту. По авторскому замыслу, модели, представленные в данной монографии, должны дополняться и уточняться описательными моделями соответствующих средств воздействия, выпускаемые уполномоченными организациями в официальном порядке.

2.1. Общие подходы к применению дестабилизирующих воздействий на системы связи в современных вооруженных конфликтах

Анализ военных конфликтов, проведенный в работе [10], показал, что им свойственны следующие ключевые особенности в отношении задействуемых СС СН:

- подавляющее большинство элементов СС СН являются разведдоступными для средств радиоэлектронной разведки противника;
- заблаговременно вскрытые элементы СС СН являются объектами первоочередного поражения средствами ВТО, а вновь выявляемые элементы СС СН оперативно подавляются средствами РЭП или поражаются самонаводящимся на излучение оружием (СНИО);
- элементы СС СН, сопряженные с сегментами СС ОП, являются критически уязвимыми перед обеспечивающими и атакующими ИТВ.

Анализ [10] позволил сформировать обобщенную последовательность применения дестабилизирующих воздействий на СС СН, реализующуюся в современных военных конфликтах.

1) Большинство пунктов государственного и военного управления, а также узлов связи стратегического и оперативного звена, объектов критической информационной инфраструктуры вскрываются заблаговременно в мирное время, а также в период нарастания военной угро-

зы по результатам ведения агентурной, видовой и радиоэлектронной разведки.

2) В период нарастания военной угрозы активно реализуются ИПВ на лиц, принимающих решения в стратегическом звене управления государством, а также на весь личный состав ВС и сил обеспечения правопорядка. Активно ведется заброска диверсионно-разведывательных групп (ДРГ) в интересах подготовки и осуществления диверсий на объектах критической информационной инфраструктуры.
3) В этот же период активно используются обеспечивающие ИТВ, во-первых, для проведения компьютерной разведки в интересах вскрытия структуры и параметров критической информационной инфраструктуры, а во-вторых – для заблаговременного формирования уязвимостей в критической инфраструктуре, которые в дальнейшем будут использоваться атакующими ИТВ. Проведение этих ИТВ осуществляется как через сети СС ОП, так и участниками ДРГ, внедренными в персонал соответствующих объектов СС СН, – в отношении критической инфраструктуры СС СН, не сопряженной с СС ОП.
4) За 1-2 суток до начала военных действий наземными и воздушными комплексами РЭП создаются «беспокоящие» радиоэлектронные помехи для СС СН и СС ОП. По результатам анализа реакции средств связи из состава СС СН на помехи вскрываются их резервные частоты, а также предположительные схемы организации связи на военное время.
5) За 6-8 ч до начала военных действий осуществляется массированная постановка радиоэлектронных помех средствам радиосвязи СС СН; средствам теле- и радиовещания СС ОП. Ведется массированное применение атакующих ИТВ на: доступные для ИТВ элементы СС СН; критические телекоммуникационные ресурсы СС ОП; сети сотовых операторов связи; шлюзы сопряжения СС СН – СС ОП; на другие объекты критической информационной инфраструктуры, которые доступны через сети СС ОП.
6) В момент начала военных действий (Ч+0) реализуется глобальный массированный удар средствами ВТО длительностью до 1-2,5 ч. В рамках данного удара средствами ВТО поражаются: пункты управления и соответствующие им узлы связи системы государственного и военного управления в стратегическом и оперативном звене; критические стационарные телекоммуникационные узлы СС ОП; средства телевизионного и радиовещания СС ОП.
7) После завершения глобального удара (на Ч+4…12 ч) проводится доразведка объектов СС СН. Против вновь вскрываемых мобильных и пространственно-распределенных сетей радиосвязи используются средства и комплексы РЭП, против стационарных узлов связи – средства СНИО.
8) Перспективной тенденцией поражения элементов СС СН, является использование оружия на новых физических принципах: гиперзвукового и кинетического оружия; оружия, основанного на поражении электро-

магнитным излучением. Данное оружие пока используется в военных конфликтах как экспериментальное, но уже в ближайшей перспективе ожидается увеличение доли этих типов оружия среди средств поражения, используемых против элементов СС СН.

Более подробная информация об особенностях применения ВТО, РЭП и ИТВ в военных конфликтах представлена в работе [10]. Обобщим тактико-технические характеристики (ТТХ) отдельных средств и комплексов, а также способов их применения в интересах формирования соответствующих описательных моделей.

2.2. Описательная модель систем и средств физического поражения

В рамках представленной модели сформированы обобщенные ТТХ основных средств физического поражения объектов СС СН, как штатно применяемых в современных войнах, так и являющихся перспективными разработками:

- средства поражения ВТО;
- средства поражения СНИО;
- гиперзвуковые средства поражения;
- средства кинетического поражения (рельсовые пушки – рельсотроны).

Данные ТТХ сформированы путем анализа военных действий в локальных конфликтах на рубеже XX-XXI вв. и перспективных направлений развития соответствующих видов вооружений, представленных в работах [10, 88].

В связи с низкой вероятностью применения в современных военных конфликтах оружия массового поражения (ОМП), в том числе и ядерного, данное оружие в составе описательной модели не рассматривалось. Также в состав описательной модели не включены артиллерийские средства поражения, ввиду их широкого описания в уже существующих моделях, а также действия ДРГ, ввиду сложности их формально-описательного представления.

2.2.1. Высокоточное оружие

С начала 2000-х гг. технически развитые страны активизировали исследования в области придания своим вооруженным силам способности к высокоточному воздействию на цели в кратчайшие сроки и на большие дальности с использованием набора ударных средств в обычном (неядерном) оснащении. Для достижения поставленной цели развернуты работы по созданию новейших типов высокоточных мобильных стратегических неядерных вооружений – систем ВТО. Главным отличительным свойством ВТО является реализованный принцип «выстрел – поражение». Дальнейшее развитие ВТО идет в направлении «интеллектуализации» данного оружия путем придания ему способности «распознавать» цели, в том числе на поле боя и в условиях помех, а при воздействии по крупным целям – выбирать наиболее уязвимое место цели для ее поражения [10].

Высокоточное оружие – вид оружия, оснащенного системой управления и обеспечивающего поражение цели одним боеприпасом в пределах дальности своего действия с высокой вероятностью.

Как правило, под ВТО подразумеваются типы обычных вооружений и средств их доставки [10]:

- крылатые ракеты воздушного, наземного и морского базирования;
- разведывательно-ударные комплексы, реализующие принцип «обнаружил – выстрелил – поразил»;
- артиллерийские управляемые и самонаводящиеся боеприпасы (снаряды и мины, в том числе кассетные);
- управляемые авиабомбы (УАБ), в том числе модульной конструкции (с ракетным ускорителем);
- управляемые ракеты типа «воздух-поверхность»;
- межконтинентальные баллистические ракеты в обычном снаряжении, а также управляемые на траектории, в том числе с кассетными боеголовками и самонаводящимися боевыми элементами.

Общая классификация ВТО приведена на рис. 2.2.

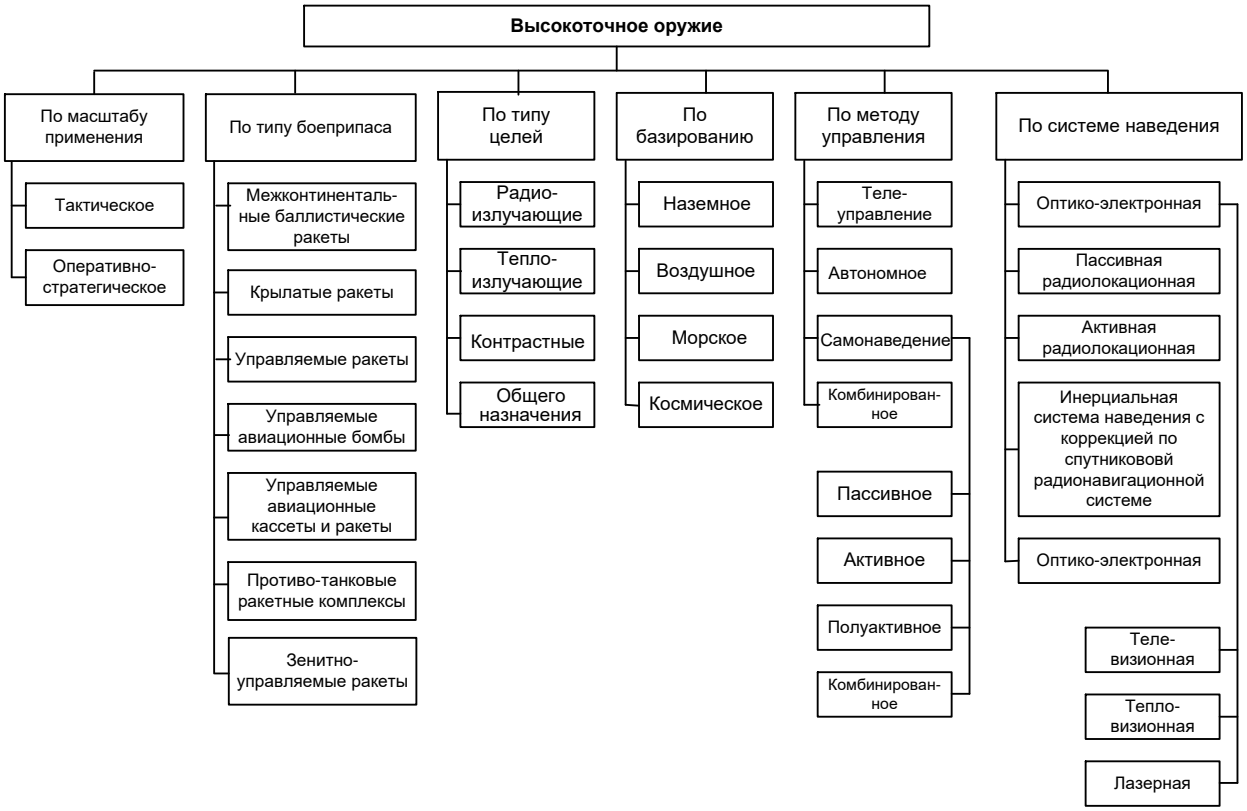

Рис. 2.2. Общая классификация ВТО [10]

Наиболее распространенным видом ВТО являются крылатые ракеты, основными достоинствами которых являются следующие возможности [10]:

- возможен пуск с земли, воды и воздуха на удалении в несколько тысяч километров от границы территории и зон ПВО противника;
- благодаря малой эффективной площади рассеивания и способности осуществлять полет с огибанием рельефа местности на малых и пре-

дельно малых высотах снижается эффективность огневого поражения крылатых ракет средствами ПВО противника;
- большая масса боевой части крылатой ракеты определяет ее значительную разрушительную мощь.

Стационарные узлы связи СС СН, как правило, поражаются крылатыми ракетами или УАБ морского или воздушного базирования. Объекты СС СН в тактическом звене управления поражаются ВТО, ориентированным на применение против радиоизлучающих целей.

В качестве обобщенного типового средства ВТО наземного базирования можно рассматривать тактические ракеты, обладающие следующими характеристиками:
- дальность действия: 80-300 км;
- варианты боевой части: кассетная (на 95-300 боевых элементов или на 6-12 самоприцеливающихся элементов), фугасная (до 150 кг), осколочно-фугасная (до 270 кг);
- точность поражения цели: 10-20 м;
- система наведения: комбинированная (автономная инерциальная система наведения с коррекцией по сигналам СРНС).

Прототипами данного типового средства являются ракеты СВ США: MGM-140, MGM-164, MGM-168 и GMLRS для тактических ракетных комплексов ATACMS и M142 HIMARS, соответственно.

В качестве обобщенного типового средства ВТО морского базирования можно рассматривать крылатую ракету, обладающую следующими характеристиками [10, 407]:
- дальность действия: 500-3000 км;
- скорость полета: 3000-5600 км/ч;
- масса боевой части: 300-450 кг;
- количество вариантов, для перенацеливания: 15-20;
- точность поражения цели: 10-35 м;
- система наведения: комбинированная (автономная инерциальная система наведения с коррекцией по электронной карте местности и по сигналам СРНС с возможностью выбора маршрута полета и поражаемой цели по командам оператора);
- профиль полета: полет на малой высоте с огибанием рельефа местности, с контролем местоположения по СРНС;
- система распознавания целей – автономная оптико-электронная, с дополнительной ТВ-камерой для передачи изображения цели оператору.

Прототипом данного типового средства являются крылатые ракеты ВМС США: BGM-109 Tomahawk; Fasthawk.

В качестве обобщенного типового средства ВТО воздушного базирования можно рассматривать крылатую ракету, обладающую следующими характеристиками [10]:
- дальность действия: 300-1000 км;
- скорость полета: 700-1000 км/ч;
- масса боевой части: 300-450 кг;

- точность поражения цели: ± 3 м;
- система наведения: комбинированная (автономная инерциальная система наведения с коррекцией по сигналам СРНС, с возможностью выбора маршрута полета и поражаемой цели по командам оператора);
- система распознавания целей: автономная радиолокационная или оптико-электронная.

Прототипом данного типового средства является крылатая ракета AGM-158 JASSM, стоящая на вооружении ВВС США.

Еще одним распространенным средством ВТО являются УАБ. При сопоставимой точности применения УАБ выигрывают у крылатых ракет в массе боевой части (до 900 кг), но проигрывают им в дальности применения. Дальность применения УАБ обычно составляет до 30 км, планирующих УАБ и УАБ модульной конструкции – до 80 км.

В последнее время, как один из вариантов операции по завоеванию стратегического превосходства военными экспертами рассматривается массированный глобальный удар межконтинентальными баллистическим ракетам (МБР) и баллистическими ракетами подводных лодок (БРПЛ) в обычном оснащении по основным командным пунктам и важным объектам военного значения.

В качестве типовой МБР шахтного базирования можно рассматривать ракету, обладающую следующими характеристиками [10, 405]:

- дальность действия: 9000-13000 км;
- средняя скорость полета: 23100 км/ч;
- точность поражения цели: ± 200 м;
- траектория полета: баллистическая, апогей траектории – 1000-1300 км.

Прототипом данной типовой МБР является МБР ВС США LGM-30G Minuteman III.

В качестве обобщенной БРПЛ можно рассматривать ракету, обладающую следующими характеристиками [10, 406]:

- дальность действия: 7800-11300 км;
- средняя скорость полета: 23000 км/ч;
- точность поражения цели: ± 90-120 м;
- траектория полета: баллистическая, апогей траектории – 1000-1300 км.

Прототипом данной типовой БРПЛ является БРПЛ ВС США UGM-133A Trident II (D5).

Основные научно-технические программы в области развития ВТО направлены на увеличение скорости и дальности полета боеприпаса, повышение точности стрельбы, снижение радиолокационной и оптической заметности, а также использование комбинированных систем наведения, которые позволяют применять оружие в любых метеорологических условиях. Особое внимание уделяется оснащению ВТО различными типами боевых частей, в частности активно ведутся работы по созданию боеприпасов ВТО для поражения электромагнитным импульсом различных типов РЭС, а также боеприпасов, снаряженных наэлектризованной графитовой смесью для вывода из строя систем электроснабжения [9, 10].

Более полные сведения о средствах ВТО представлены в работах [10, 83-86].

2.2.2. Самонаводящееся на излучение оружие

Самонаводящиеся на излучение оружие (СНИО) – оружие с пассивной системой наведения по излучениям военной техники в диапазонах электромагнитных, оптических и акустических волн.

В настоящее время средства СНИО предназначены преимущественно для поражения радиолокационных станций (РЛС) комплексов ПВО. Однако, в настоящее время ведутся активные работы по приданию средствам СНИО определенной универсальности в части их применения против различных РЭС, в том числе и против средств радиосвязи, работающих на излучение.

Рассматривая ракеты AGM-88G AARGM-ER и ALARM как прототипы, можно сформировать ТТХ обобщенного типового средства СНИО воздушного базирования [9, 87]:

- дальность пуска: 80-300 км;
- скорость полета: до 2500 км/ч;
- масса боевой части: 50-70 кг;
- точность поражения цели: 7-9 м;
- система наведения: комбинированная (автономная инерциальная система наведения с коррекцией по сигналам СРНС);
- целеуказание: запись координат РЭС и его радиосигнального портрета в память перед пуском;
- система распознавания целей: автономное радиоэлектронное распознавание цели.

Необходимо отметить, что в настоящее время подавляющая часть средств СНИО размещается самолетах пилотируемой авиации, но тенденция развития этого типа оружия предполагает его размещение на БПЛА, которые смогут вести разведку и поражение РЭС в режиме «дежурство в воздухе» в том числе и в зоне действия комплексов ПВО В связи с этим ТТХ СНИО должны рассматриваться совместно с возможностями их перспективных носителей – БПЛА.

Рассматривая MQ-1 Predator, MQ-9 Reaper и RQ-4 Global Hawk как прототипы БПЛА можно сформировать ТТХ обобщенного БПЛА – носителя средств СНИО [10]:

- вариант боевого применения для обнаружения РЭС: дежурство в воздухе до 45 ч на высоте до 18 км;
- скорость полета: до 500 км/ч;
- дальность полета: до 6000 км;
- аппаратура разведки: единый интегрированный радиотехнический, оптико-электронный и инфракрасный комплекс;
- параметры разведки: обеспечивает получение радиолокационного и оптического изображения местности с разрешением до 0,3 м. За сутки может быть получено изображение площади 138 км^2 на расстоянии 200 км.

Более полные сведения о средствах СНИО представлены в работах [9, 87, 93, 404], а сведения о БПЛА – в работе [10].

2.2.3. Оружие на новых физических принципах

В настоящее время ведется активная разработка оружия на новых физических принципах, ориентированного на высокоэффективное физические поражение целей.

Оружие на новых физических принципах – средства вооруженной борьбы, поражающее действие которых основывается на использовании направленных высокоэнергетических излучений и полей, нейтральных или заряженных частиц, доводимых до объектов поражения, а также на других нетрадиционных или принципиально новых способах поражения.

К такому оружию можно отнести:

- гиперзвуковые средства поражения;
- кинетические средства поражения (на основе рельсотронов).

Сейчас данные типы оружия являются экспериментальными, при этом если гиперзвуковое оружие уже проходит опытную эксплуатацию в виде отдельных образцов вооружения, то разработка рельсотронов пока не вышла за пределы исследовательских лабораторий. Вместе с тем, в течение следующих 15-20 лет именно эти типы вооружения могут существенно изменить порядок применения средств физического поражения и вывести возможности огневого поражения объектов СС СН на принципиально новый уровень.

2.2.3.1. Гиперзвуковые средства поражения

Гиперзвуковые летательные аппараты (ГЗЛА), по мнению аналитиков, вне зависимости от дислокации, в перспективе, смогут достигать любой точки земного шара в течение одного часа и, таким образом, служить альтернативой МБР, оснащенным ядерными боеприпасами.

ГЗЛА – это летательный аппарат (как правило, ракета или отдельный боевой блок), способный разгоняться и маневрировать в атмосфере со скоростью, многократно превышающей скорость звука. Говоря о гиперзвуке, имеют ввиду долговременный полет в атмосфере со скоростями, превышающими 3-5 М (М – число Маха, равное скорости звука в атмосфере, которое составляет 331 м/с). Такая скорость давно доступна МБР, но они достигают ее только в космосе, в безвоздушном пространстве, на высотах, где отсутствует сопротивление воздуха и, соответственно, возможность аэродинамического маневрирования и управления полетом. Применительно к ГЗЛА речь идет об управляемом полете в атмосфере со скоростями 6-12 М [10].

Тематика ГЗЛА очень важна для развития ВТО, так как позволяет обеспечить ее высокие показатели по скорости, точности и скрытности. ГЗЛА, двигаясь в атмосфере, в плазменном облаке, будут максимально скрытными и сложно доступными для систем обнаружения ПВО и ПРО. Помимо сложности обнаружения, ГЗЛА чрезвычайно сложны для перехвата. Таким образом, ГЗЛА имеют ряд присущих только им особенностей, существенно затрудняющих решение задач по их обнаружению, сопровождению, опознаванию и поражению,

возложенных на средства системы ПВО-ПРО государства, против которого они будут применяться [10]:

- возможность использования диапазона высот от 25 до 140 км от земной поверхности;
- способность ГЗЛА осуществлять полет на ранее не достижимых для средств воздушно-космического нападения скоростях (от 6 до 15 М) как в атмосфере, так и за ее пределами – в околоземном космическом пространстве;
- использование смешанных трудно прогнозируемых траекторий полета к объекту поражения (аэродинамическая – на начальном этапе полета, эллиптическая – при полете в околоземном космическом пространстве, баллистическая – на конечном этапе полета во время атаки объекта поражения);
- сочетание в одном ГЗЛА боевых свойств, как аэродинамических средств воздушного нападения, так и космического аппарата;
- эффективность применения ГЗЛА, оснащенных боевыми частями в неядерном исполнении, по высокоточному поражению точечных стратегических целей, сопоставимо с эффективностью применения МБР с ядерной боевой частью.

Рассматривая такие экспериментальные образцы ГЗЛА как Х-47М2 «Кинжал», 3М22 «Циркон», Х-51А «Waverider», HTV-2, AHW и DF-ZF можно сформировать приблизительные обобщенные ТТХ перспективного гиперзвукового средства поражения:

- варианты базирования: наземное/морское, воздушное, космическое;
- варианты пуска: пуск с наземной/морской платформы; пуск с летательного аппарата; пуск с МБР, вышедшей в стратосферу или в ближний космос; пуск с космической платформы;
- скорость полета: 6-15 М (2-5 км/с);
- высота пуска/полета: от 25-40 км до 100-120 км;
- дальность полета ГЗЛА: 300-3000 км;
- дальность действия с учетом дальности полета носителя: для ГЗЛА наземного/морского базирования – 300-1000 км; для ГЗЛА воздушного базирования – 2000-3000 км; для ГЗЛА на МБР – 8000-12000 км; космического базирования – по всей поверхности Земли;
- масса боевой части: 200-400 кг;
- точность поражения цели: 5-10 м.

2.2.3.2. Средства кинетического поражения (рельсовые пушки)

Одним из перспективнейших средств кинетического поражения является рельсовая пушка (рельсотрон) – оружие, основанное на превращении электрической энергии в кинетическую энергию снаряда. В данном виде оружия для придания начальной скорости снаряду используется магнитное поле. То есть магнитное поле применяется как альтернатива взрывчатым веществам в огнестрельном оружии. При этом сообщенная снаряду кинетическая энергия ис-

пользуется непосредственно для поражения цели. Основными привлекательными особенностями данного оружия являются конструктивная простота средств поражения и достижение ими гиперзвуковых скоростей [10].

Считается, что главным преимуществом электромагнитных орудий, по сравнению с традиционными артиллерийскими установками, станет увеличенная до 64 МДж дульная энергия (для сравнения: дульная энергия корабельных артустановок: Мк45 – 4-18 МДж, AGS – 33 МДж) и, как следствие, высокая начальная скорость полета снаряда. Например, при стрельбе на максимальную дальность около 500 км для снаряда массой 20 кг расчетная начальная скорость полета оценивается в 2,5 км/с, а скорость встречи с целью – не менее чем в 1,5 км/с [10].

Ожидается, что сравнительно низкий уровень энергетических потерь снарядов при стрельбе на большие дальности будет достигаться прохождением значительной части их баллистической траектории вне плотных слоев атмосферы с максимальной высотой полета до 160 км. Высокие начальные скорости снарядов электромагнитных орудий позволят добиться существенных боевых преимуществ над современными образцами артиллерийского вооружения, важнейшими из которых являются [10]:

- малое подлетное время до цели, значительно снижающее время устаревания данных целеуказания и не позволяющее противнику принять меры эффективного противодействия;
- высокая поражающая способность бронебойных подкалиберных снарядов благодаря их значительной кинетической энергии;
- расширенные возможности уничтожения критичных по времени мобильных целей, а также высокозащищенных стационарных объектов.

Кроме того, ожидается, что отказ от применения взрывчатых веществ обеспечит при стрельбе существенное снижение показателей заметности в видимом, инфракрасном и акустическом диапазонах длин волн, а также позволит снизить на 30% силу отдачи и повысить взрывопожаробезопасность боевых кораблей и бронированных машин [10].

Основной и наиболее трудной технологической задачей при создании электромагнитных орудий в интересах вооруженных сил является разработка компактного мощного и энергоемкого электрооборудования [10].

В 2005 г. ВМС США запустили программу разработки электромагнитных рельсовых орудий, в рамках которой было создано экспериментальное орудие, способное доставлять снаряд весом в 10 кг на расстояние более 200 км со средней скоростью около 2 км/с. По мнению экспертов, такое орудие имеет настильную траекторию на расстоянии до 30 км. В феврале 2008 г. ВМС США продемонстрировали рельсотрон с энергией 10 МДж, снаряд которого развил дульную скорость 2,5 км/с (9000 км/ч). В декабре 2010 г. в Центре разработки надводного вооружения ВМС США было проведено успешное испытание рельсотрона с дульной энергией 33 МДж. Масса используемых в тестах снарядов варьировалась от 2 до 3,2 кг. В феврале 2012 г. близкий к серийному образцу прототип промышленного рельсотрона от BAE Systems был испытан на 32 МДж. Серийный образец этой системы должен иметь дальность стрельбы до

180 км, а в перспективе – до 400 км. В настоящее время инженеры разрабатывают системы автоматической подачи снарядов, охлаждения и питания установки. ВМС США планируют установку рельсотронов на свои боевые корабли после 2020 г. Ожидается, что такое оружие будет способно поражать цель на расстоянии до 400 км с точностью до 5 м при начальной скорости полета 5,8 км/с. В перспективных разработках со сроком завершения в 2025 г. фигурирует уже установка мощностью в 64 МДж, что примерно в 7 раз выше, чем у нынешних опытных образцов. Эти орудия должны были поступить на вооружение построенных в США эсминцев серии DDG-1000 Zumwalt, чья модульная конструкция и электрическая трансмиссия проектировалась с перспективой использования именно рельсотронов. Однако по состоянию на 2020 г. данные орудия все еще находятся в стадии опытной экспликации и на вышеуказанные эсминцы не поступили [10].

Обобщая вышесказанное, можно сформировать ТТХ обобщенного электромагнитного рельсового орудия, использующего кинетического средства поражения:

- варианты базирования: морское, наземное;
- дульная энергия орудия: 30-65 МДж;
- начальная скорость снаряда: 2-6 км/с;
- скорость снаряда при поражении цели: не менее 1,5 км/с;
- масса снаряда: 2-25 кг;
- максимальная дальность стрельбы: до 200 км (в перспективе – до 400 км);
- точность стрельбы: 5-10 м.

2.3. Описательная модель систем и средств радиоэлектронной борьбы

Анализ вооруженных конфликтов последних лет позволяет сделать вывод о том, что РЭБ прочно утвердилась в качестве одного из важнейших видов обеспечения военных действий. Мероприятия РЭБ объединяют мероприятия радиоэлектронного поражения, радиоэлектронного обеспечения и радиоэлектронной защиты (рис. 2.3). Объектами первоочередного воздействия систем РЭБ в ходе операций являлись [9]:

- элементы систем государственного и военного управления, а также систем управления оружием;
- средства разведки и системы хранения, обработки и распределения информации;
- РЭС различных типов и назначения;
- комплексы средств автоматизации, информационные и автоматизированные системы, базы данных и сети ЭВМ;
- системы поддержки принятия решений для командного состава.

Анализ применения РЭБ позволил выявить основное содержание мероприятий РЭБ, а также ведущие тенденции их изменения [9]:

- мероприятия РЭБ направленны как на воздействие по целевым РЭС, так и на защиту собственных РЭС, а также распространяются на боевую технику, объекты ВС и системы вооружения (рис. 2.3);
- в рамках проведения мероприятий РЭБ уже сегодня кроме использования традиционных источников излучения электромагнитной энергии (средств РЭП) предусматривается задействование других видов оружия, основанного на излучении направленной энергии, – электромагнитного импульса, СВЧ-излучения, пучкового оружия и др.
- мероприятия РЭБ, ранее рассматриваемые как один из элементов мероприятий оперативного обеспечения, начинают рассматриваться как самостоятельная операция, проводимая в интересах дезорганизации управления войсками противника.

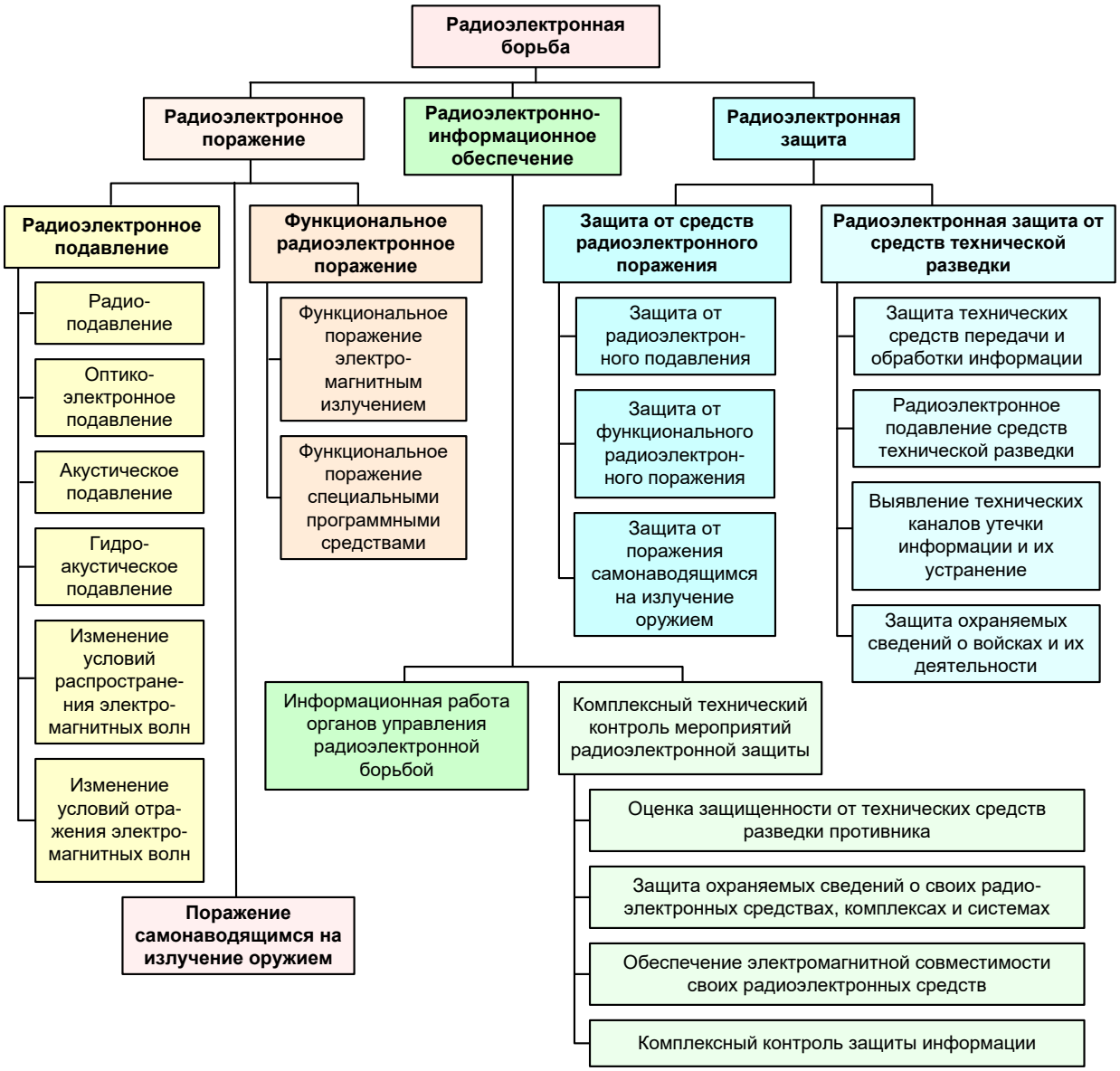

Рис. 2.3. Общая классификация мероприятий РЭБ [90]

К частным тенденциям развития мероприятий РЭБ следует отнести следующие [9]:

- частичная утрата самостоятельной роли РЭБ, которая становится одним из ведущих элементов информационного противоборства, в основном, для борьбы с системами боевого управления при проведении информационных операций;
- коренное поэтапное изменение характера, содержания и роли РЭБ в операции (бое). Так, на первом этапе она являлась одним из видов поддержки ударных сил в ходе боевых действий, на втором – составной частью ведения боевых действий каждого вида ВС со всеми специфическими особенностями. На третьем этапе РЭБ стала компонентом синергетической системы информационного противоборства – одной из составляющих военного потенциала;
- переход от подавляющего воздействия и защиты РЭС к комплексному поражающему и подавляющему информационно-техническому воздействию и защите не только РЭС, но и боевой техники, объектов ВС, систем оружия, а также личного состава ВС и органов государственного управления.
- полная автоматизация процесса радиоэлектронной борьбы.

В большинстве современных войн силы и средства РЭП до начала первого массированного удара ВТО создавали сильные помехи для РЭС противника, и прежде всего – для РЭС системы ПВО, для средств радиосвязи системы государственного и военного управления, а также средств телерадиовещания. Распределение данных средств радиосвязи по рабочим частотам показано на рис. 2.4 [91].

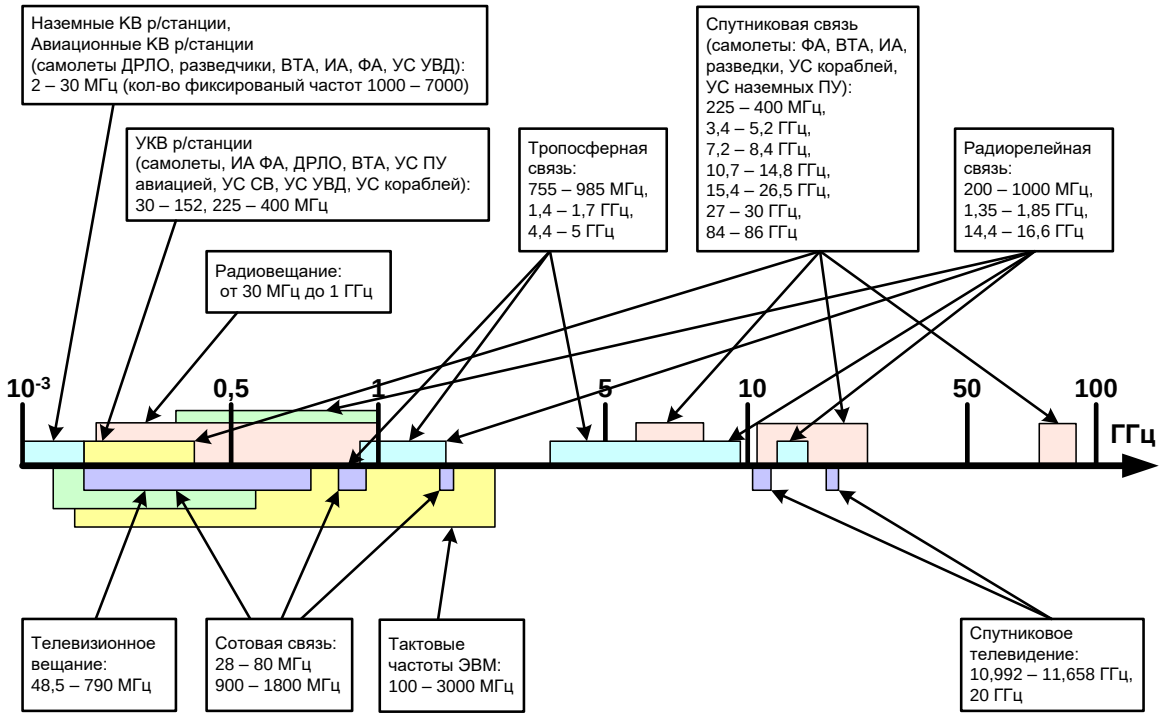

Рис. 2.4. Распределение по рабочим частотам средств связи, навигации и некоторых других систем [91]

Опыт применения средств РЭБ в локальных войнах [9] показывает, что для подавления систем связи использовались следующие виды активных электромагнитных помех (рис. 2.5):

- прицельные по одной частоте;
- скользящие в широком участке диапазона частот;
- дискретные на относительно небольшом участке диапазона частот (подавляющие одновременно несколько частот);
- сплошные заградительные, перекрывающие полностью относительно узкий участок диапазона частот.

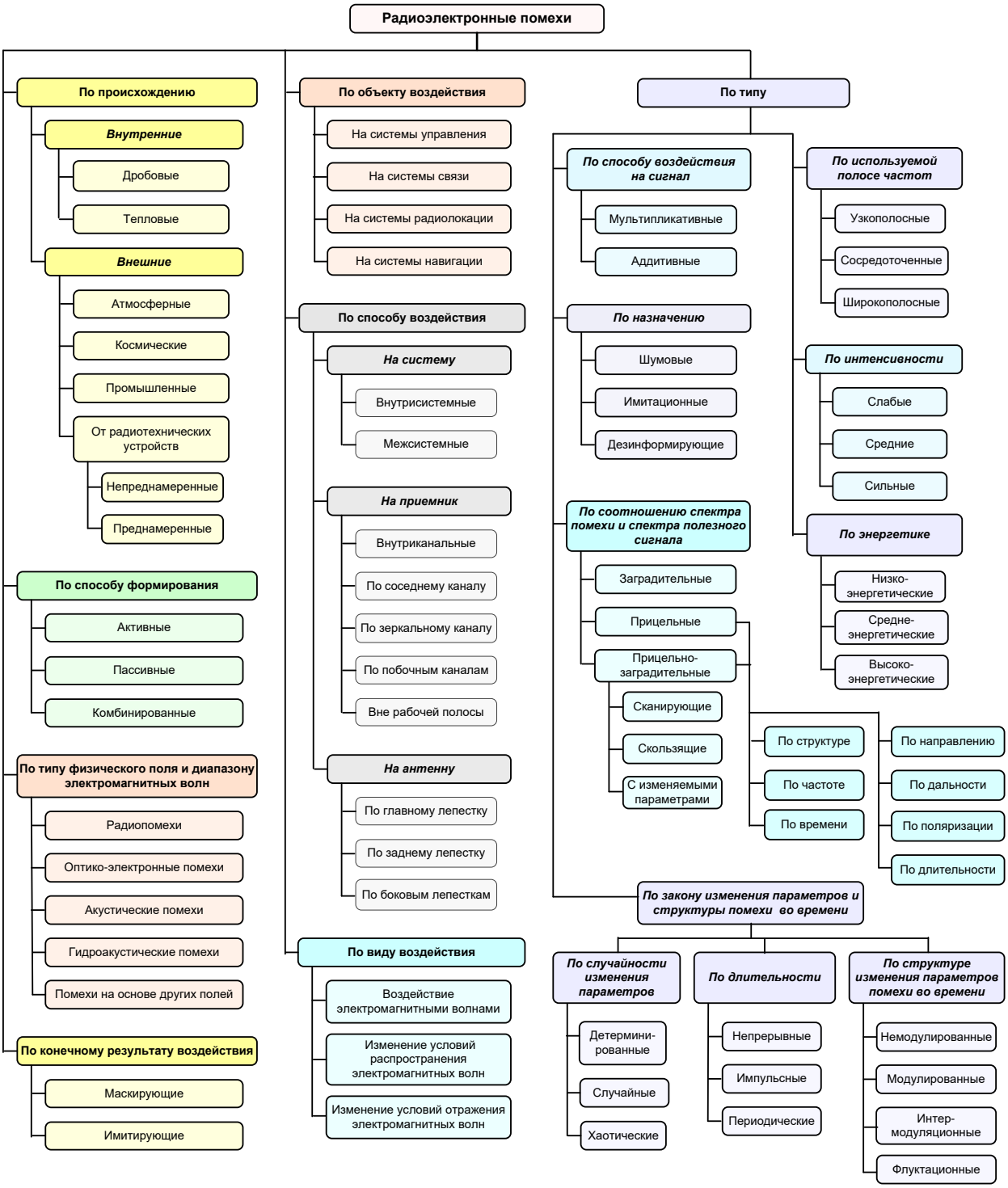

Рис. 2.5. Общая классификация радиоэлектронных помех [87, 92, 338, 411]

Помимо этих видов помех применялись ответные помехи, которые ставились при появлении сигнала противника, а также ретрансляционные помехи.

В рамках описательной модели, представленной в данном подразделе, сформированы обобщенные ТТХ основных средств радиоэлектронного поражения объектов СС СН, как штатно применяемых в современных войнах, так и перспективных разработок:

- средства РЭП;
- средства функционального поражения электромагнитным излучением (ФП ЭМИ) на основе электромагнитного излучения сверхвысокой частоты (СВЧ) и мощного электромагнитного импульса;
- ФП ЭМИ на основе лазерного излучения;
- ФП ЭМИ на преднамеренного силового электромагнитного воздействия электрическим током.

Данные ТТХ сформированы путем анализа военных действий в локальных конфликтах рубежа XX-XXI вв. и перспективных направлений развития вооружений РЭБ, представленных в работах [9, 10, 89].

Необходимо отметить, что в настоящее время штатно применяемыми средствами РЭБ являются, в основном, специализированные комплексы РЭП авиационного и наземного базирования. Применение же оружия на основе ФП ЭМИ носит, как правило, экспериментальный характер. Вместе с тем, общая тенденция применения средств радиоэлектронного поражения показывает устойчивую тенденцию к увеличению доли применения оружия на основе ФП ЭМИ, его значимости и разрушительной мощи в военных конфликтах.

В связи с низкой вероятностью применения в современных военных конфликтах электромагнитного оружия на новых физических принципах (пучкового, электромагнитного геофизического и др.), данное оружие в составе описательной модели не рассматривалось.

2.3.1. Средства радиоэлектронного подавления

В настоящее время для размещения средств РЭП, ориентированных на подавление средств радиосвязи, преимущественно используются платформы с двумя вариантами базирования:

- воздушное;
- наземное.

Данные варианты базирования имеют различные ТТХ в части возможностей по реализации способов подавления, а также различные формы боевого применения. Средства РЭП воздушного базирования ориентированы на вскрытие радиоэлектронной обстановки в стратегическом и оперативном звеньях управления, а также на подавление каналов и сетей радиосвязи государственного и военного управления, сетей мобильной связи, сетей телерадиовещания. Средства РЭП наземного базирования, как правило, размещаются в прифронтовой полосе и ориентированы на вскрытие радиоэлектронной обстановки в оперативном и тактическом звеньях управления, подавления систем радиосвязи управления подразделениями тактического звена при ведении боевых действий в районе дежурства подразделения РЭП.

2.3.1.1. Средства радиоэлектронного подавления воздушного базирования

Результаты анализа боевых действий, имевших место в последнее время в Африке и на Ближнем Востоке, показывают, что системы и средства РЭП воздушного базирования остаются одними из ключевых элементов в достижении превосходства над противником и, как следствие, в обеспечении успеха проводимых информационных операций.

Для решения задач РЭП в ходе операций, средства воздушного базирования декомпозируются на два компонента.

1) Основной компонент, образованный специализированными комплексами РЭП (например, EC-130H CompassCall), действующими в пределах воздушного пространства противника либо за его пределами и решающие основные задачи по ведению РР и РЭП.
2) Вспомогательный компонент, включающий в себя беспилотные носители средств РЭП, действующие в пределах воздушного пространства противника, недоступного для средств РЭП основного компонента (например, в пределах зон гарантированного поражения), которые решают задачи по РР и подавления РЭС противника.

В настоящее время, ведутся программы по интеграции всех сил и средств РЭП воздушного базирования в единое информационно-коммуникационное пространство (например, программа AEA в ВС США), что позволяет управлять ресурсами РЭП, осуществлять оптимальное распределение средств по объектам подавления, в зависимости от обстановки в реальном масштабе времени [9].

Рассматривая комплексы EC-130H CompassCall и EA-6B Prowler (с учетом программ их модернизации до 2020 г.) [9] как прототипы первого компонента средств РЭП воздушного базирования, можно сформировать обобщенные ТТХ такого типового средства.

ТТХ типового специализированного (пилотируемого) комплекса РЭП воздушного базирования [9]:

- варианты боевого применения:
  1) при угрозе применения средств ПВО противника: барражирование комплекса на высоте около 9 км по замкнутым маршрутам над своей территорией в 70-50 км от линии соприкосновения войск с ведением подавления РЭС на глубину до 300 км;
  2) при отсутствии угрозы применения средств ПВО противника: барражирование комплекса на высоте 7-9 км над территорией противника в зонах своего непосредственного боевого применения;
- дальность действия: 3500-4000 км;
- практическая дальность: до 9000 км;
- скорость полета: 400-700 км/ч;
- высота полета: до 10 км;
- экипаж: 6-10 человек.

Комплекс РЭП обеспечивает решение следующих задач [9]:

- ведение радио- и радиотехнической разведки;
- вскрытие дислокации узлов связи и пунктов управления;

- сбор и анализ содержания радиообмена;
- формирование в реальном масштабе времени целеуказаний на вскрытые узлы связи и РЛС противника для применения по ним средств ВТО классов «воздух – земля» и «земля – земля»;
- радиоэлектронное подавление систем коротковолновой, радиорелейной и спутниковой связи военного и государственного управления;
- радиоэлектронное подавление радиосетей управления тактической авиацией, управления комплексами ПВО, современных помехозащищенных систем радиосвязи и передачи данных оперативно-тактического звена сухопутных войск;
- радиоэлектронное подавление гражданских и коммерческих систем мобильной сотовой и транкинговой радиосвязи;
- радиоэлектронное подавление сетей телерадиовещания;
- радиоэлектронное подавление из зон барражирования РЛС обнаружения, функционирующих в МВ, ДМВ и ММВ диапазонах.

Подсистема РРТР комплекса РЭП обеспечивает вскрытие параметров и определения местоположения источников радиоизлучений в диапазоне от 20 до 3000 МГц [9].

Подсистема РЭП, состоящая из комплекта передатчиков помех мощностью по 800 Вт, обеспечивает одновременную постановку помех в диапазоне частот от 20-3000 МГц по 4 независимым лепесткам диаграммы направленности антенны на 144 дискретных частотах. При этом возможна постановка следующих типов помех [9]:

- заградительные шумовые помехи;
- ответные помехи, прицельные по частоте каналов радиосвязи;
- ответные импульсные помехи для РЛС ПВО;
- дезинформирующие помехи для сетей сотовой и транкинговой связи (рассылка ложных сообщений) и для сетей телерадиовещания (вещание собственного контента).

Рассматривая БПЛА RQ-4 Global Hawk и MQ-1C Grey Eagle [9] как прототипы второго компонента средств РЭП воздушного базирования, можно сформировать обобщенные ТТХ такого типового средства:

- вариант боевого применения:
  1) при угрозе применения средств ПВО противника: дежурство в воздухе до 45 ч на высоте до 18 км в зонах досягаемости ПВО, вскрытие радиоэлектронной обстановки с передачей целеуказаний по объектам подавления на пилотируемые комплексы РЭП, уничтожение РЭС (узлов связи и РЛС ПВО) средствами СНИО;
  2) при отсутствии угрозы применения средств ПВО противника: дежурство в воздухе до 45 ч на высоте до 7 км, ведение радиоразведки в интересах вскрытия радиосвязных РЭС, сетей Wi-Fi, базовых станций мобильной сотовой и транкинговой связи;
- скорость полета: до 500 км/ч;
- дальность полета: до 6000 км.

Задачами БПЛА, оснащенных комплексами РЭП, являются следующие [9]:

- проведение первоначальной разведки в оперативной глубине;
- формирование целеуказаний для пилотируемых комплексов РЭП и средств ВТО;
- радиоэлектронное подавление средств радиосвязи (преимущественно базовых станций сетей Wi-Fi, базовых станций мобильной сотовой и транкинговой связи, которые имеют низкую помехозащищенность);
- нанесение высокоточных ударов по узлам связи, пунктам управления, РЛС средств ПВО путем применения СНИО.

На стратегическом уровне управления основной функцией БПЛА РЭП является ведение РРТР, в ходе которой они должны осуществлять перехват сигналов, их анализ и формирование формуляров о радиоэлектронной обстановке. Одновременно происходит пополнение баз данных/библиотек РЭС, расположенных в районе патрулирования. На оперативном уровне решаются задачи ведения разведки, в том числе видовой, формирования целеуказаний системам оружия и подавления РЭС противника. На тактическом уровне БПЛА с помощью средств РРТР могут собирать и передавать пользователям критически важные данные о радиоэлектронной обстановке и формировать целеуказание на подавление или уничтожение РЭС путем применения средств СНИО, в соответствии с замыслом командования. В перспективе, размещенные на БПЛА системы и средства РЭБ должны получить наибольшее распространение именно на тактическом уровне, где они могут применяться с максимальной эффективностью, дополняя возможности систем и средств видовой разведки и РЭП, более удаленных от цели [9].

То, что на БПЛА, в основном, возлагаются задачи разведки, а не подавления объясняется следующим. Основными ограничениями при разработке аппаратуры РЭП являются их массогабаритные параметры и потребляемая мощность. Поскольку оборудование РЭП потребляет большую мощность и требует высокоэффективного охлаждения, то для БПЛА, в настоящее, время разрабатывается оборудование, имеющее относительно низкую мощность по сравнению с пилотируемыми комплексами РЭП [9].

2.3.1.2. Средства радиоэлектронного подавления наземного базирования

Наземными комплексами РЭП комплектуются соответствующие батальоны мотопехотных и бронетанковых дивизий, которые предназначены для выявления и радиоэлектронного подавления систем и средств КВ и УКВ радиосвязи и РЛС в тактическом звене, дивизий первого эшелона взаимодействия частей сухопутных войск с армейской и фронтовой авиацией на дальности до 100 км.

Принимая средства РЭП AN/TLQ-17A (V)1 Traffic Jam, AN/ALQ-151(V)2 Quick Fix II, IEWCS, EFVS, AN/MLQ-40 Prophet, Р-378, Р-330, Р-325У, Р-939Б, МВША «Атлант» [9, 58], как прототипы наземных средств РЭП можно сформировать обобщенные ТТХ такого типового средства.

Типовой наземный комплекс РЭП выполняет следующие задачи:

- ведение радио- и радиотехнической разведки;
- обработка разведывательных данных и формирование карты текущей радиоэлектронной обстановки;
- определение параметров и координат источников радиоизлучений для обеспечения целеуказания и оценки нанесенного ущерба;
- осуществление радиоэлектронного подавления средств связи и радиолокации в зоне своей ответственности.

Наземный комплекс РЭП состоит из двух подсистем:

1) воздушная подсистема (на основе средств РРТР, размещенных на вертолетах армейской авиации и/или на тактических БПЛА);
2) наземная подсистема (на основе территориально-распределенной группировки средств РЭП).

Воздушная подсистема наземного комплекса РЭП обеспечивает ведение РРТР, а также радиоэлектронное подавление объектов, находящихся на удалении 15-30 км от линии соприкосновения войск. В качестве носителей средств этой подсистемы выступают вертолеты и тактические БПЛА. Воздушная подсистема способна обнаруживать, идентифицировать, определять местоположение, а также осуществлять радиоэлектронное подавление источников радиоизлучения.

Обобщенные ТТХ средств РРТР воздушной подсистемы наземного комплекса РЭП [9]:

- диапазон частот, в котором ведется радиоразведка: 1,5-3000 МГц;
- зона ведения разведки: 150×50 км;
- точность пеленгования: 0,5°-1°;
- точность определения местоположения целей: на расстоянии до 40 км – 150-500 м; на расстоянии 80-120 км – 450-1500 м;

ТТХ средств РЭП воздушной подсистемы наземного комплекса РЭП [9]:

- диапазон частот, в котором ведется подавление: 20-450 МГц;
- мощность излучения помех: 40-150 Вт;
- ширина мгновенно подавляемой полосы частот: 10-25 кГц.

Радиоразведка и постановка радиопомех средствами воздушной подсистемы осуществляются с высоты полета 60-180 м в течение 2-2,5 ч на удалении 5-15 км от линии соприкосновения войск и на глубину до 30 км [9].

Наземная подсистема обеспечивает вскрытие радиоэлектронной обстановки и постановку помех для тактической радиосвязи преимущественно в звене управления «батальон – полк», при координации совместных действия средств РРТР и РЭП наземной и воздушной подсистемы.

Типовые ТТХ средств РРТР наземной подсистемы комплекса РЭП [9, 58]:

- диапазон частот, в котором ведется радиоразведка: 20-15000 МГц;
- зона ведения разведки: 150×120 км;
- мгновенная полоса обзора: около 2,5 ГГц;
- разрешающая способность: не хуже 1 кГц;
- скорость поиска в разведываемом диапазоне: порядка 3000 ГГц/с;

- чувствительность (при ОСШ на входе приемника не менее 10 дБ в полосе частот 20 кГц): не хуже 5 мкВ/м;
- вероятность распознавания вида сигнала и РЭС за время 0,2 с: не менее 0,8;
- точность пеленгования: 0,5°-1°.

Типовые ТТХ средств подавления наземной подсистемы комплекса РЭП [9, 58]:

- диапазон частот, в котором ведется подавление: 1,5-2500 МГц;
- мощность излучения помех: 0,5-1 кВт;
- высота антенн средств РЭП: 6-20 м;
- количество одновременно подавляемых целей: 5-300;
- ширина спектра помех: прицельных по частоте 3-50 кГц; заградительных 150-3000 кГц;
- время реакции при постановке помех: по неизвестной частоте 0,8 с; по известным частотам 0,04 с;
- обнаружение и подавление РЭС с режимом ППРЧ до 1000 скачков/с;
- дальность подавления: до 100 км от линии соприкосновения войск.

Специфичным наземным средством РЭП являются забрасываемые передатчики помех (ЗПП), которые либо выстреливаются артиллерийскими системами, либо размещаются на малогабаритных БПЛА. Такие ЗПП предназначены для дезорганизации систем управления войсками в тактическом звене путем постановки помех средствам радиосвязи в КВ и УКВ диапазонах.

Типовые характеристики ЗПП, забрасываемых артиллерийским способом [58]:

- дальность стрельбы (забрасывания) ЗПП: 13-22 км;
- радиус постановки помех: 700 м;
- диапазон подавляемых частот: 1,5-120 МГц;
- продолжительность непрерывной работы: до 1 ч.

Типовые характеристики аэродинамических ЗПП, размещаемых на малогабаритных БПЛА [58]:

- дальность полета (забрасывания) аэродинамического ЗПП: при управлении БПЛА оператором до 50 км; в режиме автономного полета до 100 км;
- высота полета БПЛА с ЗПП: до 3 км;
- количество одновременно применяемых БПЛА с ЗПП: до 35 шт;
- диапазон подавляемых частот: 1,5-200 МГц;
- продолжительность непрерывной работы: 0,5-3 ч;
- масса БПЛА с ЗПП: 3-20 кг.

Дополнительные данные о средствах и комплексах РЭП наземного и воздушного базирования представлены в работах [9, 58, 89, 91].

2.3.2. Средства функционального поражения на основе мощного СВЧ электромагнитного излучения

Функциональное поражение электромагнитным излучением (ФП ЭМИ) заключается в разрушении и/или повреждении элементов РЭС путем использо-

вания однократных или многократных импульсных электромагнитных воздействий, приводящих к необратимым изменениям электрофизических параметров в полупроводниковых или оптико-электронных элементах РЭС в результате их перегрева или пробоя [9].

Основным отличием ФП ЭМИ от РЭП является физический принцип нанесения ущерба. При ФП ЭМИ ущерб РЭС причиняется путем необратимого (катастрофического) или обратимого (восстанавливаемого) изменения физико-химической структуры элементов РЭС, вследствие воздействия электромагнитных полей на материалы, входящие в состав электронных и полупроводниковых приборов и других компонентов этих систем. Эффект воздействия средств ФП ЭМИ на РЭС основан на возможности изменения физико-химических свойств электро- и радиоматериалов при облучении их сильными электромагнитными полями. Необратимые изменения свойств вещества, приводящие к качественно новым образованиям с иной электромагнитной структурой, происходят при значительной энергии воздействующего ЭМИ [9].

В зависимости от мощности, длительности импульсов, рабочей частоты источника ЭМИ и расстояния до РЭС эффекты от электромагнитного воздействия могут быть различными – от кратковременного снижения качества функционирования и временной потери работоспособности РЭС до его полного повреждения или разрушения в результате перегрева или полевого пробоя [9].

При воздействии ЭМИ на метровых и более длинных волнах на металлических корпусах РЭС наводятся значительные ЭДС, отказывают различные электронные схемы и исполнительные элементы. При воздействии ЭМИ в дециметровом или сантиметровом диапазоне волн, совпадающем с рабочим диапазоном РЭС, повреждаются входные устройства (в частности, СВЧ-диоды). Миллиметровые волны проникают в щели экранов, повреждая как входные цепи, так и экранированные устройства микроэлектроники.

При взаимодействии мощных СВЧ-колебаний с элементами и узлами РЭС могут наблюдаться два основных эффекта [93]:

1) наведение на контурных элементах (выводах полупроводниковых приборов, печатных проводниках и т.д.) СВЧ-мощности, которая приводит к электрическим перегрузкам;
2) непосредственное взаимодействие СВЧ-импульсов со структурой и материалом полупроводникового элемента.

Мощности ЭМИ, формируемых известными средствами ФП ЭМИ, могут превышать десятки ГВт, при этом длительности их импульсов лежат в пределах от миллисекунд до наносекунд. В большинстве практических случаев функциональное поражение РЭС при применении ЭМИ имеет место при отказе хотя бы одного из основных его полупроводниковых элементов.

Перечень типовых нарушений работоспособности радио- и электротехнического оборудования РЭС при их эксплуатации в условиях воздействия ЭМИ приведен в таблице 2.1 [9, 94].

Таблица 2.1 – Типовые нарушения работоспособности радио- и электротехнического оборудования РЭС при воздействии ЭМИ [95]

Тип устройства	Характер нарушения	Причина нарушения
Антенно-фидерные устройства (АФУ)	а) отказ антенного коммутатора; б) пробой изоляции антенны, излучателя и кабельной системы фидера; в) выход из строя входных устройств приемника и выходных устройств передатчика. Все нарушения в основном носят необратимый характер	а) появление перенапряжений в АФУ; б) низкая электрическая прочность входной элементной базы
Приемные и передающие устройства, генераторы синусоидальных сигналов и сигналов специальной формы	а) обратимые изменения электрического режима СВЧ-генераторов; б) временное увеличение коэффициента шума, изменение коэффициента шума, частоты и мощности генерируемых сигналов; в) сбои, выдача ложных импульсов и подавление полезных сигналов	а) превышение по амплитуде полезных сигналов наводками; б) перекрытие спектров полезных сигналов спектрами помеховых наводок; в) высокая чувствительность полупроводниковых элементов
Устройства управления, стабилизации и формирования команд	а) сбои в структуре команд; б) выдача ложных команд по разрядам кодовых групп; в) уменьшение амплитуды полезных сигналов; г) ложные срабатывания при обработке команд, их исполнении и отработке	наложение импульсов помех в цепях устройств на формируемые полезные сигналы, и их суперпозиция во времени
Линейные усилители	а) выход из строя входных и выходных цепей; б) искажение формы входных (выходных) сигналов и появление ложных сигналов; в) самовозбуждение	а) появление перенапряжений в линиях связи; б) низкая электрическая прочность входных элементов усилителей; в) изменение тока поджига защитных разрядников
ЭВМ и цифровые системы автоматики и управления	а) сбои в работе, нарушение нормального хода программ; б) потери информации в регистрах оперативной памяти; в) ошибки и искажения вводимой и получаемой информации	а) наводки во внешних и внутренних цепях и схемах; б) выход из строя систем ввода и вывода информации
Источники питания	а) выход из строя первичных и вторичных источников электропитания; б) значительные амплитудные изменения выходного напряжения первичных источников и временное пропадание выходного напряжения вторичных источников питания	а) перенапряжение в питающих ЛЭП; б) срабатывание линейной защиты и скачки тока и напряжения в питающих линиях; в) наводки по цепям питания и системам заземления; г) низкая электрическая прочность элементов преобразования

Таблица 2.2 – Характеристика некоторых видов средств ФП ЭМИ, являющихся источниками импульса мощного СВЧ излучения [14]

Вид средства	Вероятность применения	Радиус поражения	Поражаемые цели (в зависимости от частоты излучения)	Потенциальные пользователи
Ядерный генератор электромагнитного излучения большой амплитуды	Умеренная	В радиусе до 2400 км	Электронное оборудование, компьютеры, датчики, связь, автомобили, системы передачи энергии, элементы гражданской инфраструктуры	Ядерные державы, обладающие баллистическими ракетами
СВЧ-излучатели	Низкая	Существующие СВЧ-средства пока не излучают энергии, достаточной для поражения интегральных схем на достаточном расстоянии	Интегральные схемы, печатные платы, переключательные реле	США, Англия, Австралия, Россия, Швеция
Электромагнитная бомба – взрывомагнитный генератор (ВМГ)	Высокая	~ 175 м	Незащищенные радиоэлектронные системы, соединенные проводами длиной более 75 м	Террористы
Осциллирующий виртуальный катод, СВЧ-генератор типа «варикатор»	Умеренная	~ 150 м	Интегральные схемы, переключательные реле	Любая страна

К достоинствам средств ФП ЭМИ можно отнести следующие [9]:

- расширение диапазона решаемых задач за счет возможности поражения не излучающих РЭС;
- универсальность (способность ЭМИ поражать широкую номенклатуру РЭС, при этом эффективность поражения РЭС не зависит от их функционального назначения);
- внеполосность (способность ЭМИ проникать внутрь РЭС помимо их полосы пропускания);
- эффективное воздействие на РЭС с высокой помехозащищенностью к применению традиционных способов РЭП;
- отказ от сложных средств анализа и имитации сигналов подавляемых РЭС, которые традиционно используются в РЭП;
- снижение в ряде случаев требований к качеству целеуказания (по местоположению, частотному диапазону, режимам работы), которое необходимо для поражения РЭС противника.

Перспективные образцы средств ФП ЭМИ основаны на генерации кратковременного импульса ЭМИ большой мощности, способном вывести из строя РЭС, составляющие основу любой информационной системы.

Элементная база РЭС весьма чувствительна к энергетическим перегрузкам. Поток электромагнитной энергии достаточно высокой плотности способен

выжечь полупроводниковые переходы, полностью или частично нарушив их нормальное функционирование. Даже у кремниевых сильноточных биполярных транзисторов, обладающих повышенной стойкостью к перегревам, напряжение пробоя составляет 15-65 В, а у арсенид-галлиевых приборов – 10-12 В. Запоминающие устройства имеют пороговые напряжения порядка 7 В, типовые логические интегральные схемы на МОП-структурах – 7-15 В, а микропроцессоры обычно прекращают свою работу при 3,3-5 В [9].

Кроме того, анализ результатов отечественных и зарубежных исследований воздействия импульсов ЭМИ наносекундной длительности напряженностью 2-10 кВ/м (при частоте следования импульсов порядка 1 МГц) на вычислительные блоки и микропроцессоры РЭС показал, что уровни наводимых напряжений приводят к отказам этих элементов и ложным срабатываниям в них, что делает практически невозможным корректное функционирование в них программного обеспечения [9].

Источниками импульсов мощного СВЧ ЭМИ могут быть ядерные взрывы, мощные релятивистские СВЧ-генераторы (взрывомагнитные, магнитокумулятивные), обычные электровакуумные СВЧ-генераторы (усилители), в том числе с временной компрессией излучаемых импульсов, твердотельные генераторы с полупроводниковыми коммутаторами, генераторы с газовыми коммутаторами и др. В качестве излучателей также могут применяться аппретурные антенны (зеркальные, рупорные), а также ФАР и АФАР [95].

Основным показателем устойчивости элементной базы к воздействию ЭМИ являются критериальные уровни поражения, определяемые величиной мощности, при которой возникают восстанавливаемые и невосстанавливаемые отказы в элементах РЭС. В таблицах 2.3 и 2.4 приведены энергетические уровни поражения некоторых элементов, блоков и узлов РЭС.

Таблица 2.3 – Энергетические уровни поражения элементов РЭС при воздействии СВЧ-импульсов [91]

Тип прибора	Энергия повреждения, мкДж
СВЧ-диоды	0,1 – 10
Интегральные схемы	0,1 – 300
Цифровые интегральные схемы	80
Полевые транзисторы	10
Маломощные транзисторы	$1\cdot10^4 – 3\cdot10^4$
Транзисторы средней и большой мощности	$400 – 4\cdot10^4$
Выпрямительные диоды	$100 – 4\cdot10^5$
Быстродействующие переключающие диоды	20
Туннельные диоды	500
Кремниевые тиристоры	3000
Низкочастотные транзисторы	–

Таблица 2.4 – Уровни функционального поражения некоторых блоков и узлов РЭС при воздействии импульсного СВЧ-излучения [91]

Тип изделия	Плотность потока энергии, Вт/см^2	Поток энергии, Дж/см^2	Длительность импульса, с	Частота импульсов, кГц	Длительность воздействия, с
Усилители систем управления и связи	10 – 40	10^{-2} – $4\cdot10^{-2}$	10^{-3}	–	–
Узлы систем управления и связи на ИС и БИС	70 – 600	$0{,}7\cdot10^{-2}$ – $6\cdot10^{-2}$	10^{-6}	1	1
Элементы радиопередатчиков	10^4 – 10^5	10^{-3} – 10^{-4}	10^{-7}	–	–
Радиоприемники через антенну с $S_{эфф}$ = 1-2 м^2	1 – 100	10^{-5} – 10^{-6}	10^{-7}	–	–
Телевизионные системы на видиконах (повреждение видеоусилителя)	$3\cdot10^3$ – $5\cdot10^3$	0,6 – 2	$2\cdot10^{-4}$ – $4\cdot10^{-4}$	–	–

Критериальные (критические для поражаемого оборудования) уровни функционального поражения широкой номенклатуры РЭС отличаются большим разбросом и могут составлять от 10 до 5000 Вт/см^2. Типовые критериальные уровни различных полупроводниковых приборов приведены в работах [87, 93]. При этом наиболее уязвимыми элементами РЭС являются СВЧ-диоды, работающие во входных трактах преобразователей частоты, интегральные микросхемы и диоды с точечным контактом.

В таблице 2.5 приведены характеристики нескольких типов генераторов мощных ЭМИ-импульсов миллиметрового и сантиметрового диапазонов электромагнитных волн [91].

Таблица 2.5 – Характеристики некоторых мощных СВЧ-генераторов миллиметрового и сантиметрового диапазонов волн [91]

Тип генератора	Частота, ГГц	Длительность импульса	Выходная мощность	КПД, %	Примечание
Гиратрон с импульсным соленоидом, обладающий стабилизируемым носителем энергии	500	2 мкс	более 100 кВт		Эксперимент
Тиратрон с высокой эффективностью моды TE_{031}	140	2 мкс	100 кВт	30	Эксперимент
Тиратрон с резонаторами моды TE_{031}	100	–	1000 кВт	–	–
Виркатор	До 40	3–5 нс	до 1 ГВт	–	–
Релятивистский гиратрон	35	55 нс	0,2 ГВг	–	Разработан
Взрывомагнитный генератор	–	1 мкс	10^{10} кВт	–	Разработан в Лос-Аламосе

Как видно из таблицы 2.5, наиболее короткие импульсы достигаются в виркаторах, а наибольшая выходная мощность реализуется во взрывомагнитных генераторах. Современный уровень развития СВЧ-генераторов обеспечивает выделение в нагрузке энергии 10^7-10^8 Дж, мощность которой эквивалентна мощности энергии, освобождающейся при взрыве заряда взрывчатого вещества массой 10 кг [91].

Прикладные исследования по созданию экспериментальных средств ФП ЭМИ ведутся с 1995 г. при этом опытные образцы этих средств регулярно проходят испытания в ходе военных конфликтов. Основываясь на данных об испытании опытных образцов, представленных в работах [9, 91], можно сформировать приблизительные обобщенные ТТХ средств ФП ЭМИ.

Мобильные средства ФП ЭМИ:

- используемый диапазон частот: 0,5-20 ГГц;
- частота повторения импульсов: 10 Гц;
- длительность импульса: 200-1000 нс;
- импульсная мощность излучения: 1-5 ГВт;
- энергия в импульсе: 2-10 кДж;
- тип энергоустановки: газотурбинный генератор;
- тип источника ЭМИ: гираторы, виркаторы, черенковский генератор;
- КПД генераторного прибора 36-40%;
- КПД средства ФП ЭМИ в целом: 20-25%;
- масса: 6-10 т;
- варианты базирования: автомобиль, бронетранспортер;
- диаметр антенны: 2-5 м;
- дальность действия: в пределах прямой видимости.

Средства ФП ЭМИ одноразового действия:

- используемый диапазон частот: 6-10 ГГц;
- энергия в импульсе: 3-5 ГВт;
- длительность импульса: 150-1500 нс;
- тип источника ЭМИ: взрывомагнитный генератор, резонансный магнетрон, виркатор;
- масса: 500 кг;
- дальность действия: 3-4 км.

Малогабаритные средства ФП ЭМИ:

- используемый диапазон частот: 0,5-100 ГГц;
- энергия в импульсе: 1-5 ГВт;
- длительность импульса: 1-100 нс;
- тип источника ЭМИ: взрывомагнитный генератор, ударно-волновой генератор;
- масса: 40-50 кг;
- дальность действия: 1-2 км.

Перспективным способом применения средств ФП ЭМИ является их использование в качестве боевой части средств ВТО – крылатых ракет и управляемых авиационных бомб. Образцы такого оружия уже проходили испытания. В 1991 г. во время операции «Буря в пустыне» американское командование впервые применило крылатую ракету Tomahawk, в качестве боевой части которой использовалось средство ФП ЭМИ, создающее мощный СВЧ-импульс мощностью 5 МВт. В 2009 г. в США были проведены испытания нового образца ЭМИ-боеприпаса. Его пиковая мощность составила 35 МВт при длительности импульсов 100-150 нс в диапазоне 2-6 ГГц [9, 91].

Более подробные сведения о средствах ФП ЭМИ и вариантах их боевого применения представлены в работах [9, 87, 91, 93, 95]. Дополнительно в работах [109-113] представлены результаты исследований воздействия ФП ЭМИ на элементы ТКС, а в работах [114-116] – результаты исследований воздействия ФП ЭМИ на средства вычислительной техники.

2.3.3. Средства функционального поражения на основе лазерного излучения

Лазер, являющийся оптическим квантовым генератором, способен формировать сильное ЭМИ в оптическом диапазоне волн с высокой плотностью энергии (со средней выходной мощностью более 20 кВт) в весьма узком телесном угле. Свойство очень узкой направленности луча и высокая энергетическая плотность излучения позволяют применять лазер в качестве средства ФП ЭМИ.

Атмосфера является «прозрачной» для лазерного излучения в диапазоне длин волн 0,3-1 мкм. Лазеры способны генерировать ЭМИ в широком оптическом диапазоне, однако, как средства ФП ЭМИ практический интерес представляют оптические квантовые генераторы, работающие в так называемых «окнах прозрачности» атмосферы, которым соответствуют волны оптического диапазона $\lambda = 0{,}5\text{-}2$ мкм, за исключением «непрозрачных» участков $\lambda = 0{,}95$; 1,15; 1,3-1,5 мкм [87]. Сформированное лазером ЭМИ обладает высокой степенью пространственно-временной когерентности. Временная когерентность поля достигает значения $\tau_{ког} \approx 0{,}1$ с, благодаря чему удается получить сигнал с узким спектром ($f \approx 10$ Гц) [87].

Высокая степень пространственной когерентности позволяет с помощью простых оптических устройств концентрировать энергию лазера в весьма узком телесном угле. Эта способность лазера позволяет при сравнительно небольшой энергии излучения на выходе оптической системы даже на больших расстояниях до подавляемого РЭС формировать ЭМИ с плотностью энергии, которой достаточно для достижения эффекта функционального поражения некоторых оптико- и радиоэлектронных устройств на значительных расстояниях (около 10 км). Однако, вследствие весьма малого сечения лазерного луча (0,2-0,8 м^2) на расстоянии от 20 км и дальше, возникает проблема точного наведения луча на цель [87].

Можно выделить два механизма функционального поражения радио- и оптико-электронных средств лазерным оружием [87]:

1) непосредственное поражение РЭС путем прямого воздействия сильного узконаправленного лазерного ЭМИ;
2) выведение из строя объекта за счет вторичного индуцированного излучения плазмы, порождаемой взаимодействием сильного электромагнитного поля и твердого вещества (например, материала обтекателя антенны). В этом случае возможно обратимое (временное) поражение РЭС, которое через некоторое время восстанавливает свои функции.

Кроме того, лазерные лучи деструктивно воздействуют на поверхностный слой материала цели, в результате чего они могут разрушить тонкостенные оболочки тепловым или ударным воздействием. В этом случае поражающее действие лазерного оружия определяется, в основном, термомеханическим и ударно-импульсным воздействием лазерного луча на цель и достигается за счет нагревания до высоких температур материалов объекта. Это вызывает расплавление или даже испарение материалов [87].

Действие лазерного излучения отличается внезапностью, скрытностью, отсутствием внешних признаков в виде огня, дыма, звука, высокой точностью, прямолинейностью распространения и практически мгновенным действием.

Появление первых реальных опытных лазерных средств ФП ЭМИ приходится на 2009-2011 гг. Анализ применения лазерных средств ФП ЭМИ, представленный в работе [9], позволяет сделать вывод, что современные и перспективные генераторы лазерного излучения могут быть использованы, прежде всего, для поражения ретрансляторов радиосвязи, размещенных на летно-подъемных средствах и на малых БПЛА.

Основываясь на данных об испытании опытных образцов, представленных в работе [9], можно сформировать приблизительные обобщенные ТТХ лазерного средства ФП ЭМИ для поражения ретрансляторов радиосвязи на летно-подъемных средствах и на малых БПЛА:

- мощность лазерной установки 10-50 кВт (в перспективных образцах 100-120 кВт за счет объединения нескольких лазерных генераторов);
- дальность эффективного действия до 5 км;
- режим работы импульсный.

Дополнительные сведения о средствах и способах ФП ЭМИ на основе лазерного излучения представлены в работах [9, 93].

2.3.4. Средства функционального поражения на основе преднамеренного силового электромагнитного воздействия

Преднамеренное силовое электромагнитное воздействие (ПС ЭМВ) – это воздействие с применением излучателей электромагнитного поля, генераторов напряжения и тока путем генерирования в информационных системах электромагнитной энергии, уровень которой вызывает нарушение нормального функционирования технических и программных средств информационных систем [105].

Средства ПС ЭМВ отличаются от средств ФП ЭМИ тем, что средой распространения поражающего фактора, является не эфир, а токопроводящие элементы, а источником – генераторы мощного электрического тока вместо генераторов СВЧ-излучения. При этом, с учетом того, что практически все виды РЭС, ПУ и узлов связи питаются от стационарной сети электрического тока, а сама эта сеть является широкоразветвленной (при этом ее многочисленные элементы и проводные участки не контролируются), такие ПС ЭМВ могут быть

осуществлены на значительном расстоянии от поражаемых объектов с эффективностью, сравнимой с применением средств ФП ЭМИ.

Средой проникновения и распространения ПС ЭМВ среди элементов СС СН могут являться: сети электропитания; проводные линии связи; металлоконструкции, проводящие электрический ток; электромагнитные поля. При этом, ПС ЭМВ могут распространяться по линиям сети электропитания на многокилометровые расстояния (экспериментальные ПС ЭМВ сохраняли свой поражающий потенциал на расстояниях 23 км [100]) и поражать подавляющее число РЭС, подключенных к стационарной электрической сети. В работах [101-104] приведены результаты экспериментальных исследований по поражению вычислительной техники ПС ЭМВ, которые распространяются по проводным линиям связи. Результаты анализа поражающих факторов ПС ЭМВ обобщены в стандарте [105].

Анализ тестовых ПС ЭМВ, представленных в стандарте [105], позволяет сформировать основные оценочные характеристики ПС ЭМВ, которые могут быть использованы для поражения элементов СС СН. Данные характеристики представлены в таблицах 2.6-2.9.

Необходимо отметить, что в ряде случаев задачу поражения элементов СС СН можно решить с помощью относительно маломощных импульсных ПС ЭМВ, модулированных определенным образом. Такие ПС ЭМВ передаются электромагнитным полем, либо создаются кондуктивными воздействиями на кабели связи или кабели электропитания. Как показано в работе [100], воздействие таких маломощных ПС ЭМВ не приводит к выходу из строя электронных узлов подключенных РЭС, но может вызывать у них реакцию, которая аналогична нарушению работы программного обеспечения или сбоям аппаратной части [100]:

- в проводных линиях связи может существенно снижаться скорость передачи данных, либо в них вносятся неприемлемые искажения;
- в сетях электропитания, может раскачиваться вторичный источник электропитания РЭС, вызывая заброс выходного напряжения, поражающего электронные компоненты РЭС, либо приводить к срабатыванию электронных схем защиты, инициируя тем самым провал выходного напряжения, следствием которого является остановка технологического процесса, требующая перезагрузки ПО;
- в сетях электропитания может быть спровоцирована остановка асинхронных электродвигателей;
- в сетях электропитания или других проводных линиях может изменяться частота выходного напряжения преобразователей регулируемых электроприводов, вызывая изменения скорости электродвигателей, приводящие к авариям.

Таблица 2.6 – Значения типовых параметров ПС ЭМВ, распространяющихся по сети электропитания [105]

Вид ПС ЭМВ	Параметры ПС ЭМВ	Значения параметров	
		min	max
Перенапряжения большой длительности	Кратность перенапряжений	1,5	1,7
	Длительность воздействия, с	30	60
	Мощность воздействия, кВ·А	10	100
Низковольтные однократные миллисекундные импульсы напряжения	Длительность импульса, мс	5	20
	Амплитуда тока короткого замыкания (напряжение холостого хода 1 кВ), кА	2	10
	Энергия воздействия, кДж	7	150
Высоковольтные однократные миллисекундные импульсы напряжения	Длительность импульса, мс	0,1	2
	Амплитуда тока короткого замыкания (напряжение холостого хода 3 кВ), кА	5	10
	Энергия воздействия, кДж	1	45
Комбинированные однократные импульсы напряжения (высоковольтные миллисекундные импульсы, наложенные на низковольтные миллисекундные импульсы)	Длительность основного импульса, мс	5	5
	Длительность вспомогательного импульса, мс	0,05	0,1
	Амплитуда тока короткого замыкания для основного импульса (напряжение холостого хода 1 кВ), кА	2	10
	Амплитуда тока короткого замыкания для вспомогательного импульса (напряжение холостого хода 5 кВ), кА	5	5
	Энергия воздействия, кДж	7	150
Высоковольтные периодические микросекундные импульсы напряжения	Напряжение на нагрузке сопротивлением 50 Ом, кВ	5	5
	Средняя мощность, кВт	1	1
	Частота осцилляций, МГц	0,2-1	2-1
	Частота следования, кГц	0,7	1
Высоковольтные однократные наносекундные импульсы напряжения	Длительность импульса на нагрузке сопротивлением 50 Ом, нс	500	500
	Длительность фронта, нс	50	50
	Напряжение на нагрузке сопротивлением 50 Ом, кВ	50	250
	Энергия воздействия, Дж	20	500
Высоковольтные периодические наносекундные импульсы напряжения	Длительность импульса на нагрузке сопротивлением 10 кОм, нс	50	50
	Длительность фронта на нагрузке 10 кОм, нс	5	5
	Напряжение на нагрузке 10 кОм, кВ	50	80
	Частота следования, кГц	1	1
Периодические импульсы тока короткого замыкания	Длительность импульса, мкс	500	500
	Амплитуда тока короткого замыкания, кА	0,5	1
	Дополнительные параметры: импульсы тока следуют с частотой 0,1-1 кГц, длительность пачки импульсов 1 с		

Таблица 2.7 – Значения типовых параметров ПС ЭМВ, распространяющихся по проводным линиям связи [105]

Вид ПС ЭМВ	Параметры ПС ЭМВ	Значения параметров	
		min	max
Низковольтные однократные миллисекундные импульсы напряжения	Длительность импульса, мс	1,5	7
	Амплитуда тока короткого замыкания (напряжение холостого хода 1 кВ), кА	0,5	1
	Энергия воздействия, кДж	0,5	5
Высоковольтные однократные микросекундные импульсы напряжения	Длительность импульса, мкс	50	250
	Амплитуда тока короткого замыкания (напряжение холостого хода 1 кВ), кА	2	4
	Энергия воздействия, кДж	0,25	2
Высоковольтные однократные наносекундные импульсы напряжения	Длительность импульса на нагрузке сопротивлением 50 Ом, нс	250	100
	Напряжение на нагрузке сопротивлением 50 Ом, кВ	50	150
	Энергия воздействия, Дж	15	40
	Частота следования, Гц / Длительность пачки, с	10/1	10/1
Высоковольтные периодические наносекундные импульсы напряжения	Длительность импульса на нагрузке сопротивлением 10 кОм, нс	50	50
	Длительность фронта на нагрузке сопротивлением 10 кОм, нс	5	5
	Напряжение на нагрузке сопротивлением 10 кОм, кВ	50	80
	Частота следования, кГц	1	1

Таблица 2.8 – Значения типовых параметров ПС ЭМВ, распространяющихся по металлоконструкциям [105]

Вид ПС ЭМВ	Параметры ПС ЭМВ	Значения параметров	
		min	max
Токи большой длительности в непрерывном режиме	Действующее значение тока (при сопротивлении нагрузки 0,3 Ом), кА	0,1	1
	Мощность воздействия, кВ·А	1	30
	Длительность воздействия, с	60	60
Токи большой длительности в импульсном режиме	Длительность импульса, мс	5	10
	Действующее значение тока (при сопротивлении нагрузки 0,3 Ом), кА	2	2,5
	Мощность воздействия, кВ·А	2	50
	Энергия воздействия, кДж	5	100
Импульсные токи большой длительности	Длительность импульса, мс	5	50
	Амплитудное значение тока (при сопротивлении нагрузки 0,3 Ом), кА	2	2,5
	Энергия воздействия, кДж	7	90
Импульсные токи малой длительности	Длительность импульса, мс	0,2	5
	Амплитуда тока (при сопротивлении нагрузки 3 Ом), кА	1,25	2,5
	Энергия воздействия, кДж	1	60
Высоковольтные однократные наносекундные импульсы напряжения	Длительность импульса на нагрузке сопротивлением 50 Ом, нс	250	100
	Напряжение на нагрузке сопротивлением 50 Ом, кВ	50	150
	Энергия воздействия, Дж	15	40
	Частота следования, Гц / Длительность пачки, с	10/1	10/1

Таблица 2.9 – Значения типовых параметров ПС ЭМВ, распространяющихся электромагнитным полем [105]

Вид ПС ЭМВ	Параметры ПС ЭМВ	Значения параметров	
		min	max
Однократные наносекундные импульсы электромагнитного поля	Длительность импульса, нс	100	100
	Напряженность импульсного электрического поля, кВ/м	1	10
Периодические наносекундные импульсы электромагнитного поля с низкой частотой повторения	Длительность импульса, нс	0,2 ±0,1 0,8 ±0,3	0,2 ±0,1 0,8 ±0,3
	Напряженность импульсного электрического поля, кВ/м	0,3	30
	Частота следования, кГц	1	1
Периодические наносекундные импульсы электромагнитного поля с высокой частотой повторения	Длительность импульса, нс	0,2 ± 0,1 0,8 ± 0,3	0,2 ±0,1 0,8 ±0,3
	Напряженность импульсного электрического поля, кВ/м	0,02	0,2
	Частота следования, кГц	1000	1000

Дополнительные сведения о средствах и способах ПС ЭМВ представлены в работах [100-108].

2.4. Описательная модель средств и способов информационно-технических воздействий

В рамках представленной модели сформированы обобщенная классификация и характеристики основных средств и способов ИТВ, направленных на объекты СС СН. Данные характеристики сформированы путем анализа тенденций развития ИТВ и их применения в локальных конфликтах на рубеже XX-XXI вв., представленных в работах [9, 10]. Ввиду существенных отличий в реализации ИТВ, решающих одну и ту же задачу, формирование типовых ТТХ, и базовых сценариев их проведения ИТВ является затруднительной. В связи с этим, в данном разделе представлены только основные сведения о наиболее распространенных типовых ИТВ, а более подробная информация о вариантах их практической реализации представлена в работе [9]. Кроме того, необходимо отметить, что данный тип воздействий является стремительно развивающимся, и в ближайшем будущем представленные в данном подразделе материалы могут претерпеть существенные изменения вследствие изменения самих концептуальных основ разработки и применения ИТВ.

2.4.1. Общая классификация информационно-технических воздействий и средств их реализации

Информационно-техническое воздействие – воздействие на информационный ресурс, информационную систему, информационную инфраструктуру, на технические средства или на программы, решающие задачи формирования,

передачи, обработки, хранения и воспроизведения информации, с целью вызвать заданные структурные или функциональные изменения.

Рассмотрим классификацию средств и способов ИТВ, направленных на объекты СС СН, взяв за основу классификацию, предложенную в работах [9, 17] и представленную на рис. 2.6.

Различают следующие виды ИТВ:

- одиночные;
- групповые.

По характеру поражающих свойств ИТВ классифицируют как:

- высокоточные – ИТВ, которые ориентированы на определенный информационный ресурс, процесс, технический объект или систему;
- комплексные – ИТВ, которые ориентированы на несколько информационных ресурсов, процессов, технических объектов или систем.

По типу воздействия на информацию или информационный ресурс ИТВ классифицируются следующим образом:

- пассивные:
  - перехват;
  - несанкционированный доступ;
- активные:
  - разрушающие воздействия;
  - манипулирующие воздействия;
  - блокирующие воздействия;
  - отвлекающие воздействия.

Пассивные ИТВ не оказывают непосредственного влияния на работу информационной системы, но могут нарушать ее политику безопасности. Именно отсутствие непосредственного влияния на функционирование информационной системы приводит к тому, что пассивные ИТВ трудно обнаружить. Примером пассивного ИТВ является сетевая компьютерная разведка.

Активные ИТВ оказывают непосредственное влияние на функционирование информационной системы (изменение ее конфигурации, нарушение работоспособности и т.д.) и нарушают принятую в ней политику безопасности. Очевидной особенностью активных ИТВ, в отличие от пассивных, является принципиальная возможность их обнаружения, так как в результате осуществления этих ИТВ в информационной системе происходят определенные деструктивные изменения.

По цели использования ИТВ классифицируются следующим образом:

- оборонительные;
- обеспечивающие;
- атакующие;
- комбинированные.

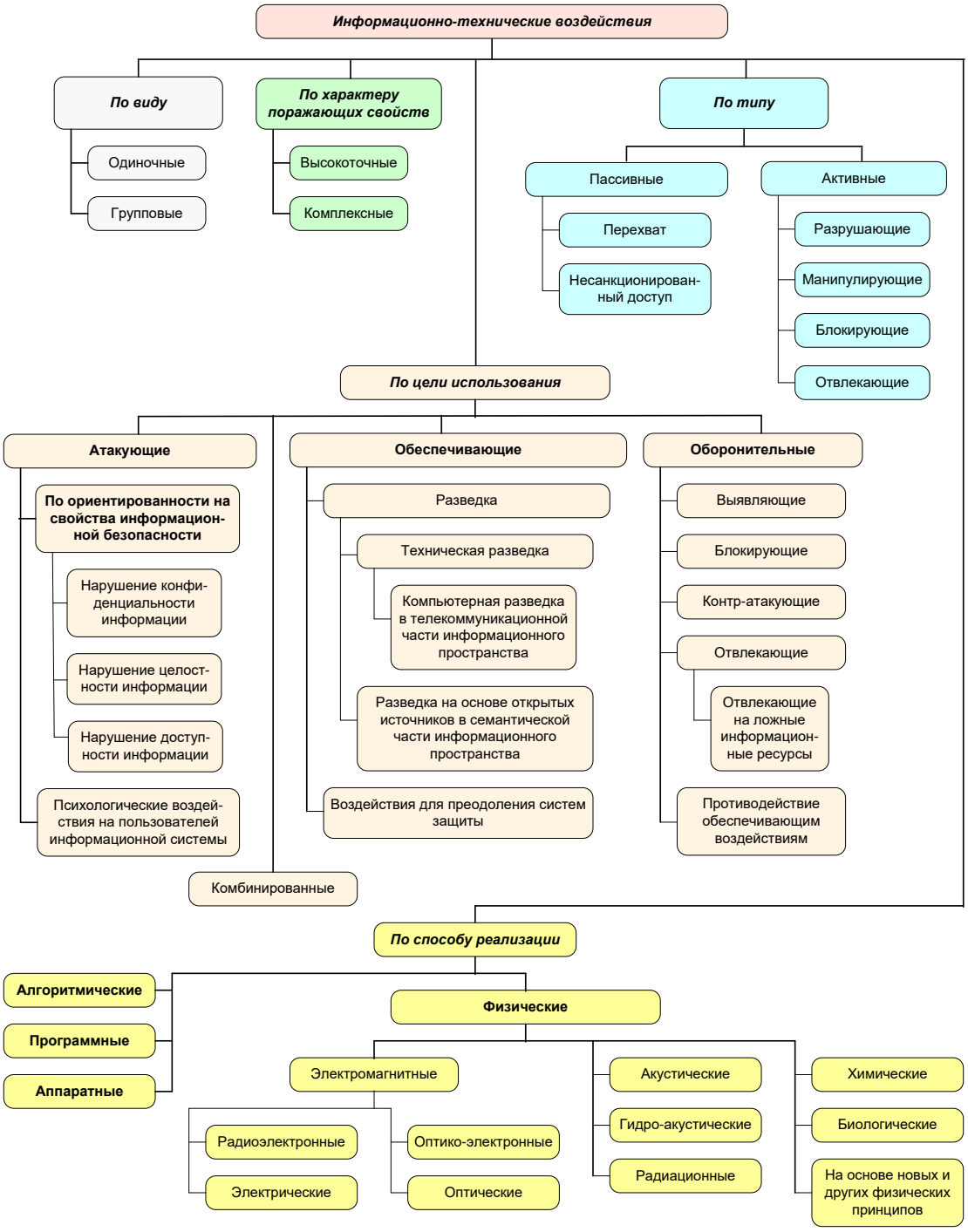

Рис. 2.6. Классификация ИТВ

Далее будут рассмотрены основные ИТВ, которые могут быть использованы для воздействия на объекты СС СН именно с учетом цели их применения.

Основные средства ИТВ можно классифицировать по способу реализации (рис. 2.7).

1) Алгоритмические (атакующие):
   - эксплойты, ориентированные на управляющую программу информационной системы (ядро или модули операционной системы, драйвера, BIOS);

- эксплойты, ориентированные на прикладные программы информационной системы (пользовательские приложения, серверные приложения, сетевые приложения, браузеры);
- эксплойты, ориентированные на сетевые протоколы информационной системы;
- эксплойты, ориентированные на перевод информационной системы или управляемой ею технологической системы в нештатные или технологически опасные режимы функционирования.

2) Программные:
   - атакующие:
     - компьютерные вирусы;
     - программные закладки;
     - нейтрализаторы тестовых программ и программ анализа кода;
   - обеспечивающие:
     - программные средства для моделирования боевых действий;
     - программные средства компьютерной разведки в телекоммуникационной части информационного пространства;
     - программные средства ведения разведки на основе открытых источников в семантической части информационного пространства;
   - оборонительные:
     - программные средства антивирусной защиты;
     - системы обнаружения и предотвращения вторжений;
     - программные средства криптографической защиты;
     - программные стеганографические средства обеспечения конфиденциальности, скрытности и целостности информационных ресурсов;
     - средства тестирования ПО и анализа кода для выявления программных закладок и недекларируемых возможностей;
     - средства создания ложных объектов и ресурсов в информационном пространстве.

3) Аппаратные:
   - атакующие:
     - аппаратные закладки;
   - оборонительные:
     - средства технического анализа элементной базы РЭС для выявления аппаратных закладок и недекларируемых возможностей.

4) Физические:
   - атакующие:
     - средства радиоэлектронного подавления;
     - средства оптико-электронного подавления;
     - средства ФП ЭМИ (генераторы электромагнитных импульсов, генераторы СВЧ-излучения, генераторы лазерного излучения);

- средства и комплексы функционального поражения преднамеренными силовыми электромагнитными воздействиями (генераторы электрического тока сверхвысокого напряжения);
- биологические и химические средства воздействия на элементную базу РЭС, токонесущие элементы и проводники (например, графитовые бомбы).

- обеспечивающие:
  - средства технической разведки (в том числе и средства компьютерной разведки).

Общая схема классификации средств ИТВ представлена на рис. 2.7.

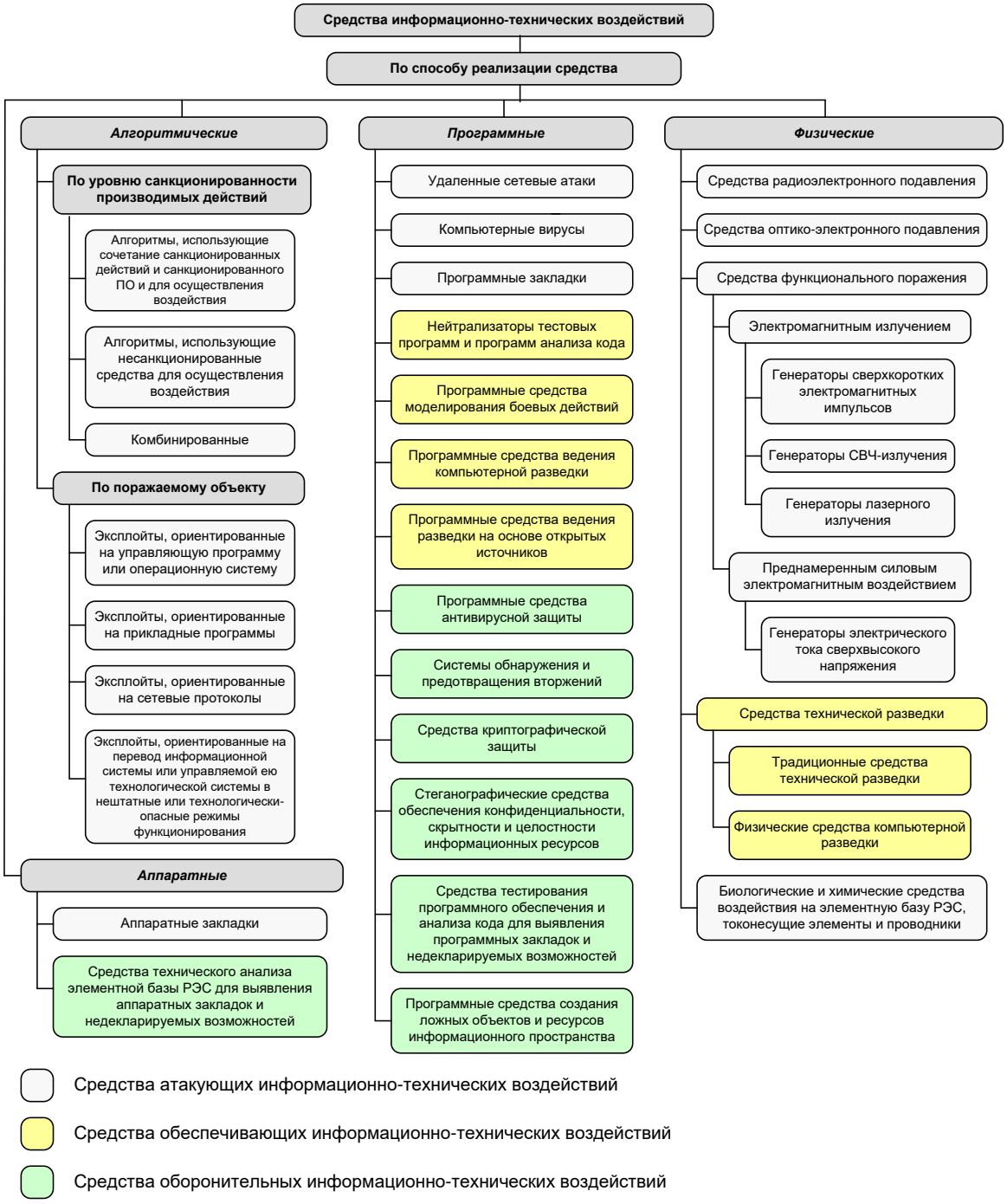

Рис. 2.7. Классификация средств ИТВ

Отдельно необходимо отметить следующее. К средствам технической разведки, представленным в данной классификации, относятся те средства, которые добывают информацию об атакующих источниках ИТВ и способах их применения, таким образом, средства технической разведки являются средствами обеспечивающего ИТВ. Средства технической разведки могут оказывать воздействие на информационные системы как путем пассивных воздействий, направленных на добывание информации, что, как правило, связанно с нарушением ее конфиденциальности, так и путем активных действий (атак), направленных на создание условий, которые благоприятствуют добыванию информации.

2.4.2. Оборонительные информационно-технические воздействия

Оборонительные ИТВ ориентированы на противодействие обеспечивающим и атакующим ИТВ нарушителя/противника. Эти средства, в подавляющем числе работ, рассматриваются как основной элемент обеспечения информационной безопасности (ИБ), но не как средства оборонительных ИТВ. На взгляд автора это является не совсем правильным, так как именно оборонительные средства играют одну из ведущих ролей в информационном противоборстве при организации защиты объектов СС СН.

К средствам оборонительных ИТВ можно отнести:

- средства антивирусной защиты;
- системы обнаружения и предотвращения вторжений, системы управления информационной безопасностью;
- средства криптографической защиты;
- стеганографические средства обеспечения конфиденциальности, скрытности и целостности информационных ресурсов;
- средства технического анализа элементной базы РЭС для выявления аппаратных закладок и недекларируемых возможностей;
- средства тестирования ПО и анализа кода для выявления программных закладок и недекларируемых возможностей;
- средства создания ложных объектов и ресурсов в информационном пространстве.

Средства и способы оборонительных ИТВ можно классифицировать следующим образом (рис. 2.7):

- *выявляющие* – ориентированы на выявление как самого факта, так и последовательности атакующих и обеспечивающих ИТВ со стороны нарушителя/противника;
- *блокирующие* – ориентированы на блокировку атакующих ИТВ нарушителя/противника;
- *контратакующие* – воздействия на информацию, информационные ресурсы и информационную инфраструктуру нарушителя/противника с целью срыва его атакующих ИТВ;

- *отвлекающие* – ориентированы на дезинформацию нарушителя/противника, отвлечение его атакующих или обеспечивающих ИТВ на второстепенные или ложные объекты;
- *противодействие обеспечивающим воздействиям противника* – средства и способы маскировки, обеспечения безопасности, повышения скрытности реальных режимов функционирования, а также мониторинга каналов утечки в отношении собственных информационных систем.

В целом, средства и способы вышеуказанных оборонительных ИТВ довольно широко описаны в известной литературе, поэтому здесь подробно не рассматриваются.

2.4.3. Обеспечивающие информационно-технические воздействия

Обеспечивающие ИТВ представляют собой воздействия, которые применяются для сбора данных, обеспечивающих эффективное применение оборонительных или атакующих ИТВ, а также для преодоления средств защиты атакуемой системы.

Обеспечивающие ИТВ можно классифицировать следующим образом.

- Средства разведки:
  - традиционные средства технической разведки, классифицированные по физическим средам, в которых ведется добывание информации;
  - средства компьютерной разведки (как программные средства, так и средства доступа к физической инфраструктуре);
  - средства ведения разведки на основе открытых источников.
- Средства преодоления систем защиты.

Необходимо отметить, что в подавляющем числе случаев, в качестве обеспечивающих ИТВ выступают именно средства технической разведки. Именно они позволяют получить информацию об атакующих средствах ИТВ нарушителя/противника и способах его применения, что позволяет более рационально сконфигурировать собственные средства защиты. Воздействие средств разведки проявляется как в виде пассивных действий, направленных на добывание информации и, как правило, связанных с нарушением ее конфиденциальности, так и активных действий, направленных на создание условий, благоприятствующих добыванию информации.

Обеспечивающие ИТВ, ориентированные на ведение компьютерной разведки, а также средства технической разведки подробно насмотрены в 3-ей главе данной монографии.

2.4.4. Атакующие информационно-технические воздействия

Атакующие ИТВ ориентированы на непосредственное воздействие на информацию, системы ее сбора, передачи, хранения, обработки и представления, а также на используемые в этих системах информационные технологии, как правило, с целью снижения уровня ИБ или эффективности функционирова-

ния соответствующих информационных систем. Применение атакующих ИТВ направлено на срыв выполнения информационной системой своих целевых задач.

Далее кратко описаны классификация и основные типы атакующих ИТВ, а более подробная информация об атакующих ИТВ представлена в работе [9].

2.4.4.1. Классификация атакующих информационно-технических воздействий

Классификация средств и способов атакующих ИТВ представлена на рис. 2.8.

Атакующие ИТВ, в зависимости от их ориентированности на нарушение конкретного свойства ИБ, можно классифицировать на четыре основных типа:

- ориентированные на нарушение конфиденциальности информации;
- ориентированные на нарушение целостности информации;
- ориентированные на нарушение доступности информации;
- ориентированные на психологическое или информационно-психологическое воздействие на пользователей информационной системы [11].

По способу реализации ИТВ классифицируются на:

- алгоритмические:
  - эксплойты, ориентированные на управляющую программу информационной системы (ядро или модули операционной системы, драйвера, BIOS);
  - эксплойты, ориентированные на прикладные программы информационной системы (пользовательские приложения, серверные приложения, сетевые приложения, браузеры);
  - эксплойты, ориентированные на сетевые протоколы информационной системы;
  - эксплойты, ориентированные на перевод информационной системы или управляемой ею технологической системы в нештатные или технологически опасные режимы функционирования;
- программные:
  - компьютерные вирусы;
  - программные закладки;
  - нейтрализаторы тестовых программ и программ анализа кода;
- аппаратные:
  - аппаратные закладки;
- физические:
  - электромагнитные:
    - радиоэлектронное подавление;
    - оптико-электронное подавление;
    - ФП ЭМИ (электромагнитные импульсы, СВЧ-излучение, лазерное излучение);
    - функциональное поражение преднамеренными силовыми электромагнитными воздействиями (электрический ток сверхвысокого напряжения);

- по другим полям (акустическим, радиационным и др.);
- биологические и химические средства воздействия на элементную базу РЭС, токонесущие элементы и проводники.

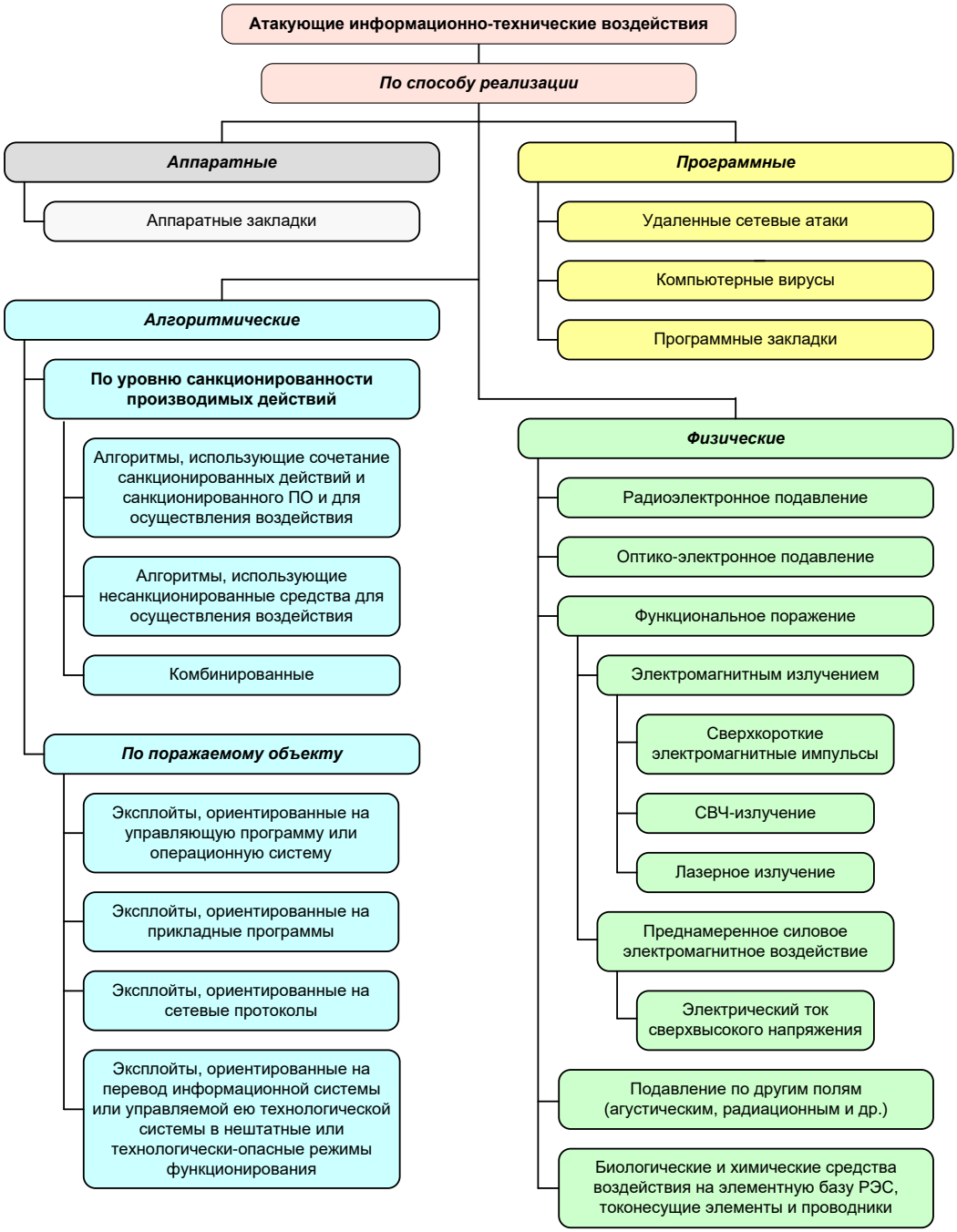

Рис. 2.8. Классификация средств и способов атакующих ИТВ

Рассмотрим более подробно основные, широко распространенные атакующие ИТВ, которые могут быть использованы для дестабилизирующего воздействия на объекты СС СН:

- удаленные сетевые атаки;
- компьютерные вирусы;
- программные закладки;
- аппаратные закладки.

2.4.4.2. Удаленные сетевые атаки

Удаленная сетевая атака – это атакующее ИТВ, осуществляемое по каналам связи, удаленным относительно атакуемой системы, субъектом и характерное для структурно- и пространственно-распределенных информационных систем. Удаленные сетевые атаки можно классифицировать в соответствии с различными основаниями. Общая схема классификации удаленных сетевых атак представлена на рис. 2.9, а классификация способов их осуществления – на рис. 2.10.

В настоящее время атаки типа «отказ в обслуживании» являются наиболее распространенными и наиболее опасными удаленными сетевыми атаками. Атака «отказ в обслуживании» направлена на блокировку доступа к объекту путем исчерпания его ресурсов. Классификация основных способов осуществления атаки «отказ в обслуживании» представлена на рис. 2.11.

Более подробная информация по удаленным сетевым атакам приведена в работе [9].

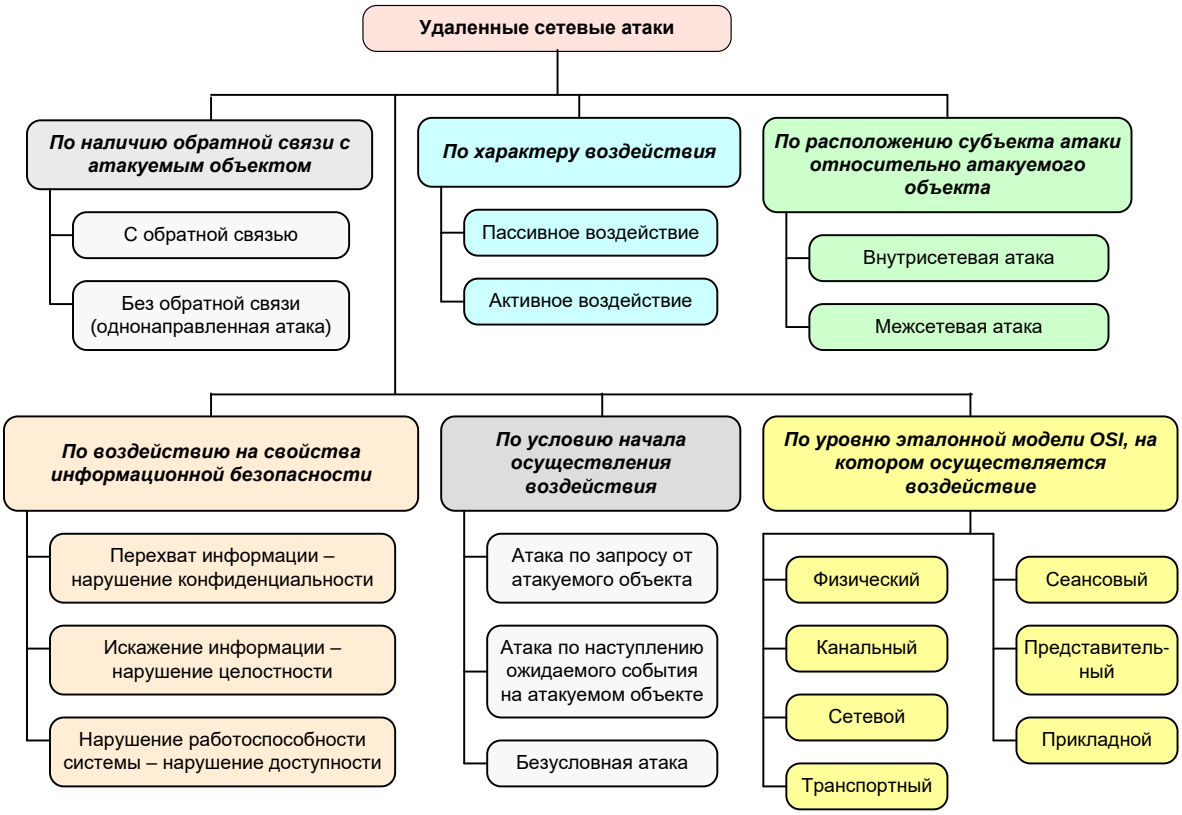

Рис. 2.9. Классификация удаленных сетевых атак

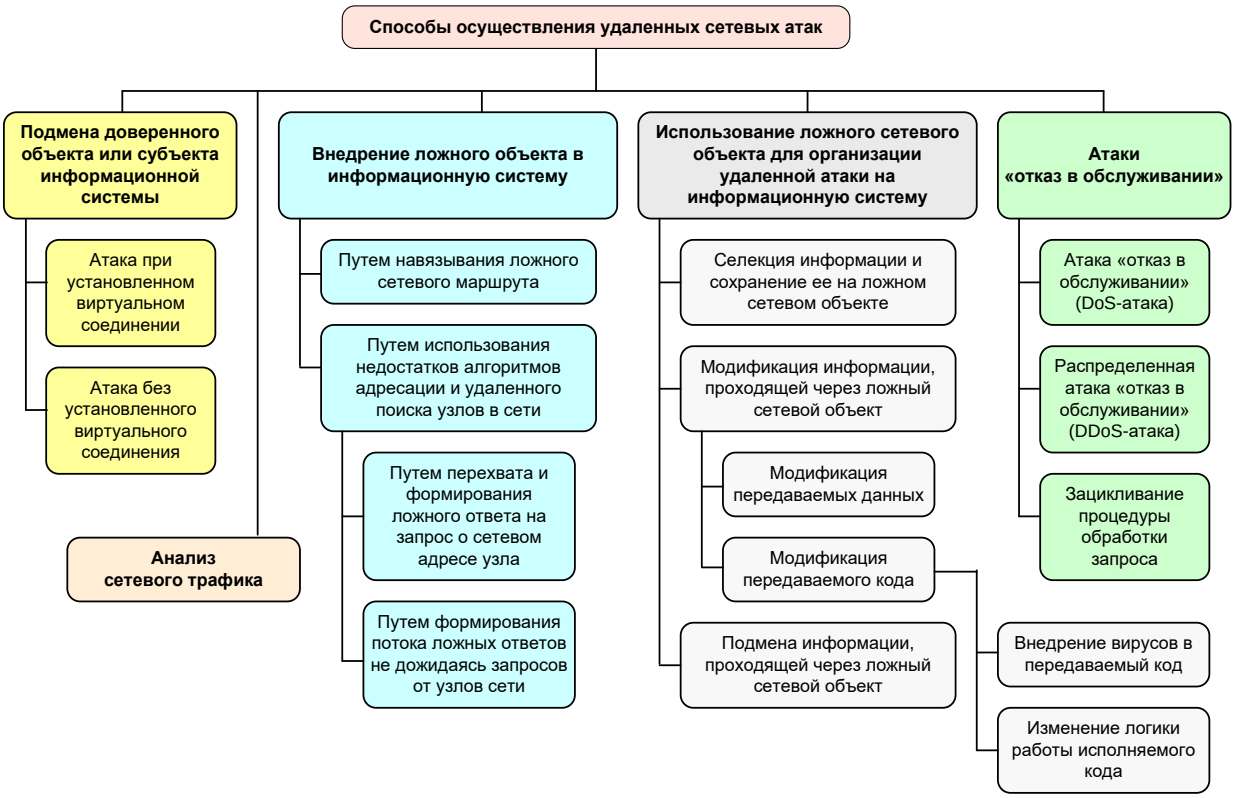

Рис. 2.10. Классификация способов осуществления удаленных сетевых атак

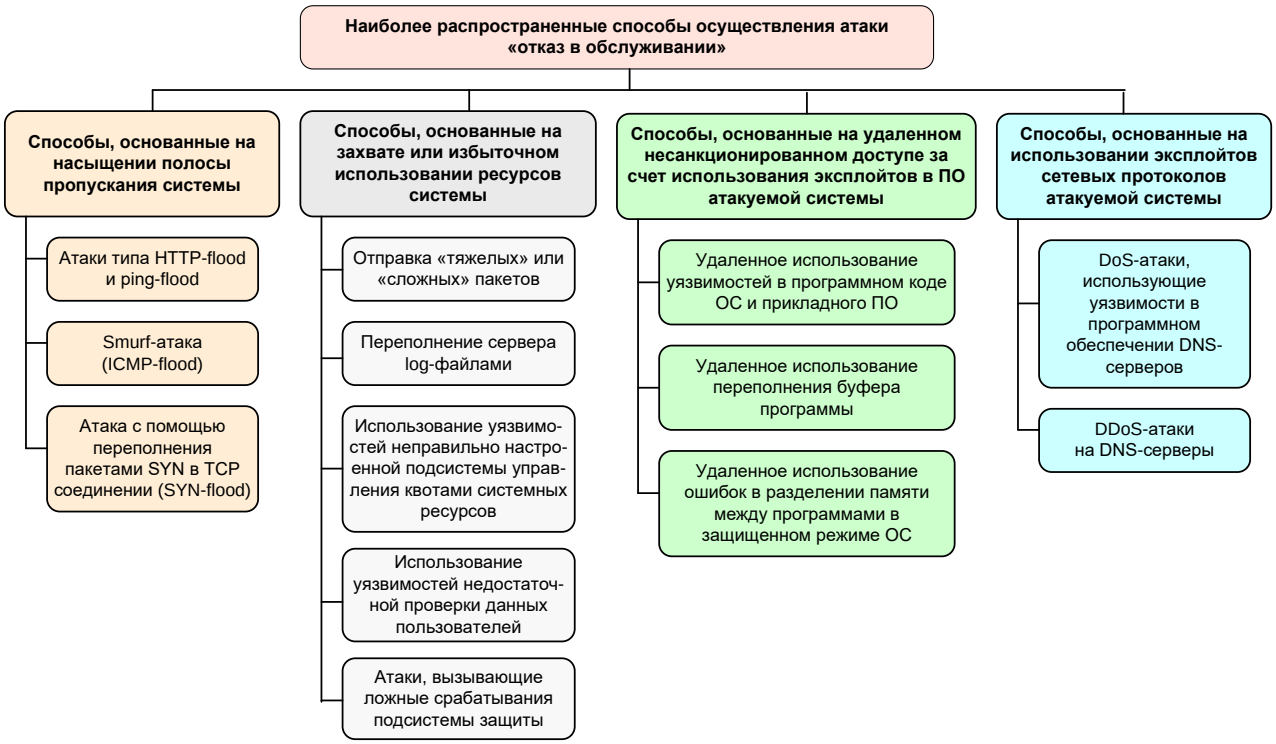

Рис. 2.11. Наиболее распространенные способы осуществления атаки «отказ в обслуживании»

2.4.4.3. Компьютерные вирусы

Несмотря на долгую историю компьютерной вирусологии, использование вирусов в качестве боевых средств ИТВ начато сравнительно недавно. К первому случаю такого использования относится использование в 2010 г. вируса Stuxnet [9].

Вирус – программа, несанкционированно внедренная в информационную систему и способная осуществлять создание собственных дубликатов (не всегда совпадающих с оригиналом), несанкционированное самораспространение, несанкционированный доступ к информационным ресурсам, изменение логики функционирования зараженной программы, снижение качества или эффективности информационной системы.

Особенностью современных боевых вирусов является то, что они, как правило, являются комплексными продуктами и состоят из различных модулей, которые относятся к различным типам и ориентированы на решение конкретной задачи (модули типа «классический вирус» – для саморазмножения в информационной системе, модули типа «червь» – для распространения по сети, модуль типа «троян» – для организации дестабилизирующего воздействия).

Классификация атакующих средств на основе компьютерных вирусов представлена на рис. 2.12.

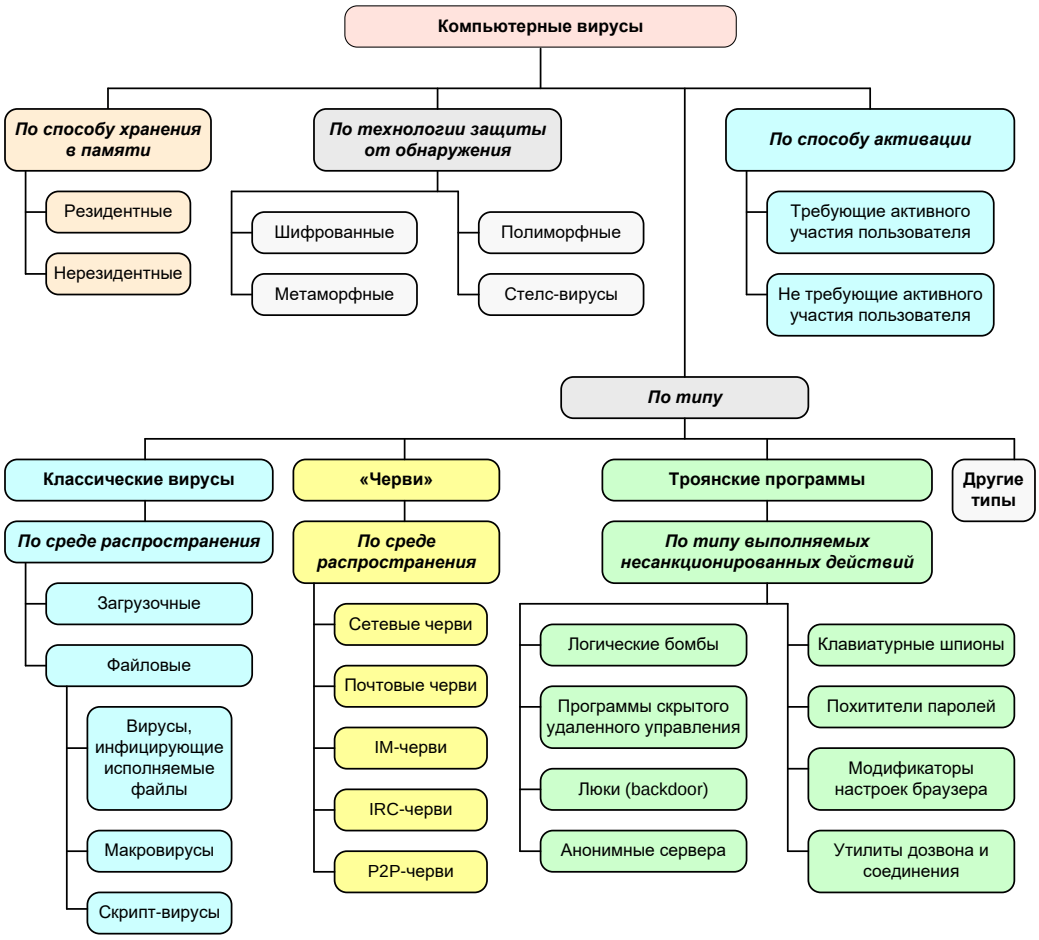

Рис. 2.12. Классификация компьютерных вирусов

Средства ИТВ на основе вирусов обладают следующими особенностями функционирования относительно других «непрофессиональных» вирусных средств [9]:

- избирательность цели и действий;
- использование уязвимостей, в том числе уязвимостей 0-дня, закладок и скрытых каналов;
- маскировка, скрытность, криптозащита, самоликвидация;
- широкая функциональность в плане решения целевых задач;
- гибкая система саморазмножения;
- инфраструктурная поддержка, обновление и управление;
- масштабируемость, наличие СУБД-атак;
- высокое качество кода и возможности обработки некорректных ситуаций.

Более подробная информация о вирусных средствах ИТВ представлена в работе [9].

2.4.4.4. Программные закладки

Программная закладка – скрытно внедренная в защищенную информационную систему программа либо намеренно измененный фрагмент программы, которая позволяет осуществить несанкционированный доступ к ресурсам системы на основе изменения свойств системы защиты [96]. При этом закладка может внедряться самим разработчиком ПО для реализации в информационной системе некоторых сервисных или недекларируемых функций.

Классификация программных закладок представлена на рис. 2.13.

Программные закладки, получая несанкционированный доступ к данным в памяти информационной системы, перехватывают их. После перехвата эти данные копируются и сохраняются в специально созданных разделах памяти или передаются по сети. Программные закладки, подобно вирусам, могут искажать или уничтожать данные, но, в отличие от вирусов, деструктивное действие таких программ, как правило, более выборочно и направлено на конкретные данные. Довольно часто программные закладки играют роль перехватчиков паролей, сетевого трафика, а также служат в качестве скрытых интерфейсов для входа в систему. Однако, в отличие от вирусов, программные закладки не обладают способностью к саморазмножению, они встраиваются в ассоциированное с ними программное обеспечение и латентно функционируют вместе с ним. При этом особенностью закладок, внедренных на стадии разработки ПО, является то, что они становятся фактически неотделимы от прикладных или системных программ информационной системы [97].

Как и вирус, программная закладка должна скрывать свое присутствие в программной среде информационной системы. Однако программные закладки невозможно обнаружить при помощи стандартных антивирусных средств, их выявление возможно только специальными тестовыми программами, выявляющими аномальное поведение и недекларируемые возможности ПО. В связи с этим, средства маскировки программных закладок преимущественно ориентированы на противодействие отладчикам программ, анализаторам кода и дисас-

семблерам. В качестве одного из широко применяемых способов маскировки является обфускация программ, в которые внедрена закладка [97].

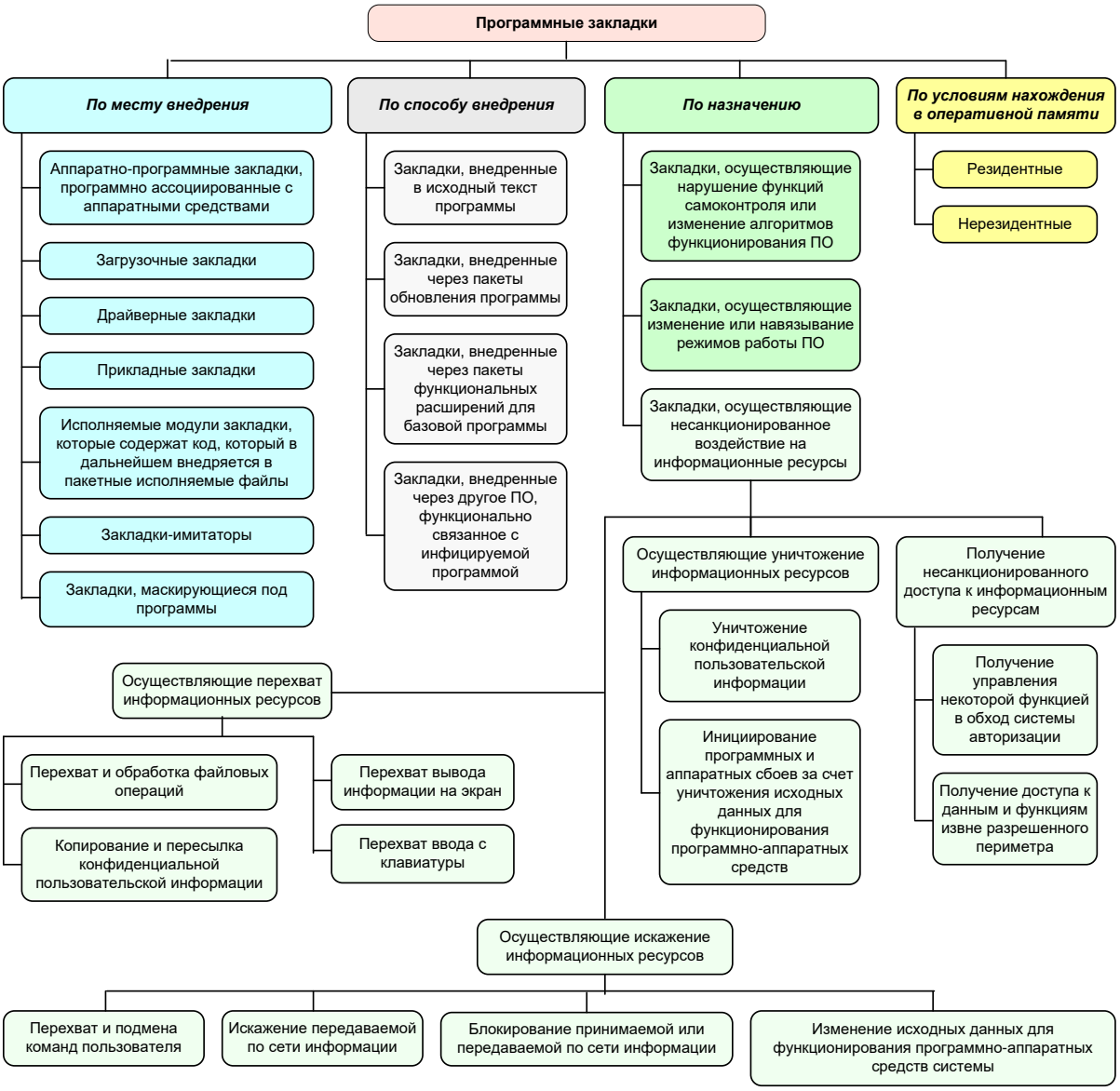

Рис. 2.13. Классификация программных закладок

2.4.4.5. Аппаратные закладки

Аппаратная закладка – электронное устройство, скрытно внедряемое к остальным элементам, которое способно вмешаться в работу аппаратных или технических средств информационной системы.

Результатом работы аппаратной закладки может быть, как полное выведение системы из строя, так и нарушение корректности ее функционирования, например, несанкционированный доступ к информации, ее изменение или блокирование [98].

Схематическая сложность современного микроэлектронного оборудования и тенденции к миниатюризации его элементов ведут к тому, что производители такого оборудования могут бескомпроматно и практически неограниченно наращивать функциональные возможности аппаратных закладок, функционирующих в интересах тестирования такого оборудования, а при подклю-

чении устройств к глобальной сети – осуществлять обновление алгоритма их функционирования, а также условий срабатывания.

Классификация аппаратных закладок приведена на рис. 2.14 [9]. Краткая характеристика технологий современных аппаратных закладок представлена в таблице 2.10 [99].

Таблица 2.10 – Технологии современных аппаратных закладок [99]

Методы внедрения	Методы обнаружения	Методы маскировки
Встраивание закладок в технологию микроядра управления в современных СБИС, построенного на уникальном списке команд (управление основной работой и блокировка и замена неисправных узлов для продления срока службы СБИС)	Технологии послойного сканирования кристаллов	Механизм технологической защиты топологии кристалла от послойного сканирования (впервые внедрен в i486)
	Вычитывание и дизассемблирование аппаратно доступных микрокодов	Размещение микроядер с закладками и ресурсов памяти в области, недоступной пользователю. Шифрование (мутирование) участков кода, антитрассировка
Виртуализация вычислений	Анализ контента проходящих по сети данных	
Встраивание целевых микроядер и узлов, реализующих стратегию влияния	Мониторинг аномальной активности платформы. Радиомониторинг. Электромагнитный контроль.	

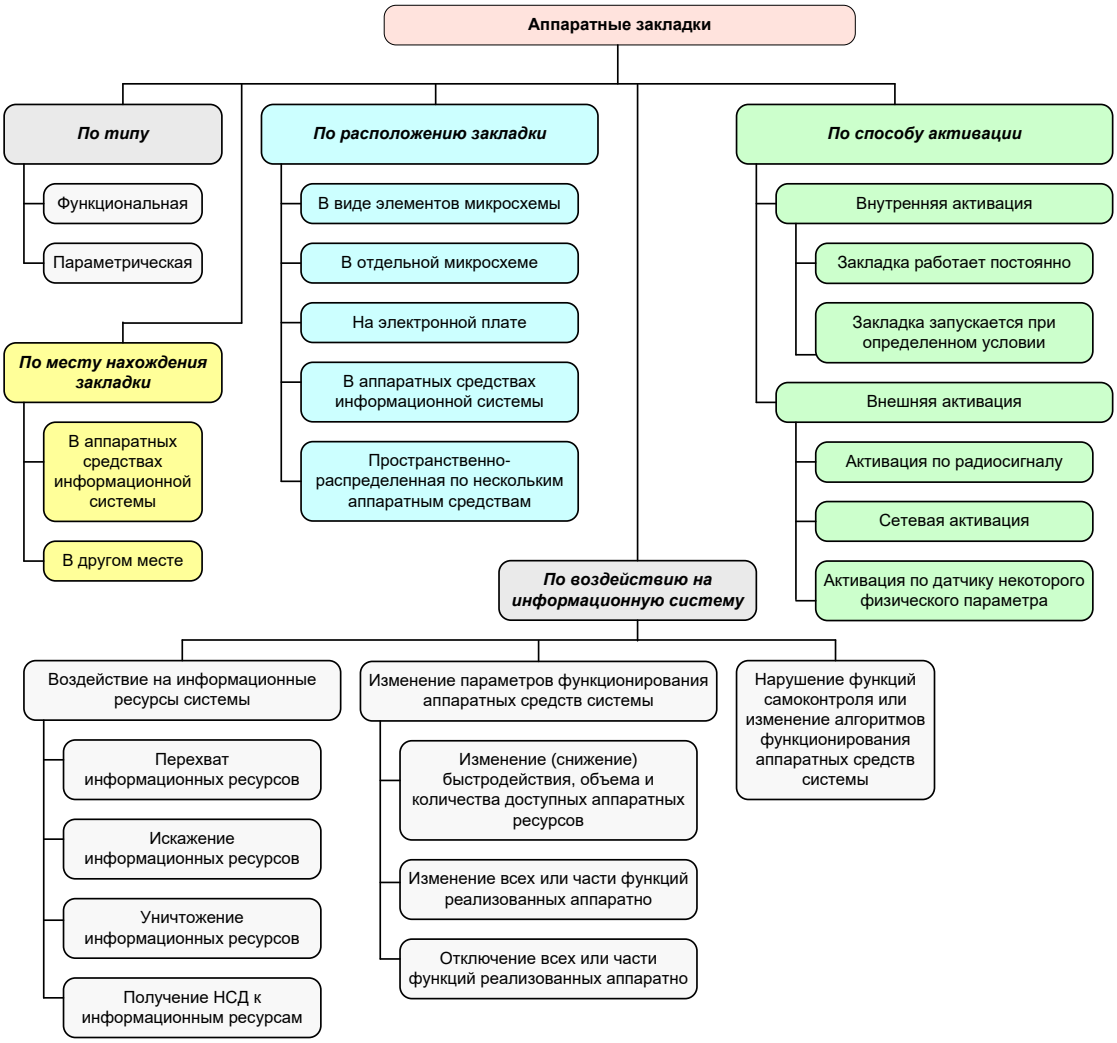

Рис. 2.14. Классификация аппаратных закладок

Выводы по второй главе

Преднамеренные дестабилизирующие воздействия – это основной фактор, влияющий на устойчивость СС СН. При этом, подавляющую часть преднамеренных воздействий на СС СН можно объединить в три основных категории:

1) физическое поражение элементов СС СН обычным оружием, а также оружием на новых физических принципах, работающим по принципу физического поражения (рельсотроны, гиперзвуковые средства поражения);
2) воздействие на элементы СС СН средств РЭБ, а также оружия на новых физических принципах, работающего по принципу функционального поражения электромагнитным излучением (средства создания мощных электромагнитных импульсов, излучатели направленной энергии, генераторы мощного электрического тока, лазерное оружие);
3) воздействие на элементы СС СН средств и способов ИТВ.

Отметим, что, будучи рассматриваемым отдельно, фактор физического поражения соответствуют снижению свойства живучести СС СН, а фактор воздействия средств РЭБ – снижению помехоустойчивости (рис. 1.4). При этом, в настоящее время, отсутствует общепринятое наименование категории, которая определяет вклад в снижение устойчивости СС СН со стороны средств и способов ИТВ. Отдельные авторы вводят понятия «киберустойчивости», «функциональной устойчивости» и т.д., однако эти термины, как и показатели их оценки, не являются, на данный момент, общепризнанными, а в некоторых случаях, еще и довольно спорными.

В данной главе представлены описательные модели основных типов преднамеренных воздействий на СС СН с учетом их перспективного развития в период до 2030 г., которые могут быть использованы при формировании исходных данных при оценке устойчивости (живучести, помехоустойчивости) СС СН в соответствующих моделях, а также при разработке методов, методик и способов повышения соответствующих показателей СС СН.

3. Описательная модель систем и средств разведки

3.1. Общие подходы к разведке систем связи специального назначения

Анализ тенденций развития сил и средств разведывательного обеспечения, представленный в работе [10], показал, что в эпоху информатизации систем государственного и военного управления во многом изменился характер выполнения своих задач разведкой. Если ранее основной задачей разведки являлось опережающее оповещение высшего руководства страны о возможной агрессии, то сейчас на силы и средства разведки возлагаются задачи заблаговременного вскрытия систем государственного и военного управления, а также постоянного мониторинга циркулирующих в этих системах информационных потоков в интересах достижения полного информационного превосходства над противником. В результате, ведущие в технологическом отношении страны приступили к формированию единого информационно-разведывательного пространства, объединяющего в себе все информационные ресурсы сил и средств разведки (различной видовой принадлежности, различных ведомств и даже стран), которые обновляются и обрабатываются в режиме времени, близком к реальному.

Отличительной особенностью современных подходов к разведке СС СН является тренд на плотную интеграцию радио-, радиотехнической и компьютерной разведок, которые в мирное время не только вскрывают местоположения узлов связи, используемое ими аппаратное и программное обеспечения, но и решают важнейшую задачу получения доступа к оперативно ценным информационным потокам, циркулирующим в системах государственного и военного управления. В угрожаемый период и в военное время, роль компьютерной разведки снижается и традиционно главенствующую роль играют средства РРТР, причем современные тенденции показывают возрастающую роль средств космического и авиационного базирования [10].

Проведенный в работе [10] анализ перспектив развития систем разведывательного обеспечения, а также анализ военных конфликтов показал наличие следующих тенденций, относительно разведки объектов и режимов работы СС СН:

1) в мирное время:
   - осуществляется заблаговременное внедрение вирусов, аппаратных и программных закладок как в оборудование СС СН, так и в оборудование СС ОП, работающих совместно с СС ОП, в интересах ведения вирусной и алгоритмический компьютерной разведки;
   - ведется компьютерная разведка (сетевая, потоковая, аппаратная) против элементов СС СН, сопряженных с сегментами СС ОП, которые являются потенциально уязвимыми перед атакующими ИТВ;

- ведется совместная радио- и компьютерная разведка (семантическая, форматная, пользовательская), направленная на идентификацию лиц высшего командного состава, вскрытие местоположения ПУ и узлов связи, дислокации сил и средств, схем организации связи, которые в дальнейшем используются для целеуказания при ведении ИПБ и РЭБ в военное время и в угрожаемый период;
- ведется радио- и радиотехническая, оптико-электронная космическая разведка, направленная на получения сведений о местоположении ПУ и узлов связи, дислокации сил и средств, которые в дальнейшем используются для целеуказания при поражении вскрытых объектов средствами ВТО и при ведении РЭП.

2) в военное время:
- средствами радио-, радиотехнической, оптико-электронной разведки космического и воздушного базирования производится доразведка заблаговременно вскрытых элементов СС СН в интересах формирования окончательных данных целеуказаний на поражение элементов СС СН средствами ВТО;
- ведется компьютерная разведка (сетевая, потоковая, аппаратная) в сетях СС СН, сопряженных с СС ОП, в интересах добывания как оперативно ценной информации, так и в интересах формирования целеуказаний для атакующих ИТВ;
- основным средством получения разведывательных сведений о стационарных и мобильных объектах СС СН в стратегическом и оперативном звене управления становятся космические системы радио-, радиотехнической и оптико-электронной разведки, информация от которых обрабатывается комплексно с данными СРНС и позволяет точно определить местонахождение критически важных узлов связи и ПУ;
- источниками разведывательных сведений в тактическом звене становятся практически все средства вооружения, имеющие радио- и радиотехические, оптические, электронные датчики, а также все участники боевых действий;
- за счет комплексирования разнотиповых средств разведки резко снижается продолжительность цикла ведения разведки с одновременным увеличением ее достоверности и полноты;
- все большее распространение в качестве оперативных средств ведения разведки получают средства авиационного базирования, в том числе и на БПЛА. При этом перспективным направлением является создание на основе БПЛА разведывательно-ударных комплексов, реализующих принцип «обнаружил – уничтожил»;
- передача разведсведений от средств добывания и обеспечение разведывательной информацией потребителей производятся в едином информационно-разведывательном пространстве в соответствии с уровнем допуска потребителей и их принадлежностью к конкретному уровню управления;

- обработка разведывательных данных ведется с использованием суперкомпьютерных технологий на основе интеллектуальных методов обработки «Больших данных» в масштабе времени, близкому к реальному, и предусматривает формирование единого виртуального театра военных действий на основе комплексирования данных от всех разведывательных источников.

Таким образом, для вскрытия элементов СС СН, критически важными являются следующие виды разведки:

- радио- и радиотехническая разведка, ориентированная на вскрытие местоположения источников радиоизлучений (ИРИ), которые потенциально могут принадлежать абонентам или элементам СС СН, местоположения абонентов, а также содержания радиообмена с последующим формированием целеуказаний для средств поражения ВТО и средств РЭБ;
- компьютерная разведка, ориентированная на вскрытие структуры организации связи; используемых протоколов, программного и аппаратного обеспечения; уязвимостей в подсистеме обеспечения ИБ; получения доступа к оперативно ценной информации, циркулирующей в системах государственного и военного управления, с последующим формированием целеуказаний для атакующих ИТВ;
- оптико-электронная разведка, ориентированная на уточнение местоположения и классификацию типов ИРИ (ранее вскрытых средствами РРТР) как объектов СС СН; вскрытие стационарных и мобильных ПУ, узлов связи; вскрытие местоположения узлов и ретрансляторов связи, мест прокладки кабельных, оптико-волоконных и других линий связи, обладающих высокой скрытностью в радиодиапазоне.

3.2. Общие сведения о технической разведке

Техническая разведка – целенаправленная деятельность по добыванию информации с помощью технических средств [117].

Доля технической разведки, в общей системе добывания защищаемой информации, достаточно велика и, по некоторым оценкам, может составлять до 50% и более. Причем дальнейшее развитие науки и техники объективно приводит к повышению роли и значимости технической разведки [118].

При анализе технических средств разведки используют различные классифицирующие признаки. Классификация средств технической разведок приведена на рис. 3.1.

Для разведки используются различные каналы утечки информации, которые по используемой физической среде (полю) классифицируются следующим образом [118, 120]:

- радиоканалы (электромагнитные излучения радиодиапазона);
- акустические каналы (звуковые колебания в звукопроводящей среде);
- электрические каналы (напряжения и токи в токопроводящих коммуникациях);

- оптические каналы (электромагнитные излучения в инфракрасной, видимой и ультрафиолетовой частях спектра);
- материально-вещественные каналы (фото, бумажные и магнитные носители, отходы, выбросы и т. д.);
- другие каналы (радиационные, магнитометрические и т.д.).

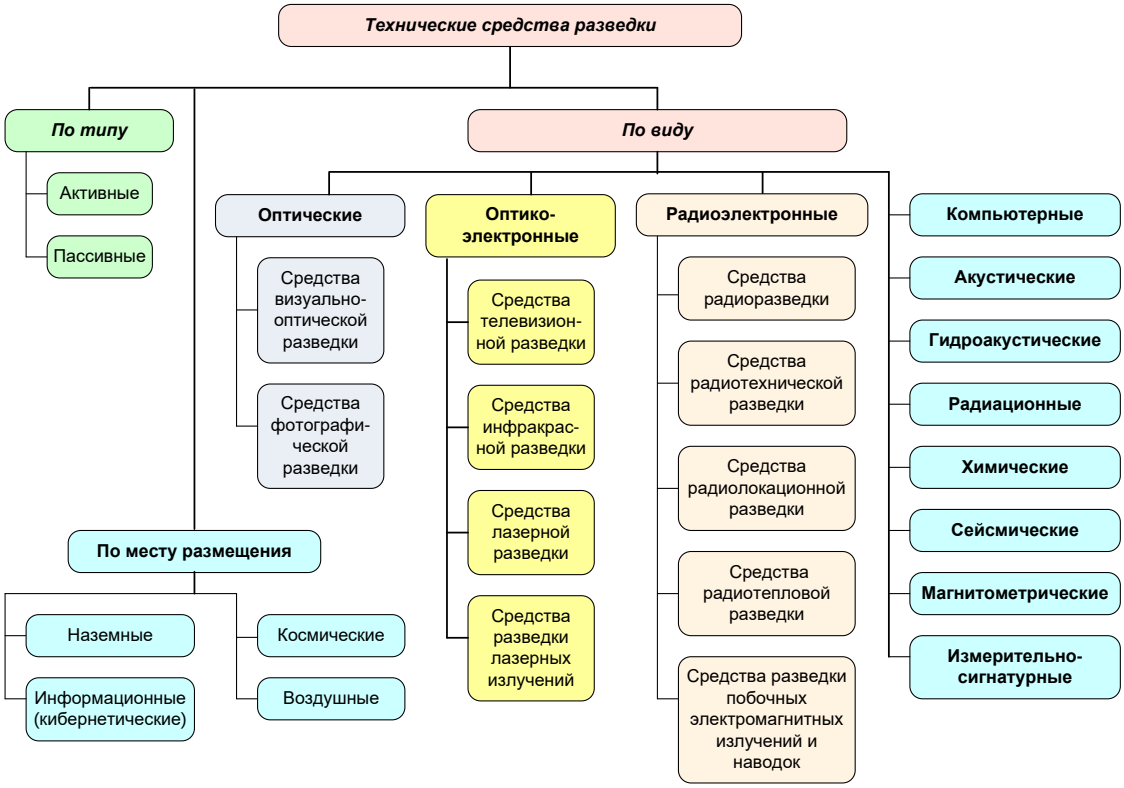

Рис. 3.1. Классификация технических средств разведки [119]

Выделяют следующие виды технической разведки, которые используют соответствующие средства и каналы утечки информации [117, 120]:

- радиоэлектронную;
- оптическую;
- оптико-электронную;
- акустическую;
- гидроакустическую;
- химическую;
- радиационную;
- сейсмическую;
- магнитометрическую;
- компьютерную;
- измерительно-сигнатурную.

Далее, на основании материала, представленного в работе [117], более подробно рассмотрены основные виды разведок, решающие задачи вскрытия объектов, элементов, режимов работы и схем организации связи в СС СН:

- радио- и радиотехническая разведка;
- оптико-электронная разведка;
- компьютерная разведка.

3.3. Описательная модель систем и средств радио- и радиотехнической разведки

Радиоэлектронная разведка (РЭР) – процесс получения информации в результате приема и анализа электромагнитных излучений радиодиапазона, создаваемых работающими радиоэлектронными средствами [117].

Составной частью радиоэлектронной разведки являются радиоразведка и радиотехническая разведка.

Радиоразведка (РР) – вид радиоэлектронной разведки, ориентированной на различные виды радиосвязи, основным содержанием которой является: обнаружение и перехват открытых, засекреченных, кодированных передач связных радиостанций; пеленгование их сигналов; анализ и обработка добываемой информации с целью вскрытия ее содержания и определения местонахождения ИРИ; снижение нагрузки или подрыв криптографических систем [117].

Радиотехническая разведка (РТР) – вид радиоэлектронной разведки, целью которой являются сбор и обработка информации, получаемой с помощью РЭС о радиоэлектронных системах противника по их собственным излучениям, и последующая их обработка с целью получения информации о положении источника излучения, его скорости, наличии данных в излучаемых сигналах.

Объектами РТР являются: радиотехнические устройства различного назначения (РЛС, импульсные системы радиоуправления, радиотелекодовые системы, а также ЭМИ, создаваемые работающими электродвигателями, электрогенераторами, вспомогательными устройствами и т.п.) [117].

Средства РТР позволяют:

- установить несущую частоту передающих радиосредств;
- определить координаты источников излучения;
- измерить параметры импульсного сигнала (частоту повторения, длительность и другие параметры);
- установить вид модуляции сигнала (амплитудная, частотная, фазовая, импульсная);
- определить структуру боковых лепестков излучения радиоволн;
- определить поляризацию радиоволн;
- установить скорость сканирования антенн и метод обзора пространства РЛС;
- проанализировать и записать информацию.

Необходимо отметить, что средства РР ориентированы, главным образом, на перехват и выделение семантического содержания передаваемых сообщений, а средства РТР – на определение параметров сигналов, их накопление с целью формирования радиоэлектронного портрета ИРИ, и его последующее отождествление с конкретным образцом вооружения или военной техники (ВВТ). Однако особенностью нынешнего этапа развития средств РР и РТР является, во-первых, невозможность дешифровки сообщений, которые в подавляющем большинстве передаются в зашифрованном виде, во-вторых, средствам РРТР на современном этапе их развития, свойственна определенная универсальность относительно объектов разведки [189]. При этом отнесение тех или иных объ-

ектов СС СН к объектам РР или РТР может быть произведено уже после обработки результатов разведки и классификации вскрытых объектов. Такая тенденция не позволяет утверждать об ориентированности на вскрытие объектов СС СН исключительно средств РР, а требует учитывать возможности интегрированных средств РРТР при оценке разведзащищенности СС СН.

Основными способами обнаружения сигналов, используемыми системами РРТР, являются [91]:

- непрерывное сканирование диапазона частот;
- дискретное сканирование полосы частот;
- комбинированное сканирование.

Различные диапазоны систем связи характеризуются следующими параметрами, значимыми для средств разведки [91]:

- приоритет;
- скорость сканирования;
- порог обнаружения;
- исключение сигналов, не представляющих интереса.

Вероятность обнаружения РЭС систем радиосвязи зависит от отношения скорости сканирования к длительности принимаемых сигналов. Например, при продолжительности связи в УКВ-диапазоне, равной нескольким секундам, скорость сканирования в этом диапазоне, равная 20-50 МГц/с, будет являться приемлемой [91].

Чувствительность приемников разведывательных устройств в КВ- и УКВ-диапазонах с широкополосными антеннами лежит в пределах 0,5-5 мкВ/м, а разрешающая способность по частоте находится в пределах 20-30 кГц [91].

Сложнее обстоит дело с перехватом сигналов средств радиосвязи, которые используют режимы псевдослучайной перестройки рабочей частоты (ППРЧ). В этом случае средствам РРТР необходимо дополнительно вскрыть программу, по которой изменяется ППРЧ [92].

Современные цифровые приемные устройства, работающие в режиме радиомониторинга в диапазоне частот 1,5-30 МГц, имеют чувствительность 184 дБВт/Гц, динамический диапазон не менее 80 дБ, скорость поиска по частоте 3-50 ГГц/с, разрешение по частоте от 100 Гц до 5 кГц. Они способны вести разведку сигналов с ППРЧ, сигналов со сжатием, со всеми видами модуляции и кодирования [91]. Однако вскрытие содержания передаваемых сообщений, за предполагаемое время оперативной ценности передаваемой информации, является практически нерешаемой задачей из-за повсеместного использования средств криптографической защиты.

Дальность электромагнитной доступности ИРИ из состава систем связи для средств РРТР определяется типом ИРИ и используемым ими диапазоном [91]:

- для средств КВ радиосвязи – 3000 км;
- для средств УКВ радиосвязи – 200 км (при наличии прямой видимости);
- для средств радиотехнического обеспечения – 100 км для наземных целей, до 300 км для воздушных целей.

3.3.1. Средства космического базирования

Рассматривая космические аппараты (КА) РТР Ferret-D, SSU и SSU-2 как прототипы космических средств РТР можно сформировать обобщенные ТТХ такого типового средства [10]:

- диапазон ведения РТР: от 30 МГц до 80 ГГц;
- вскрываемые параметры РЭС: местоположение, тип, режимы работы;
- точность определения местоположения РЭС: 1-10 км;
- ширина полосы сканирования: 5500-8000 км;
- высота развертывания орбитальной группировки КА: 800-1200 км
- периодичность безпропускного обзора поверхности Земли: 1,5-5,5 ч.

Рассматривая КА РР Vortex, Mercury, Magnum, Orion, Mentor как прототипы космических средств РР можно сформировать обобщенные ТТХ такого типового средства [10]:

- диапазон ведения РР: от 45 МГц до 40 ГГц;
- функциональность: вскрытие местоположения, типа, режимов работы связных РЭС; перехват информации наземных средств, а также переговоров по УКВ-линиям радиосвязи; перехват сообщений в УВЧ каналах правительственной и военной радиосвязи;
- периодичность безпропускного обзора поверхности Земли: непрерывно.

3.3.2. Средства воздушного базирования

Как показано в работе [10], средства РРТР воздушного базирования являются основными средствами добывания информации об СС СН в военных конфликтах. При этом могут использоваться как специализированные самолеты РРТР (RC-135W Rivet Joint, EC-130H CompassCall), так и относительно универсальные БПЛА (типа RQ-4 Global Hawk), оборудованные аппаратурой РРТР.

Как правило, для решения задач РРТР в ходе военных операций средства воздушного базирования декомпозируются на два компонента.

1) Основной компонент, образованный специализированными комплексами РРТР (например, RC-135W Rivet Joint), действующими в пределах воздушного пространства противника либо за его пределами и решающими базовые задачи по ведению РРТР.
2) Вспомогательный компонент, включающий в себя средства РРТР на БПЛА, действующие в пределах воздушного пространства противника, недоступного для средств РРТР основного компонента (например, в пределах зон гарантированного поражения), которые решают задачи РРТР непосредственно на территории противника.

Рассматривая комплексы RC-135W Rivet Joint, RC-12, RC-7B и EC-130H CompassCall как прототипы первого компонента средств РРТР воздушного базирования, а также с учетом ТТХ таких средства РРТР как ES-5000, AN/ALQ-61, WJ-1740, FASTHAT, LR-5200 можно сформировать обобщенные ТТХ такого типового средства.

ТТХ типового средства основного компонента средств РРТР [9, 10, 91, 121, 122]:

- назначение: ведение РРТР ИРИ наземного, морского и воздушного базирования в СМВ, ДМВ и МВ диапазонах длин волн, а также пеленгование ИРИ в автоматическом и ручном режимах;
- функциональность РР: перехват и пеленгование, запись, дешифрирование и анализ радиопереговоров противника, в том числе переговоров экипажей боевых самолетов между собой и с наземными ПУ на дальности до 900 км;
- функциональность РТР: одновременное обнаружение, распознавание и предварительное определение местоположения ИРИ на дальности до 500 км;
- диапазон ведения РР: от 3 МГц до 18 ГГц;
- диапазон ведения РТР: 0,5-40 ГГц;
- точность пеленгования ИРИ: 0,01° – 2°;
- точность определения координат ИРИ: 100-150 м;
- ширина мгновенной полосы обзора: 0,5 ГГц;
- скорость перестройки: 100 МГц/мкс;
- чувствительность: 190 дБВт/Гц;
- высота ведения разведки: 3-7 км;
- удаление от линии соприкосновения войск: 50-100 км;
- дальность полета: до 11000 км;
- скорость полета: до 970 км/ч;
- высота полета: до 16,5 км;
- масса: 54-146 т;
- экипаж: до 5 человек, оперативная группа – до 25 человек.

Рассматривая БПЛА RQ-4 Global Hawk, RQ-6 Outrider и MQ-1C Grey Eagle [9] как прототипы второго компонента средств РРТР воздушного базирования, можно сформировать обобщенные ТТХ такого типового средства:

- диапазон частот: 1,8-18 ГГц;
- динамический диапазон: 60 дБ;
- точность определения частоты ИРИ: 2 МГц;
- точность пеленга ИРИ: 0,8°;
- скорость полета: до 500 км/ч;
- дальность полета: до 6000 км.

Задачами БПЛА, оснащенных комплексами РРТР, являются следующие [9]:

- проведение первоначальной разведки в оперативной глубине;
- формирование целеуказаний для комплексов РЭП и средств ВТО по результатам РРТР;
- вскрытие местоположения базовых станций сетей Wi-Fi, базовых станций мобильной сотовой и транкинговой связи.

На стратегическом уровне управления основной функцией БПЛА является ведение РРТР, в ходе которой они должны осуществлять перехват сигналов, их анализ и формирование карты радиоэлектронной обстановки. Одновременно

происходит пополнение баз данных/библиотек РЭС, расположенных в районе патрулирования. На оперативном уровне решаются задачи по ведению разведки, в том числе видовой, формированию целеуказаний системам оружия. На тактическом уровне БПЛА с помощью систем и средств РРТР могут собирать и передавать пользователям критически важные данные о радиоэлектронной обстановке и формировать целеуказание на подавление или уничтожение РЭС [9].

В перспективе до 2030 г. ожидается, что воздушные средства РТР будут использовать диапазон частот 0,7-160 ГГц для тактических самолетов и 0,25-160 ГГц для стратегических самолетов. Чувствительность приемной части систем РТР может составить до 190 дБВт/Гц, динамический диапазон – до 90 дБ, точность пеленга – до 0,02-0,05°, число каналов – более 100, число РЭС, параметры которых хранятся в запоминающем устройстве, может составить несколько тысяч. К этому же сроку ожидается, что системы РР будут использовать диапазон частот от 0,03 МГц до 100 ГГц, иметь чувствительность 150-180 дБВт/Гц, избирательность 90-95 дБ, точность пеленга 0,1-0,5 °, точность определения координат на дальности до 300 км – 10-20 м [91].

3.3.3. Средства наземного базирования

Наземными комплексами РРТР комплектуются соответствующие разведывательные части и подразделения в составе дивизий и других соединений, предназначенные для выявления средств КВ и УКВ радиосвязи, а также РЛС в тактическом звене, дивизий первого эшелона, органов взаимодействия частей сухопутных войск с тактической авиацией на дальности до 100 км.

Принимая такие средства РРТР, состоящие на вооружении в ВС США, как JEWCS, Guardrail/Common Sensors, AN/TSQ-152(V) Trackwolf и AN/TSQ-199 Enhanced Trackwolf за прототипы наземных средств РРТР можно сформировать обобщенные ТТХ такого типового средства.

Типовой наземный комплекс РРТР выполняет следующие задачи:

- ведение радио- и радиотехнической разведки;
- обработка разведывательных данных и формирование карты текущей радиоэлектронной обстановки;
- определение параметров и координат ИРИ.

Наземный комплекс РРТР состоит из 2-х подсистем:

1) воздушная подсистема – на основе средств РРТР размещенных на самолетах (например, на RC-7B, RC-12P), вертолетах и на тактических БПЛА;
2) наземная подсистема (на основе территориально-распределенной группировки средств РРТР).

Воздушная подсистема способна обнаруживать, идентифицировать, определять местоположение, а в некоторых случаях – осуществлять радиоэлектронное подавление ИРИ.

ТТХ средств воздушной подсистемы наземного комплекса РРТР [9, 10, 58, 91, 122]:

- вариант боевого применения:
  а) для самолетов и вертолетов армейской авиации – барражирование на высоте 3-7 км на дальности 50-100 км от линии соприкосновения войск;
  б) БПЛА – обеспечивает ведение видовой и радиотехнической разведки в пределах 200 км за линией фронта;
- диапазон частот РР: 0,5-18 ГГц;
- диапазон частот РТР: 0,5-40 ГГц;
- точность пеленгования: 0,5-1^0;
- точность определения местоположения ИРИ: на расстоянии до 150 км – 50-150 м.

Типовые ТТХ средств наземной подсистемы комплекса РРТР [9, 10, 58]:

- вариант боевого применения: несение дежурства в тылу своих войск на удалении в 80-200 км от линии соприкосновения войск;
- функциональность: обнаружение, распознавание типов функционирующих ИРИ, перехват сообщений средств радиосвязи, высокоточное определения местоположения РЛС, радиостанций и постановщиков помех противника;
- диапазон частот, в котором ведется радиоразведка: 20-18000 МГц;
- зона ведения разведки: 150×120 км;
- мгновенная полоса обзора: до 2,5 ГГц;
- разрешающая способность: не хуже 1 кГц;
- скорость поиска в разведываемом диапазоне: порядка 3000 ГГц/с;
- обнаружение и пеленгование ИРИ, излучающих в режиме ППРЧ до 1000 скачков/с;
- чувствительность радиоприемников: не хуже 5 мкВ/м;
- точность пеленгования: 0,5°-1°.

Наземная подсистема обеспечивает вскрытие радиоэлектронной обстановки в звене управления «батальон – полк», при координации совместных действия средств РРТР наземной и воздушной подсистемы.

Дополнительные данные о средствах и комплексах РРТР наземного и воздушного базирования представлены в работах [9, 10, 58, 91, 121, 122].

3.4. Описательная модель систем и средств оптико-электронной разведки

Оптико-электронная разведка (ОЭР) – процесс добывания информации с помощью средств, включающих входную оптическую систему с фотоприемником и электронные схемы обработки электрического сигнала, которые обеспечивают прием и анализ электромагнитных волн видимого и ИК-диапазонов, излученных или отраженных объектами и местностью [117].

Оптико-электронная разведка ориентирована на доразведку объектов, вскрытых по результатам РРТР, уточнение местоположения и классификацию

типа ИРИ как объекта СС СН; вскрытие стационарных и мобильных ПУ, узлов связи; вскрытие местоположения узлов и ретрансляторов связи, мест прокладки кабельных, оптико-волоконных и других линий связи обладающих высокой скрытностью в радиодиапазоне.

3.4.1. Средства космического базирования

Принимая средства КА KeyHole, TacSat-3 и ORS как прототипы космических средств ОЭР можно сформировать их обобщенные ТТХ [10]:

- диапазон ведения разведки: днем – видимый диапазон волн (с получением стереоизображений), ночью – ИК-диапазон;
- разрешающая способность: до 0,15 м в панхроматическом режиме и до 1,5 м в многоспектральном режиме;
- ширина полосы обзора: 1200-3600 км;
- высота развертывания орбитальной группировки КА: 200-500 км;
- периодичность безпропускного обзора поверхности Земли: 1,5-2,5 ч.

3.4.2. Средства воздушного базирования

Необходимо отметить, что подавляющая часть средств ОЭР размещается на БПЛА. Данные БПЛА ведут разведку в режиме «дежурство в воздухе». Рассматривая MQ-9 Reaper и RQ-4 Global Hawk как варианты типового БПЛА можно сформировать ТТХ обобщенного БПЛА – носителя средств ОЭР [10]:

- вариант боевого применения для обнаружения РЭС: дежурство в воздухе до 45 ч на высоте до 18 км;
- скорость полета: до 500 км/ч;
- дальность полета: до 6000 км;
- аппаратура разведки: единый интегрированный радиотехнический, оптико-электронный и радиолокационный комплекс;
- параметры разведки: обеспечивает получение радиолокационного и оптического изображения местности с разрешением до 0,3 м. За сутки может быть получено изображение с площади 138 км^2 на расстоянии 200 км.

Более полные сведения о средствах ОЭР представлены в работе [10].

3.5. Описательная модель средств и способов компьютерной разведки

3.5.1. Средства и способы компьютерной разведки

Компьютерная разведка (КР) – добывание информации из компьютерных систем и сетей, характеристик их программно-аппаратных средств и пользователей [9].

Выделяют три типа источников информации для компьютерной разведки [117]:

- данные, сведения и информация, обрабатываемые, передаваемые и хранимые в компьютерных системах и сетях;

- характеристики программных, аппаратных и программно-аппаратных комплексов;
- данные о пользователях компьютерных систем и сетей, а также об их деятельности и интересах.

По виду реализации средства и способы компьютерной разведки можно классифицировать следующем образом:

- *физические* – реализованные в виде физических или аппаратных средств, которые подключаются к инфокоммуникационной инфраструктуре, ведут анализ физических полей, побочных электромагнитных излучений и наводок (ПЭМИН) в интересах добывания данных, сведений и информации;
- *программные* – реализованные в виде программных средств, которые в виде вирусов, закладок или специализированного программного обеспечения добывают данные, сведения и информацию за счет анализа логики построения и функционирования компьютерных систем, а также информационных потоков, циркулирующих в них.

По принципам построения средств и их функциональному предназначению можно выделить следующие типы компьютерной разведки [117]:

- *семантическая* – обеспечивающая добывание фактографической и индексно-ссылочной информации путем поиска, сбора и анализа структурируемой и неструктурируемой информации из общедоступных информационных ресурсов или конфиденциальных источников компьютерных систем и сетей, а также путем семантической (аналитической) обработки полученных и накопленных массивов сведений и документов;
- *алгоритмическая* – обеспечивающая добывание информации путем использования заранее внедренных изготовителем программных или аппаратных закладок, ошибок и недекларированных возможностей компьютерных систем и сетей;
- *вирусная* – обеспечивающая добывание данных путем внедрения вирусных программ в уже эксплуатируемые программные комплексы и системы для перехвата управления компьютерными системами;
- *разграничительная* – обеспечивающая добывание информации из отдельных (локальных) компьютерных систем, которые могут не входить в состав сети, осуществляемая на основе преодоления средств разграничения доступа путем несанкционированного доступа к информации, физического доступа к компьютерной системе или к носителям информации;
- *сетевая* – обеспечивающая добывание информации из компьютерных сетей путем мониторинга сети, инвентаризации и анализа уязвимостей сетевых ресурсов и объектов пользователей, а также последующего удаленного доступа к информации путем использования выявленных уязвимостей систем и средств сетевой (межсетевой) защиты ресурсов,

а также блокирование доступа к ним, модификация, перехват управления либо маскировка своих действий;

- *потоковая* – обеспечивающая добывание информации путем перехвата, обработки и анализа сетевого трафика, выявления структур компьютерных сетей, а также их технических параметров;
- *аппаратная* – обеспечивающая добывание информации путем обработки сведений, получения аппаратуры, оборудования, технических модулей и их анализа, испытания для выявления их технических характеристик и возможностей, полученных другими видами компьютерной разведки;
- *форматная* – обеспечивающая добывание информации путем агрегированной обработки, фильтрации, декодирования, а также проведения других преобразований форматов (представления, передачи и хранения) добытых данных в сведения, а затем – в информацию для последующего ее наилучшего представления пользователям;
- *пользовательская* – обеспечивающая добывание информации о пользователях, их деятельности и интересах на основе определения их сетевых адресов, местоположения, организационной принадлежности, анализа их сообщений и информационных ресурсов, а также путем обеспечения доступа пользователей к информации, циркулирующей в специально созданной информационной инфраструктуре.

На данном этапе развития компьютерных систем и сетей эти типы компьютерной разведки охватывают все существующие многоуровневые «горизонтальные» и «вертикальные» каналы утечки информации из компьютерных систем и сетей. При этом внутри указанных типов возможно выделение нескольких подтипов разведки, например, по виду добываемой информации на: *фактографическую* («*видовую*») и *параметрическую*.

Общая классификация средств и способов компьютерной разведки представлена на рис. 3.2.

Основным способом реализации разведки является атака средств компьютерной разведки [123, 124].

Атака средств компьютерной разведки – как пассивные действия, направленные на добывание информации и, как правило, связанные с нарушением ее конфиденциальности, так и активные действия, направленные на создание условий, благоприятствующих добыванию информации.

К настоящему времени сложился подход к описанию компьютерных атак, основанный на использовании их классификации с учетом множества признаков. Один из наиболее полных учетов признаков реализован в классификации CAPEC [125], разработанной корпорацией MITRE. Однако классификация CAPEC не выделяет в отдельную категорию атаки средств компьютерной разведки. Учитывая этот недостаток классификации CAPEC, отечественными специалистами в работе [124] была предложена классификация атак средств ком-

пьютерной разведки с включением в классификацию образцов конкретных атак. Эта классификация представлена на рис. 3.3.

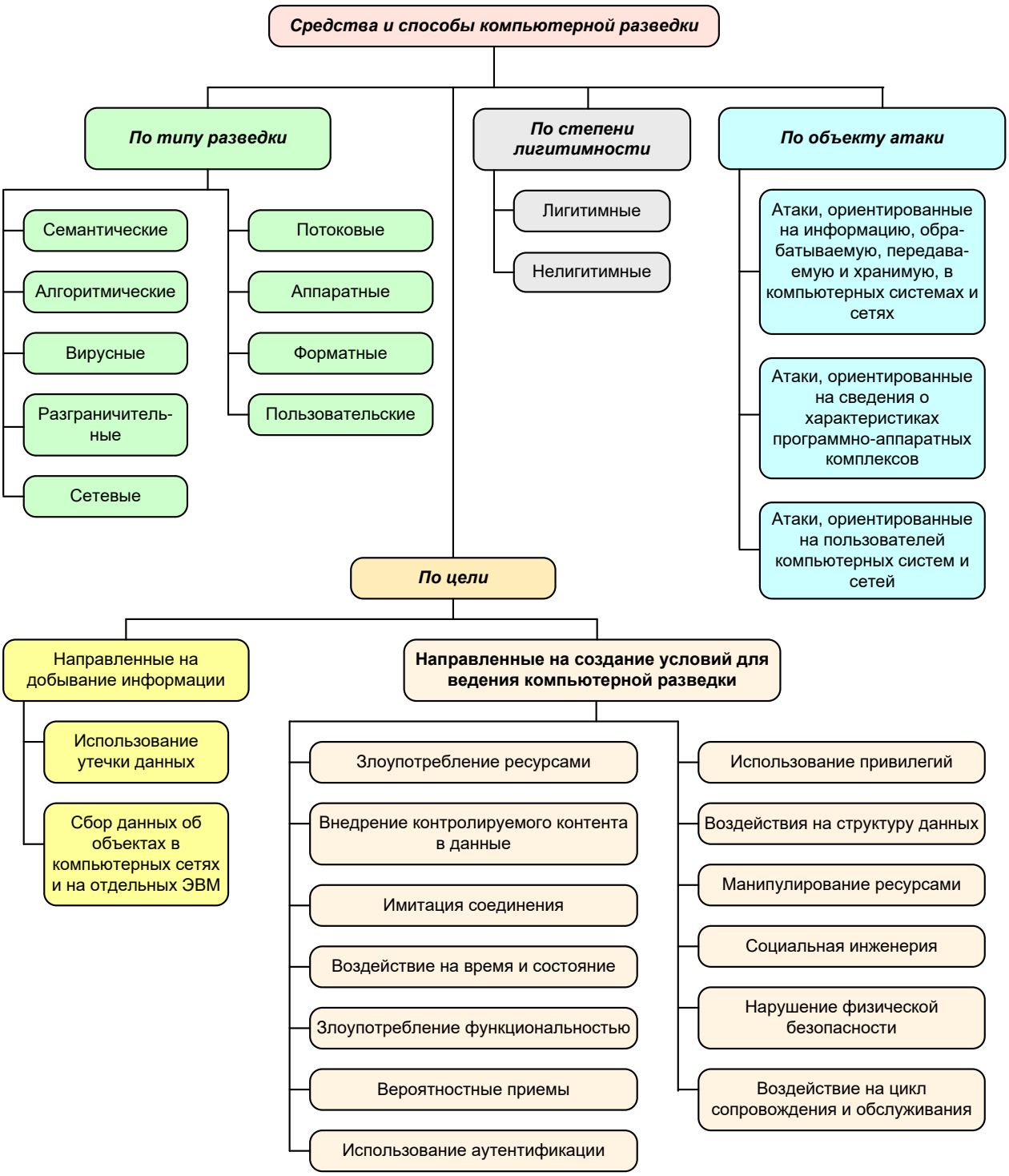

Рис. 3.2. Классификация средств и способов компьютерной разведки [9]

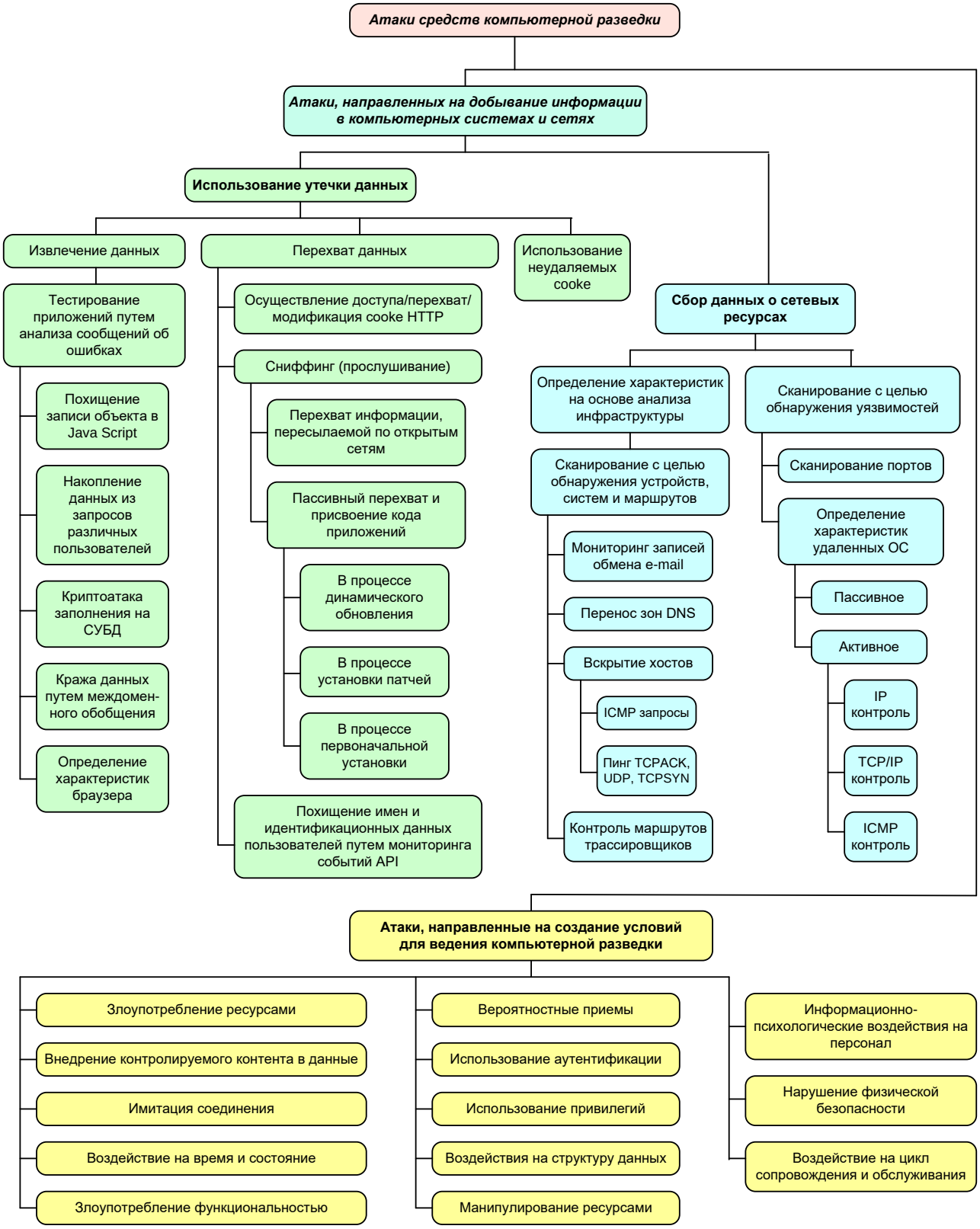

Рис. 3.3. Классификация атак средств компьютерной разведки [124]

3.5.2. Разведка по открытым источникам

При вскрытии параметров СС СН большую роль играет сбор организационной и технической информации об элементах СС СН, а также об эксплуатирующем ее персонале и лицах, принимающих решения. При сборе такой информации широко используются средства разведки по открытым источникам –

в рамках проведения семантической и пользовательской компьютерной разведки. Классификация средств разведки по открытым источникам представлена на рис. 3.4. Более подробные данные об этих средствах представлены в работе [9].

Во многом, повышение значимости разведки по открытым источникам обусловлено тем фактом, что порядка 10-15% необходимой информации имеется в глобальной сети Интернет уже в готовом виде (необходима только ее верификация), а остальные 85-90% информации могут быть получены в результате сравнения, анализа и синтеза разрозненных и представленных в различных источниках фактов. Естественно, что информация, полученная таким образом, нуждается в верификации.

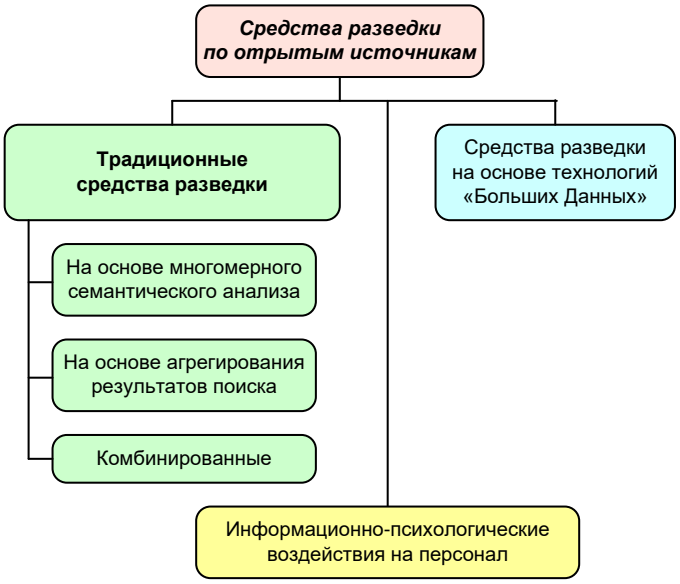

Рис. 3.4. Классификация средств разведки
по отрытым источникам

Для решения задач анализа открытых источников используются аппаратно-программные средства, основу которых составляют алгоритмы поиска и семантического анализа. Специальные программы опрашивают сайты и извлекают из них нужную информацию, используя широкий спектр средств лингвистического, семантического и статистического анализа. Действуя автономно, такие программы анализа данных выявляют любую целевую информацию, как только она появится в сети Интернет.

Особенностью программ анализа данных на основе семантических поисковых алгоритмов является то, что они могут находить только ту информацию, которая в явном виде находится в документах, размещенных в сети Интернет, а уже потом, за счет анализа различных документов с совпадающим целевым контентом, начинают «собирать» информационное наполнение запроса пользователей. Более интересным направлением развития таких средств разведки является анализ разнородных, изначально семантически не связанных между собой данных с целью выявления неслучайных совпадений или скрытых закономерностей и последующей их «привязкой» к объектам разведки. Такое направ-

ление получило развитие в рамках исследования проблемы «больших данных» (Big Date).

Формирование глобального электронного, постоянно пополняющегося архива поведенческой активности самых различных субъектов, от отдельных государств и коммерческих компаний до небольших групп и отдельных индивидуумов в сети Интернет послужило основой появления Больших данных.

Технологии Больших данных основаны, прежде всего, на методах статистического и интеллектуального анализа данных, применяемых на огромных, постоянно пополняемых массивах данных.

Технологии Больших данных позволяют [126]:

- проводить различные и подробные классификации той или иной совокупности людей, компаний, иных объектов по самым разнообразным признакам. Такие классификации обеспечивают понимание взаимосвязи тех или иных характеристик объекта, с теми или иными его действиями;
- осуществлять многомерный статистический корреляционный анализ, выявляющий закономерности и связи различных факторов;
- прогнозировать и управлять, путем использования выявленной корреляционной связи факторов для определения наиболее целесообразного способа воздействия для того, чтобы один набор факторов, характеризующих тот или иной объект, лицо, компанию, событие и т.п., был преобразован в другой.

Более подробная информация об использовании технологий Больших данных при решении задач разведки представлена в работах [9, 126].

Выводы по третьей главе

Средства технической разведки – это основной фактор, влияющий на разведзащищенность структуры, режимов работы, местоположения объектов СС СН, а также сведений об ее обслуживающем персонале и пользователях. При этом для СС СН, из всего многообразия средств технической разведки основную угрозу представляют следующие типы разведки:

1) радио- и радиотехническая разведка, ориентированная на вскрытие параметров и местоположения ИРИ, которые соответствуют абонентам или элементам СС СН; места, времени и содержания ведения радиообмена, с последующим формированием целеуказаний для средств поражения ВТО и средств РЭБ;
2) компьютерная разведка, ориентированная на вскрытие структуры организации связи; используемых протоколов, программного и аппаратного обеспечения; уязвимостей в подсистеме обеспечения ИБ; получения доступа к оперативно ценной информации, циркулирующей в системах государственного и военного управления, с последующим формированием целеуказаний для атакующих ИТВ;
3) оптико-электронная разведка, ориентированная на уточнение местоположения и классификацию типа ИРИ как объекта СС СН; вскрытие стационарных и мобильных ПУ, узлов связи; вскрытие местоположе-

ния узлов и ретрансляторов связи, мест прокладки кабельных, оптиковолоконных и других линий связи обладающих высокой скрытностью в радиодиапазоне.

Отметим, что в последнее время стремительно увеличивается значимость ведения компьютерной разведки, позволяющей на основе технологии обработки «Больших данных» добывать оперативно-ценную информацию из открытых источников (документов, социальных сетей, новостных порталов в сети Интернет) не только о протоколах и структуре сетей связи, но и о месте дислокации объектов СС СН, и даже о морально-психологическом состоянии личного состава войск связи. Также стоит отметить важность средств космической разведки, которая зачастую недооценивается на тактическом и оперативном уровне по сравнению с наземными и воздушными средствами, развертываемыми в районе ТВД. Современные космические средства РРТР и ОЭР позволяют в масштабе времени 1,5-2 ч осуществлять глобальный мониторинг источников ИРИ на поверхности Земли, вскрывать режимы работы средств связи, уточнять местоположение и принадлежность ПУ и узлов связи. Кроме того, в технологически развитых странах проводятся работы по созданию единых комплексов сбора и обработки разведывательной информации (например, таких как DCGS в ВС США), что позволяет комплексировать информацию от различных источников и формировать более полную и достоверную информацию о состоянии СС СН, местоположении ее объектов и режимах работы.

В данной главе представлены описательные модели средств разведки, источниками которых являются СС СН, с учетом их перспективного развития в период до 2030 г., которые могут быть использованы при формировании исходных данных при оценке разведзащищенности и скрытности СС СН в соответствующих моделях, а также при разработке методов, методик и способов повышения соответствующих показателей СС СН.

4. Концептуальная модель системы связи в условиях дестабилизирующих воздействий и ведения разведки

4.1. Общие подходы к представлению системы связи в условиях дестабилизирующих воздействий и ведения разведки в виде информационного конфликта

Становление и развитие методологии исследования эффективности систем связи в условиях дестабилизирующих воздействий и ведения разведки неразрывно связано с совершенствованием научно-методического аппарата (НМА) формализации процессов влияния средств физического и радиоэлектронного поражения, а также средств технической разведки на СС СН.

В теоретической сфере процессы взаимодействия СС СН со средствами дестабилизирующих воздействий и разведки формализуются в виде информационного конфликта.

Информационный конфликт – процесс столкновения сторон на этапах сбора, формирования, передачи, хранения, обработки, представления и интерпретации информации о состоянии, намерениях и действиях своей и противостоящей стороны, при этом каждая из сторон стремится к упреждающим действиям по отношению к противостоящей стороне и предпринимает определенные действия по снижению возможностей противостоящей стороны, а также к обеспечению независимости и эффективности своих систем от вмешательства и воздействий другой стороны.

Информационный конфликт является характерной формой проявления противоборства информационных систем противостоящих сторон на разных иерархических уровнях, а также на различных этапах сбора, формирования, передачи, хранения, обработки, представления и интерпретации информации. Информационный конфликт в общем случае декомпозируется на упорядоченную во времени совокупность отдельных локальных конфликтных противоборств, каждое из которых представляет собой конфликт строго определенного состава сторон, иерархического уровня при фиксированных и неизменных направлении и содержании действий противоборствующих сторон в рамках решения ими собственных целевых задач.

Отображение информационного конфликта на процессы передачи информации позволяет говорить об информационном конфликте применительно к СС СН. Анализ различных научно-методических подходов, к формализации и исследованию информационных конфликтов, применительно к различным конфликтующим объектам (системам связи, разведки, РЭБ, информационного противоборства и т.д.), достаточно полно представлен в работе [192].

Отметим, что на данном этапе развития НМА, в основу работ по моделированию и исследованию информационного конфликта СС СН, как правило, положен один из четырех теоретических базисов:

- теория марковских процессов;
- теория игр;
- теория стохастических сетей;
- теория сетей Петри.

На рис. 4.1 приведен вариант классификации информационных конфликтов. При этом далее будут рассматриваться информационные конфликты только антагонистического типа.

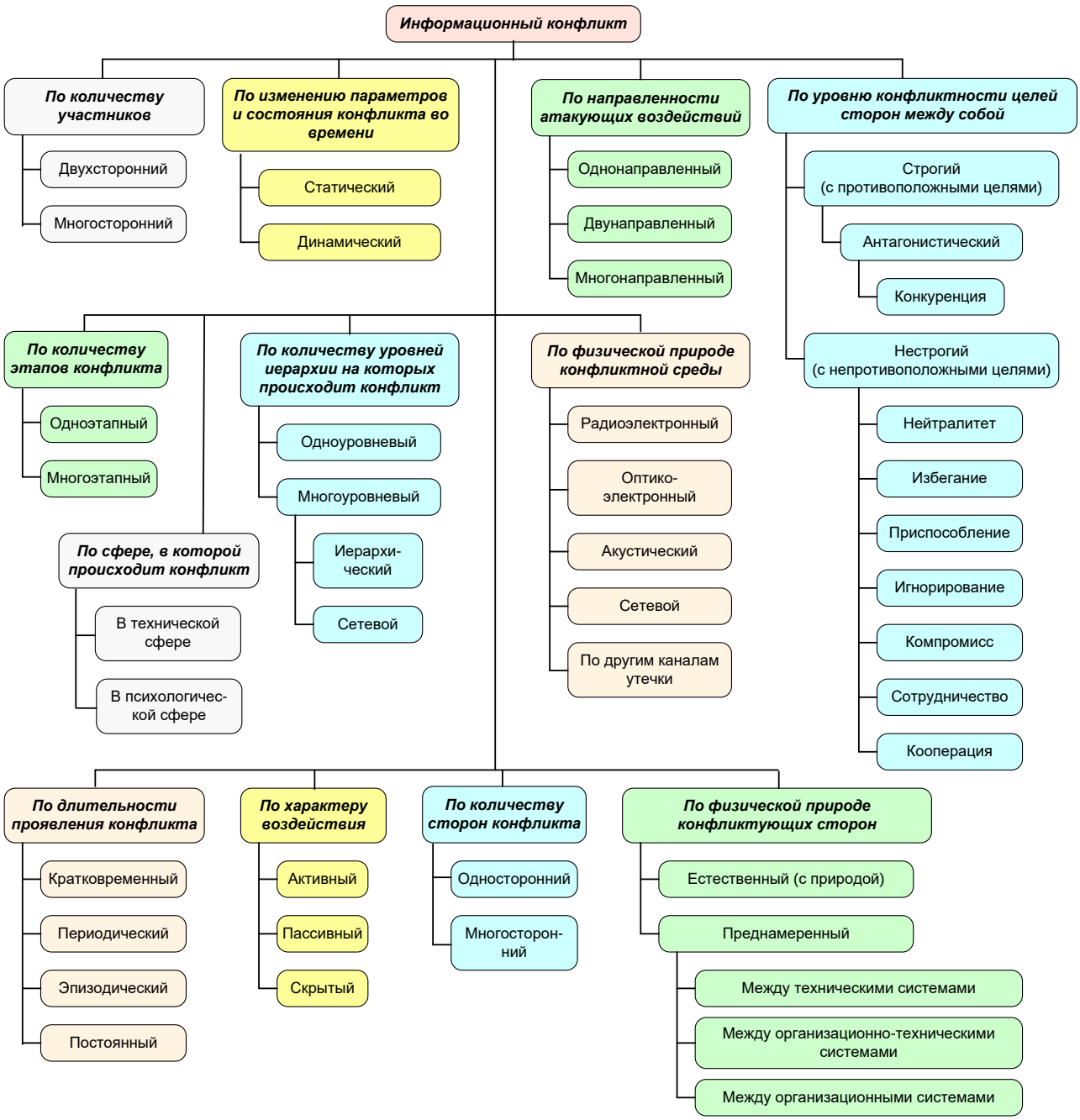

Рис. 4.1. Классификация информационных конфликтов

К исследованиям, в которых представлены наиболее общие концептуальные модели и в самом общем виде формализованы информационные конфликты СС СН со средствами разведки и дестабилизирующих воздействий, необходимо отнести работы [1-6, 94, 193-195, 203]. Представленная далее концептуальная модель сформирована на основе теоретического подхода, представленного в работе В.И. Владимирова, И.В. Владимирова [5].

4.2. Описание условий информационного конфликта

Рассмотрим СС СН как организационно-техническую систему (ОТС), представляющую собой объединение технических средств, обслуживающего персонала и лиц, принимающих решения, для достижения цели передачи информации. Особенностью функционирования СС СН как ОТС является то, что такая ОТС является эргодической системой с управлением, и основная цель ее функционирования достигается путем согласованной и упорядоченной совокупности управляющих воздействий на управляемые объекты СС СН (узлы и каналы связи, режимы работы средств связи и т.д.) со стороны системы управления связью. Управление в таких системах, в широком смысле, представляет собой процесс преобразования информации о состоянии и поведении элементов (объектов) самой ОТС (S_1), окружающей среды, поведение и действия элементов других ОТС (S_2), которые являются противниками в использовании ограниченных ресурсов.

Целью управления СС СН является формирование и реализация управляющих воздействий (командных, распорядительных, информационных) на управляемые объекты в интересах достижения цели функционирования. Управление как процесс преобразования постоянной и оперативной информации реализуется в ОТС с применением соответствующих технологий по выработке и принятию решений: программно-аппаратных комплексов обработки информации; систем поддержки принятия решений; способов формирования управляющих воздействий и доведения их до управляемых объектов.

О степени эффективности функционирования ОТС в условиях ограниченности материального, энергетического, частотного и других видов ресурсов судят по достигнутым результатам, в соответствии с целевым назначением ОТС, учитывая конфликтное взаимодействие этой ОТС (S_1), как с окружающей средой, создающей угрозы естественного происхождения, так и с другой ОТС (S_2), которая содержит подсистему разведки и подсистему преднамеренных дестабилизирующих воздействий. Эта ОТС (S_2) является потенциальным противником и может создавать преднамеренные угрозы различного характера, воздействующие на различные элементы и подсистемы СС СН (S_1) как объекта защиты.

Угроза – совокупность условий, факторов и воздействий на систему, создающих потенциальную или реальную опасность нарушения ее работоспособности, ухудшения характеристик, снижения качества или эффективности ее функционирования. Количественной характеристикой опасности угрозы является потенциальный ущерб (материальный, экономический, информационный, моральный и т.д.).

Среди всех типов информационных конфликтов, как процесса взаимодействия ОТС S_1 и S_2, особый интерес представляют следующие:

1) антагонистический информационный конфликт с обратно пропорциональным изменением показателей эффективности, когда цели функционирования взаимодействующих ОТС S_1 и S_2 прямо противоположны, а увеличение (уменьшение) эффективности одной приводит к пропорциональному уменьшению (увеличению) другой;
2) антагонистический информационный конфликт с не пропорциональным изменением показателей функционирования конфликтующих ОТС, когда они изменяются в среднем строго противоположно, но не пропорционально;
3) нестрогий информационный конфликт, когда цели функционирования ОТС нестрого противоположны, а изменение показателя эффективности одной из ОТС в среднем приводит к противоположному изменению показателя эффективности другой.

Далее конфликтные взаимодействия типа нестрогий конфликт (с не противоположными интересами) не рассматриваются, так как противоречия в конфликте данного типа могут быть устранены на основе реализации принципа согласованного оптимума [196] и перевода этого типа конфликтного взаимодействия в конфликты типа «коалиция» или «кооперация» [197, 198].

Антагонистические конфликты 1-го и 2-го типа являются составными частями открытого и/или скрытого целенаправленного информационного противоборства ОТС S_1 и S_2 друг против друга в информационном пространстве с целью получения определенного информационного превосходства [199-201]. Под информационным пространством, как средой информационного противоборства здесь понимается совокупность носителей информации различной физической природы, которые перемещаются в соответствующих средах распространения (каналах передачи информации, линиях связи) и технических устройствах, предназначенных для формирования, сбора, хранения и преобразования информации, обладающей семантическими и прагматическими свойствами для органов управления конфликтующих ОТС. При этом техническую основу для добывания информации об окружающей среде и действиях противоборствующей ОТС составляют средства технической разведки. Техническую основу передачи (приема) информации составляют линии и узлы связи, объединенные в сети связи, и обслуживающие соответствующие системы военного и государственного управления [2].

Приведенные выше исходные положения определяют основное существо концептуальной модели СС СН в условиях информационного конфликта, которая содержит качественное описание факторов конфликтного взаимодействия объекта защиты S_1, с субъектом нападения (S_2). Целью субъекта нападения S_2 в информационном конфликте на системном уровне является изменение поведения или состояния элементов S_1 таким образом, при котором защищающаяся ОТС S_1 либо не выполняет задачу по предназначению, либо функционирует в режимах, навязанных нападающей ОТС S_2.

Крайне важным для начала информационного конфликта является возможность доступа субъекта нападения S_2 к каналам наблюдения (каналам утечки) за объектом защиты S_1, которые формируются путем пересечения информационных сред конфликтующих сторон, в первую очередь, в электромагнитном диапазоне (для средств РРТР) и в компьютерно-сетевой среде (для средств компьютерной разведки). При этом информационное пространство как в отношении ОТС, являющейся субъектом нападения, так и в отношении ОТС, являющейся объектом защиты, характеризуется: информационной емкостью, скоростью передачи информации, пропускной способностью линий связи, электромагнитным и сетевым ресурсом, выделенных для обеспечения функционирования ОТС по их назначению.

Информационный конфликт в составе рассматриваемой концептуальной модели фактически соответствует процессу антагонистического информационного противоборства.

Информационное противоборство – конфликт в информационном пространстве с целью завоевания и удержания информационного превосходства над противоположной стороной, который предполагает проведение взаимоувязанных по целям, месту и времени информационных операций, основанных как на дестабилизирующих воздействиях на информацию, информационные системы и информационную инфраструктуру противоположной стороны, так и на одновременной защите собственной информации, информационных систем и информационной инфраструктуры от подобных воздействий.

Информационное противоборство является формой крайнего проявления конфликта ОТС в информационном пространстве. Информационное противоборство применительно к СС СН включает два типа мероприятий:

1) мероприятия по обеспечению информационной безопасности ОТС, направленные на обеспечение устойчивости СС СН в информационном конфликте;
2) мероприятия по воздействию на СС СН и вышестоящую систему управления в целях разрушения (искажения, задержки) оперативной информации, определяющей качество принимаемых решений органами управления.

Необходимо отметить, что особой составной частью информационного противоборства является ведение РЭБ. Средства и способы РЭБ как интегрировано, так и самостоятельно решают задачи не только по защите информационного пространства объекта защиты (S_1), но и/или по нарушению (искажению) информационного пространства объекта нападения (S_2). В области информационного противоборства средства РЭБ следует рассматривать не только в контексте нападения, как средства радиоэлектронного поражения, но и как средства радиоэлектронной защиты (рис. 2.3), в том числе и путем радиоэлектронных контратак. Разрушение (искажение) информационного пространства объекта нападения (S_2) способами и средствами РЭБ является одним из самых эффективных и быстро приносящих результаты воздействий. Дезорганизация системы управления связью, например, за счет информационной блокады линий связи приводит к нарушению процедур формирования управляющих воздей-

ствий, и, следовательно, к неэффективному функционированию СС СН в целом. При этом способы и средства РЭБ, применяемые в целях радиоэлектронной защиты органов управления, направлены на сохранение работоспособности собственных систем связи, а также циркулирующей и хранящейся в них информации.

4.3. Постановка задачи на моделирование

Целью формирования концептуальной модели СС СН в условиях информационного конфликта является представление структурных схем конфликтующих ОТС на первом уровне их декомпозиции (управляющая система, управляемые объекты): путей реализации стратегий разведки, нападения и защиты; направлений реализации угроз для каждой из сторон. При этом под концептуальной моделью информационного конфликта понимается описание процесса установления конфликтно-устойчивого или конфликтно-неустойчивого состояния процесса «объект защиты – субъект нападения» в интересах формализации и последующей оценки математическими методами каждого из этих состояний (исхода информационного конфликта) с учетом реализуемых стратегий разведки, нападения и защиты, а также ресурсных возможностей каждой из сторон.

Для формализации концептуальной модели введем следующие обозначения:

d – оперативная информация;

d_1 – оперативная информация о состоянии объекта защиты S_1, получаемая системами мониторинга ОТС S_1;

d_2 – оперативная информация о состоянии объекта защиты S_1, получаемая системами разведки ОТС S_2;

$e_{ад}$ – единица показателя адекватности управления в ОТС;

$e_{непр}$ – единица показателя непрерывности управления в ОТС;

$e_{оп}$ – единица показателя оперативности управления в ОТС;

$e_{скр}$ – единица показателя скрытности управления в ОТС;

$e_{ус}$ – единица показателя устойчивости управления в ОТС;

F_1 – функция выигрыша ОТС S_1;

F_2 – функция выигрыша ОТС S_2;

I – множество стратегий нападения;

i – стратегия нападения ОТС S_2 на ОТС S_1, включающая в себя стратегии ведения разведки $i_р$ и использования средств нападения $i_н$;

$i_н$ – стратегия использования средств нападения ОТС S_2;

$i_{н\ ИТВ}$ – стратегия нападения ОТС S_2 средствами и способами ИТВ;

$i_{н\ ИТВ}^{защ}$ – стратегия защиты средств ИТВ в составе ОТС S_2 от контратакующих воздействий со стороны ОТС S_1;

$i_{н\ РЭП}$ – стратегия нападения ОТС S_2 средствами РЭП;

$i_{н\ РЭП}^{защ}$ – стратегия защиты средств РЭП в составе ОТС S_2 от контратакующих воздействий со стороны ОТС S_1;

$i_{н\ ФП}$ – стратегия нападения ОТС S_2 средствами физического (огневого) поражения;

$i_{н\ ФП\ ЭМИ}$ – стратегия нападения ОТС S_2 средствами ФП ЭМИ;

$i_{н\ ФП\ ЭМИ}^{защ}$ – стратегия защиты средств ФП ЭМИ в составе ОТС S_2 от контратакующих воздействий со стороны ОТС S_1;

$i_{н\ ФП}^{защ}$ – стратегия защиты средств физического (огневого) поражения ОТС S_2 от контратакующих воздействий со стороны ОТС S_1;

$i_{н}^{защ}$ – стратегия защиты средств нападения ОТС S_2 от контратакующих воздействий со стороны ОТС S_1;

$i_{р}$ – стратегия ведения разведки со стороны ОТС S_2;

$i_{р\ КР}$ – стратегия ведения компьютерной разведки со стороны ОТС S_2;

$i_{р\ КР}^{защ}$ – стратегия защиты средств компьютерной разведки ОТС S_2 от от контратакующих воздействий со стороны ОТС S_1;

$i_{р\ ОЭР}$ – стратегия ведения ОЭР со стороны ОТС S_2;

$i_{р\ ОЭР}^{защ}$ – стратегия защиты средств ОЭР в составе ОТС S_2 от контратакующих воздействий со стороны ОТС S_1;

$i_{р\ РРТР}$ – стратегия ведения РРТР со стороны ОТС S_2;

$i_{р\ РРТР}^{защ}$ – стратегия защиты средств РРТР в составе ОТС S_2 от контратакующих воздействий противоборствующей стороны;

$i_{р}^{защ}$ – стратегия защиты средств разведки от контратакующих воздействий со стороны ОТС S_1;

J – множества стратегий защиты;

j – стратегия защиты ОТС S_1;

$j_{сс}$ – стратегия защиты элементов СС СН в составе ОТС S_1;

$j_{ИТВ}$ – стратегия контратак средствами ИТВ в составе ОТС S_1 на нападающую ОТС S_2;

$j_{ИТВ}^{защ}$ – стратегия защиты СС СН в составе ОТС S_1 от средств ИТВ нападающей ОТС S_2;

$j_{КР}$ – стратегия контратак средствами компьютерной разведки ОТС S_1 на нападающую ОТС S_2;

$j_{КР}^{защ}$ – стратегия защиты СС СН в составе ОТС S_1 от средств компьютерной разведки нападающей ОТС S_2;

$j_{лс}$ – стратегия управления конфигурацией и режимами работы линий связи СС СН;

$j_{н}$ – стратегия контратак ОТС S_1 на средства нападения ОТС S_2;

$j_{н}^{защ}$ – стратегия защиты СС СН в составе ОТС S_1 от средств нападения ОТС S_2;

$j_{ОЭР}$ – стратегия контратак ОТС S_1 на средства ОЭР нападающей ОТС S_2;

$j_{ОЭР}^{защ}$ – стратегия защиты СС СН в составе ОТС S_1 от средств ОЭР нападающей ОТС S_2;

$j_{р}$ – стратегия контратак ОТС S_1 на средства разведки ОТС S_2;

$j_{р}^{защ}$ – стратегия защиты СС СН в составе ОТС S_1 от средств ведения разведки ОТС S_2;

$j_{РРТР}$ – стратегия контратак средств РРТР нападающей стороны;

$j_{РРТР}^{защ}$ – стратегия защиты СС СН в составе ОТС S_1 от средств РРТР нападающей ОТС S_2;

$j_{РЭП}$ – стратегия контратак ОТС S_1 на средства РЭП нападающей ОТС S_2;

$j_{РЭП}^{защ}$ – стратегия защиты СС СН от средств РЭП нападающей ОТС S_2;

$j_{ус}$ – стратегия управления конфигурацией и режимами работы узлов связи СС СН в составе ОТС S_1;

$j_{ФП}$ – стратегия контратак ОТС S_1 на средства физического (огневого) поражения нападающей ОТС S_2;

$j_{ФП\ ЭМИ}$ – стратегия контратак ОТС S_1 на средства ФП ЭМИ нападающей ОТС S_2;

$j_{ФП\ ЭМИ}^{защ}$ – стратегия защиты СС СН в составе ОТС S_1 от средств ФП ЭМИ нападающей ОТС S_2;

$j_{ФП}^{защ}$ – стратегия защиты СС СН в составе ОТС S_1 от средств физического (огневого) поражения нападающей ОТС S_2;

k – счетчик этапов информационного конфликта;

N – количество этапов информационного конфликта;

$P_{акт}$ – вероятность обеспечения актуальности информации;

$P_{без}$ – вероятность обеспечения в СС СН требуемого уровня безопасности связи;

$P_{дост}$ – вероятность достоверности информации;

$P_{дост}^{треб}$ – требуемый уровень достоверности информации;

$P_{полн}$ – вероятность полноты информации;

$P_{св}$ – вероятность обеспечения в СС СН требуемого уровня своевременности связи;

Q – совокупность показателей, которые характеризуют качество формирования ($Q_{форм}$), передачи ($Q_{прд}$), хранения ($Q_{хр}$), обработки ($Q_{обр}$) и представления ($Q_{пр}$) информации в ОТС;

$Q_{обр}$ – показатель, который характеризует качество обработки информации в ОТС;

$Q_{пр}$ – показатель, который характеризует качество представления (визуализации) информации в ОТС для лиц, принимающих решения;

$Q_{прд}$ – показатель, который характеризует качество передачи информации в ОТС;

$Q_{форм}$ – показатель, который характеризует качество формирования информации в ОТС;

$Q_{хр}$ – показатель, который характеризует качество хранения информации в ОТС;

$R_{сс}$ – ресурс СС СН;

$R_{ИТВ}$ – ресурс средств ИТВ;

$R_{КР}$ – ресурс средств компьютерной разведки;

$R_{лс}$ – ресурс совокупности линий связи в составе СС СН;

$R_{н}$ – ресурс средств нападения;

$R_{ОЭР}$ – ресурс средств ОЭР;

$R_{р}$ – ресурс средств разведки;

$R_{РРТР}$ – ресурс средств РРТР;

$R_{РЭП}$ – ресурс средств РЭП;

$R_{ус}$ – ресурс совокупности узлов связи в составе СС СН;

$R_{ФП}$ – ресурс средств физического (огневого) поражения;

$R_{ФПЭМИ}$ – ресурс средств ФП ЭМИ;

S_1 – ОТС, соответствующая объекту защиты, в состав которой входит СС СН;

S_2 – ОТС, соответствующая субъекту нападения, содержащая в своем составе подсистему разведки и подсистему нападения;

t_k – момент времени окончания k-го этапа информационного конфликта;

$T_{изм}$ – среднее время изменения реальной обстановки, появления новых или изменения существующих объектов или явлений в процессе функционирования ОТС;

$T_{ик}$ – длительность информационного конфликта;

$T_{обн}$ – среднее или фиксированное время обновления информации в системе управления;

$T_{обр}$ – среднее время обработки информации в управляющей системе.

$T_{пр}$ – среднее время представления информации органу или лицу, принимающему решение;

$T_{прд}$ – время передачи информации;

$T_{прд}$ – среднее время передачи информации по СС СН;

$T_{прд}^{треб}$ – требуемое время передачи информации, в течение которого информация сохраняет свою актуальность (оперативную ценность);

$T_{форм}$ – среднее время формирования информации о новых событиях и явлениях реальной обстановки;

$T_{хр}$ – среднее время хранения информации;

U – вектор качества управления в ОТС S_1;

$U_{ад}$ – адекватность управления;

$U_{непр}$ – непрерывность управления;

$U_{оп}$ – оперативность управления;

$U_{скр}$ – скрытность управления;

$U_{ус}$ – устойчивость управления;

V – объем информации;

$V_к$ – объем командной (распорядительной) информации;

$V_{пос}$ – объем постоянной информации;

$V_{тек}$ – объем текущей информации;

x – абсолютное значение некоторого показателя ОТС;

$x_{ид}$ – некоторое идеальное значение показателя x в условиях отсутствия дестабилизирующих воздействий на элементы ОТС;

$x^{норм}$ – нормированное значение показателя x;

γ – информационный ущерб;

Δt_k – длительность k-го этапа информационного конфликта;

$\Delta\xi_1$ – изменение уровня выигрыша ОТС S_1 в ходе k-го этапа информационного конфликта;

$\lambda_{изм} = 1/T_{изм}$ – средняя интенсивность (темп) изменения реальной обстановки, появления новых или изменения существующих объектов или явлений в процессе функционирования ОТС;

ξ_1 – показатель выигрыша ОТС S_1;

$\xi_{1\,ож}$ – некоторый усредненный удельный (в единицу времени) ожидаемый выигрыш ОТС S_1 от применения управляемых средств связи, в отсутствии дестабилизирующих воздействий на элементы СС СН;

ξ_1^0 – выигрыш ОТС S_1, в отсутствие дестабилизирующих воздействий нападающей ОТС;

$\xi_1^{инт}$ – средний интегральный выигрыш ОТС S_1 за время конфликта $T_{ик}$;

ξ_2 – показатель выигрыша ОТС S_2;

$\xi_2^{инт}$ – средний интегральный выигрыш ОТС S_2 за время конфликта $T_{ик}$;

$\tau_1^{защ}$ – длительность этапа защиты ОТС S_1 от ОТС S_2;

$\tau_1^{реак}$ – время реакции управляющей системы ОТС S_1;

$\tau_2^{нап}$ – длительность этапа нападения ОТС S_2 на ОТС S_1;

$\tau_2^{реак}$ – время реакции управляющей системы ОТС S_2;

ψ – семантическая (энтропийная) ценность информации.

4.4. Схема концептуальной модели

На рис. 4.2 приведена схема концептуальной модели информационного конфликта ОТС S_1 и S_2.

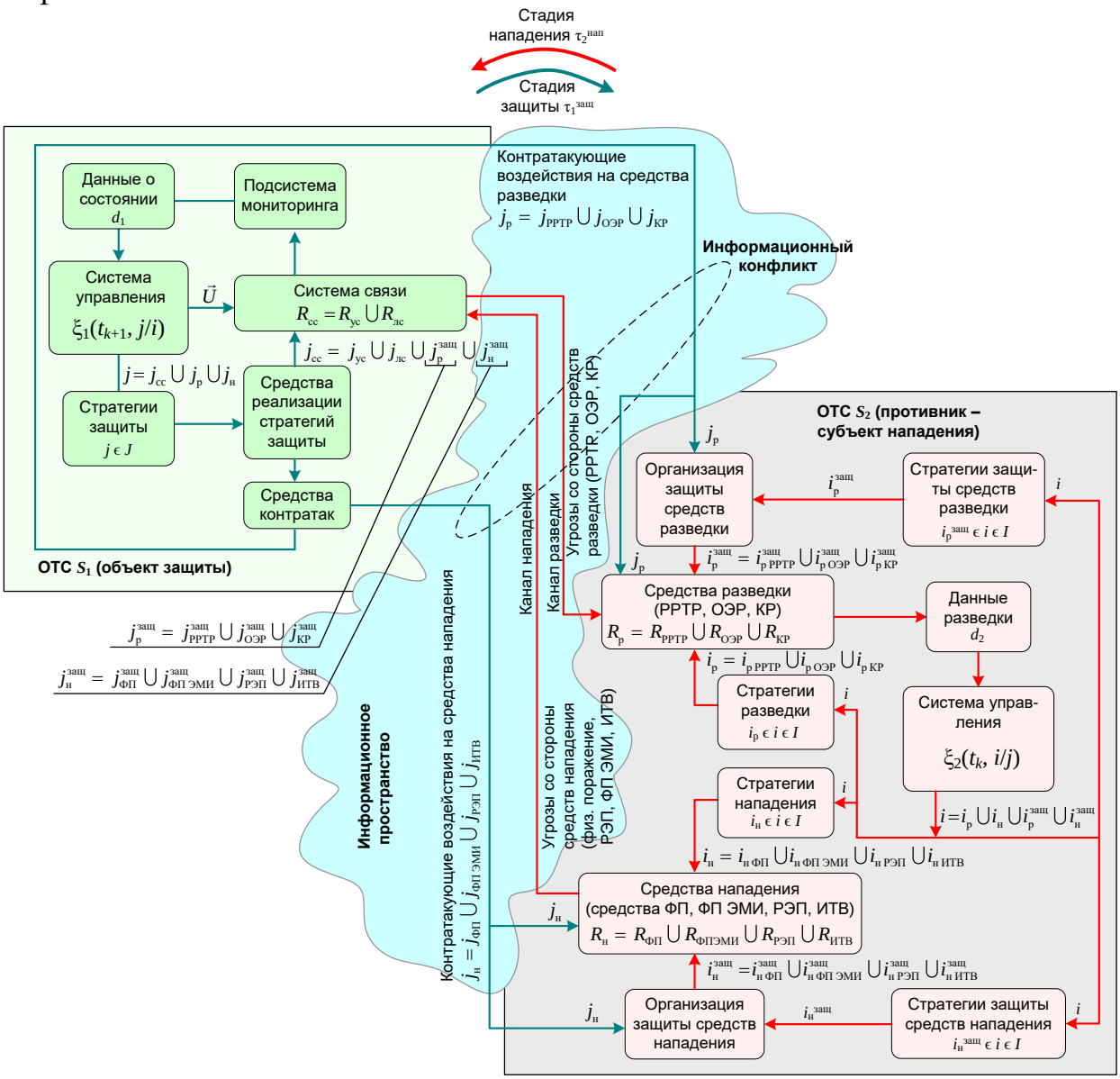

Рис. 4.2. Схема концептуальной модели информационного конфликта ОТС S_1 и S_2

Как показано на рис. 4.2, в каждой из конфликтующих ОТС можно выделить:

- основной контур управления, формирующий целевые стратегии функционирования по предназначению. Для ОТС S_2 – это стратегии нападения $i_н$ и разведки $i_р$, для ОТС S_1 – вектор управления $\vec{U}$ ресурсами ОТС;
- контур защиты, представленный для ОТС S_1 стратегией защиты j и стратегиями контратак средств разведки $j_р$ и средств нападения $j_н$, для ОТС S_2 – стратегиями защиты от контратак средств разведки $i_р^{защ}$ и средств нападения $i_н^{защ}$.

Для решения текущих задач, как в основном управляющем контуре, так и в защитном контуре, каждая ОТС располагает определенными ресурсами. ОТС S_1 располагает ресурсами СС СН $R_{сс}$, состоящими из совокупности ресурсов узлов связи $R_{ус}$ и совокупности ресурсов линий связи $R_{лс}$. ОТС S_2 – ресурсами средств нападения $R_н$ и ресурсами средств разведки $R_р$.

В модели ресурсы $R_н$ и $R_р$ могут быть декомпозированы по типу средств нападения и разведки:

$$R_р = R_{РРТР} \cup R_{ОЭР} \cup R_{КР},$$

$$R_н = R_{ФП} \cup R_{ФПЭМИ} \cup R_{РЭП} \cup R_{ИТВ},$$

где: $R_{РРТР}$ – ресурс средств РРТР; $R_{ОЭР}$ – ресурс средств ОЭР; $R_{КР}$ – ресурс средств компьютерной разведки; $R_{ФП}$ – ресурс средств физического (огневого) поражения; $R_{ФПЭМИ}$ – ресурс средств ФП ЭМИ; $R_{РЭП}$ – ресурс средств РЭП; $R_{ИТВ}$ – ресурс средств ИТВ.

Процесс конфликтного взаимодействия ОТС S_1 и S_2 возможен в том случае, когда данные ОТС совместно функционируют в едином информационном пространстве. Такая область их совместного функционирования в информационном пространстве формируется принципиальной возможностью радиоэлектронного и сетевого взаимодействия элементов каждой из ОТС и является ключевой с точки зрения начала и развития информационного конфликта. При этом информацию о своем состоянии и состоянии противоборствующей стороны, необходимую для выработки стратегий защиты j и нападения i, добывают подсистемы разведки/мониторинга, которые решают задачи [5]:

- наблюдения за состоянием объектов защиты и нападения;
- наблюдения за результатами воздействия и эффективности защиты от них;
- наблюдения за изменением ресурсных возможностей сторон и условий их конфликтного функционирования.

Нарушение информационной сопряженности компонент основного контура управления с информационной средой приводит к потере устойчивости управления, и, как следствие, – к конфликтно-неустойчивому состоянию, например, объекта защиты. Контур управления представляет собой замкнутую последовательность процедур в системе управления, заключающуюся в формировании стратегии действий, доведении стратегии до управляемых объектов с оперативным контролем результатов реализации принятого решения.

В контуре защиты ОТС S_1 реализуются стратегия j защиты СС СН с целью ее эффективного применения в интересах вышестоящей системы управления в динамике информационного конфликта. Стратегия j защиты СС СН, методы защиты информации при ее обработке, хранении, передаче и при воздействии ИТВ рассмотрены, например, в работе [202] и далее подробно в данной модели не обсуждаются.

Стратегия защиты СС СН $j = j_{\text{сс}} \cup j_{\text{р}} \cup j_{\text{н}}$ предполагает не только стратегию реконфигурации параметров СС СН $j_{\text{сс}}$ и применение пассивных стратегий защиты ($j_{\text{р}} = j_{\text{РРТР}} \cup j_{\text{ОЭР}} \cup j_{\text{КР}}$ и $j_{\text{н}} = j_{\text{ФП}} \cup j_{\text{ФП ЭМИ}} \cup j_{\text{РЭП}} \cup j_{\text{ИТВ}}$), но и возможное применение активных стратегий защиты – так называемых контратак ($j_{\text{р}} = j_{\text{РРТР}} \cup j_{\text{ОЭР}} \cup j_{\text{КР}}$ и $j_{\text{н}} = j_{\text{ФП}} \cup j_{\text{ФП ЭМИ}} \cup j_{\text{РЭП}} \cup j_{\text{ИТВ}}$).

Целью стратегии защиты j является сужение области совместно доступного информационного пространства ОТС S_1 и S_2 до таких границ, при которых отсутствует область их взаимного пересечения. Вариантами достижения этого являются:

- проведение в СС СН мероприятий маскировки, повышения разведзащищенности и скрытности связи, формирование ложных элементов СС СН (линий и узлов связи) в интересах отвлечения средств разведки и нападения ОТС S_2 на ложные объекты СС СН;
- стратегии контратак защищающейся ОТС S_1 на средства разведки ($j_{\text{р}}$) и нападения ($j_{\text{н}}$) ОТС S_2;
- получение информации о намерениях, целях и планируемых стратегиях действий нападающей ОТС S_2 путем перехвата принимаемых решений, данных о технико-эксплуатационных характеристиках (параметрах) средств этой ОТС, их местоположении и назначении.

В отношении стратегий защиты j и нападения i необходимо отметить следующее. При реализации j-ой стратегии защиты со стороны ОТС S_1 следует учитывать декомпозицию этой стратегии на непосредственно стратегию защиты элементов СС СН $j_{\text{сс}}$, стратегии контратаки на средства разведки $j_{\text{р}}$ и контратаки на средства разведки $j_{\text{н}}$:

$$j = j_{\text{сс}} \cup j_{\text{р}} \cup j_{\text{н}} .$$

При этом стратегии защиты элементов СС СН $j_{\text{сс}}$, а также стратегии контратак $j_{\text{р}}$ и $j_{\text{н}}$ могут, в свою очередь, быть декомпозированы далее, в зависимости от угрожаемых типов средств разведки и нападения, а также по типу управления конфигурацией средств связи (линиями и узлами связи):

$$j_{\text{сс}} = j_{\text{ус}} \cup j_{\text{лс}} \cup j_{\text{р}}^{\text{защ}} \cup j_{\text{н}}^{\text{защ}},$$

при

$$j_{\text{р}}^{\text{защ}} = j_{\text{РРТР}}^{\text{защ}} \cup j_{\text{ОЭР}}^{\text{защ}} \cup j_{\text{КР}}^{\text{защ}} \text{ и } j_{\text{н}}^{\text{защ}} = j_{\text{ФП}}^{\text{защ}} \cup j_{\text{ФП ЭМИ}}^{\text{защ}} \cup j_{\text{РЭП}}^{\text{защ}} \cup j_{\text{ИТВ}}^{\text{защ}};$$

$$j_{\text{р}} = j_{\text{РРТР}} \cup j_{\text{ОЭР}} \cup j_{\text{КР}};$$

$$j_{\text{н}} = j_{\text{ФП}} \cup j_{\text{ФП ЭМИ}} \cup j_{\text{РЭП}} \cup j_{\text{ИТВ}};$$

где: $j_{\text{ус}}$ – стратегия управления конфигурацией и режимами работы узлов связи; $j_{\text{лс}}$ – стратегия управления конфигурацией и режимами работы линий связи; $j_{\text{р}}^{\text{защ}}$ – стратегия защиты СС СН от средств ведения разведки нападающей сто-

роны; $j_{н}^{защ}$ – стратегия защиты СС СН от средств нападения; $j_{РРТР}^{защ}$ – стратегия защиты СС СН от средств РРТР нападающей стороны; $j_{ОЭР}^{защ}$ – стратегия защиты СС СН от средств ОЭР нападающей стороны; $j_{КР}^{защ}$ – стратегия защиты СС СН от средств компьютерной разведки нападающей стороны; $j_{ФП}^{защ}$ – стратегия защиты СС СН от средств физического (огневого) поражения нападающей стороны; $j_{ФП\ ЭМИ}^{защ}$ – стратегия защиты СС СН от средств ФП ЭМИ нападающей стороны; $j_{РЭП}^{защ}$ – стратегия защиты СС СН от средств РЭП нападающей стороны; $j_{ИТВ}^{защ}$ – стратегия защиты СС СН от средств ИТВ нападающей стороны; $j_{РРТР}$ – стратегия контратак средств РРТР нападающей стороны; $j_{ОЭР}$ – стратегия контратак средств ОЭР нападающей стороны; $j_{КР}$ – стратегия контратак средств компьютерной разведки нападающей стороны; $j_{ФП}$ – стратегия контратак средств физического (огневого) поражения нападающей стороны; $j_{ФП\ ЭМИ}$ – стратегия контратак средств ФП ЭМИ нападающей стороны; $j_{РЭП}$ – стратегия контратак средств РЭП нападающей стороны; $j_{ИТВ}$ – стратегия контратак средств ИТВ нападающей стороны.

Аналогично, при реализации i-ой стратегии нападения со стороны ОТС S_2 следует учитывать декомпозицию этой стратегии на непосредственно стратегию использования средств нападения $i_{н}$, стратегию ведения разведки $i_{р}$, а также стратегии защиты своих средств разведки $i_{р}^{защ}$ и своих средств нападения $i_{н}^{защ}$ от контратакующих стратегий ОТС S_1:

$$i = i_{р} \cup i_{н} \cup i_{р}^{защ} \cup i_{н}^{защ}.$$

При этом стратегии ведения разведки $i_{р}$ и стратегии нападения, а также стратегии зашиты соответствующих средств $i_{р}^{защ}$ и $i_{н}^{защ}$, могут, в свою очередь, быть декомпозированы далее по типу средств разведки и нападения:

$$i_{р} = i_{р\ РРТР} \cup i_{р\ ОЭР} \cup i_{р\ КР},$$

$$i_{р}^{защ} = i_{р\ РРТР}^{защ} \cup i_{р\ ОЭР}^{защ} \cup i_{р\ КР}^{защ},$$

$$i_{н} = i_{н\ ФП} \cup i_{н\ ФП\ ЭМИ} \cup i_{н\ РЭП} \cup i_{н\ ИТВ},$$

$$i_{н}^{защ} = i_{н\ ФП}^{защ} \cup i_{н\ ФП\ ЭМИ}^{защ} \cup i_{н\ РЭП}^{защ} \cup i_{н\ ИТВ}^{защ},$$

где: $i_{р\ РРТР}$ – стратегия ведения разведки средствами РРТР; $i_{р\ ОЭР}$ – стратегия ведения ОЭР; $i_{р\ КР}$ – стратегия ведения компьютерной разведки; $i_{р\ РРТР}^{защ}$ – стратегия защиты средств РРТР от контратакующих воздействий противоборствующей стороны; $i_{р\ ОЭР}^{защ}$ – стратегия защиты средств ОЭР от контратакующих воздействий противоборствующей стороны; $i_{р\ КР}^{защ}$ – стратегия защиты средств компьютерной разведки от контратакующих воздействий противоборствующей стороны; $i_{н\ ФП}$ – стратегия нападения средствами физического (огневого) поражения; $i_{н\ ФП\ ЭМИ}$ – стратегия нападения средствами ФП ЭМИ; $i_{н\ РЭП}$ – стратегия нападения средствами РЭП; $i_{н\ ИТВ}$ – стратегия нападения средствами и способами ИТВ; $i_{н\ ФП}^{защ}$ – стратегия защиты средств физического (огневого) поражения от контратакующих воздействий противоборствующей стороны; $i_{н\ ФП\ ЭМИ}^{защ}$ – стратегия защиты средств ФП ЭМИ от контратакующих воздействий противоборствующей стороны; $i_{н\ РЭП}^{защ}$ – стратегия защиты средств РЭП от контратакующих воздействий противоборствующей стороны; $i_{н\ ИТВ}^{защ}$ – стратегия защиты средств ИТВ от контратакующих воздействий противоборствующей стороны.

Формализованное описание информационного конфликта ОТС S_1 и S_2, представленное в виде концептуальной модели (рис. 4.2), в общем случае, отображает совокупность частных информационных конфликтов между отдельными подсистемами и элементами конфликтующих ОТС.

Целями всей возможной совокупности локальных информационных конфликтов, как уже отмечалось, являются:

- со стороны субъекта нападения (ОТС S_2) – получение оперативной информации d_2 о состоянии элементов S_1, как объекта защиты, их возможностях для формирования стратегии нападения i по снижению эффективности/качества функционирования ОТС S_1 по предназначению и достижения выигрыша ξ_2 в информационном конфликте;
- со стороны объекта защиты (ОТС S_1) – получение оперативной информации d_1 о состоянии собственных элементов и их возможностях, а также результатов дестабилизирующих воздействий со стороны ОТС S_2 в интересах выработки стратегии защиты j, направленной на обеспечение требуемой эффективности/качества функционирования ОТС S_1 и достижения выигрыша ξ_1 в информационном конфликте.

Среди множества возможных альтернативных вариантов информационных конфликтов можно выделить следующие, которые являются основными [5]:

- конфликт средств разведки ОТС S_2 с элементами СС СН в составе ОТС S_1, ориентированный на сбор информации о состоянии системы связи путем анализа как ИРИ в электромагнитном диапазоне, так и других каналов утечки информации;
- конфликт средств физического поражения и средств ФП ЭМИ в составе нападающей ОТС S_2 с СС СН в составе ОТС S_1, ориентированный на физическое разрушение информационной инфраструктуры СС СН;
- конфликт средств РЭП и ИТВ в составе ОТС S_2 с СС СН в составе ОТС S_1, ориентированный на нанесение информационного ущерба ОТС S_1, в целом;
- конфликт средств мониторинга ОТС S_1, решающих задачи сбора информации о состоянии системы связи, со средствами разведки стороны ОТС S_2, которые также решают задачу сбора информации о состоянии ОТС S_1 в интересах последующей выработки решения о стратегии нападения;
- конфликт средств разведки ОТС S_2 с ОТС S_1, когда S_1 реализует стратегию контратак на средства разведки S_2 и мероприятия по повышению скрытности S_1;
- конфликт средств нападения ОТС S_2 с ОТС S_1, когда S_1 реализует стратегию контратак на средства нападения S_2 и мероприятия по маскировке элементов S_1;
- локальные конфликты отдельных средств ОТС S_1 и S_2 между собой.

4.5. Формализация основных аспектов, определяющих выигрыш в информационном конфликте

В концептуальной модели информационного конфликта ОТС S_1 и S_2 (рис. 4.2) основополагающими являются следующие основные аспекты.

1) Поведение противоборствующих сторон можно представить в виде последовательности этапов конфликта. На каждом этапе стороны меняют свои состояния. При этом управляющие воздействия сторон, в соответствии с которыми они меняют свои состояния, направлены на восстановление утраченной эффективности функционирования каждой из сторон из-за принятых контрмер противостоящей стороной.

2) Для изменения состояния ОТС на каком-то отдельном этапе конфликта в некоторый момент времени t_k ($k = 0, 1, 2, \ldots, N$) каждой из сторон требуется вполне конкретный временной ресурс $\tau_{1,2}^{реак} > 0$ на выбор стратегии нападения i и стратегии защиты j, а также доведения этих выбранных стратегий действий до объектов управления, где: $\tau_{1,2}^{реак}$ – время реакции управляющей системы; 1, 2 – номера ОТС S_1 и S_2, соответственно.

Для выработки нового решения о стратегиях нападения i и защиты j, которые с учетом эффективности этих стратегий на предыдущем этапе конфликта t_{k-1} обеспечивали бы восстановление или наращивание выигрыша сторон ξ_1, ξ_2 (где 1, 2 – номера ОТС S_1 и S_2), необходимо получение определенного объема данных d_1, d_2 как о состоянии элементов ОТС, так и об эффективности ранее принятого решения.

3) Точки перехода системы из состояния, определяющего успех обороняющейся ОТС S_1, в состояние, определяющее успех нападающей ОТС S_2, являются граничными для двух итерационно-повторяющихся стадий на каждом этапе конфликта:

- стадия нападения длительностью $\tau_2^{нап}$, в течение которого i-ая стратегия нападения ($i \in I$) обеспечивает выигрыш $\xi_2(t_k, i/j)$ ОТС S_2 по отношению к j-ой стратегии защиты ($j \in J$), реализованной противостоящей стороной S_1 на предыдущей стадии t_{k-1}, где I, J – множества альтернативных стратегий нападения и защиты, соответственно;
- стадия защиты длительностью $\tau_1^{защ}$, в течение которого j-ая стратегия защиты обеспечивает выигрыш $\xi_1(t_{k+1}, j/i)$ обороняющейся ОТС S_1 по отношению к i-ой стратегии нападения, реализованной противостоящей стороной S_2 на предыдущей стадии конфликта t_k.

Персональный выигрыш противостоящих ОТС в каждой из точек смены попарно зависимых управляющих воздействий зависит от качества управления в каждой из ОТС, а именно от оперативности, устойчивости, непрерывности и скрытности управляющих воздействий, а также их адекватности сложившейся ситуации на момент t_k.

При этом в формализованном виде выигрыш ξ_1, ξ_2 каждой из сторон S_1, S_2 на каждом из t_k этапов конфликта можно представить в виде функций F_1 и F_2:

$$\begin{cases} \xi_1\left(t_k, j/i\right) = F_1\left(U_{\text{оп}}^{(1)}, U_{\text{ус}}^{(1)}, U_{\text{непр}}^{(1)}, U_{\text{скр}}^{(1)}, U_{\text{ад}}^{(1)}, t_k, j/i\right); \\ \xi_2\left(t_k, i/j\right) = F_2\left(U_{\text{оп}}^{(2)}, U_{\text{ус}}^{(2)}, U_{\text{непр}}^{(2)}, U_{\text{скр}}^{(2)}, U_{\text{ад}}^{(2)}, t_k, i/j\right); \end{cases}$$

где: i, j – i-ая и j-ая стратегии нападения и защиты; $U_{\text{оп}}$, $U_{\text{ус}}$, $U_{\text{непр}}$, $U_{\text{скр}}$, $U_{\text{ад}}$ – показатели оперативности, устойчивости, непрерывности, скрытности и адекватности управления соответственно в ОТС S_1 и S_2.

4) Информационный конфликт характеризуется этапностью протекания. По признаку, определяемому количеством этапов ($N \geq 1$) на длительности конфликта, конфликты ОТС классифицируются на одноэтапные и многоэтапные.

Одноэтапный конфликт (N=1), состоящий из одной стадии – нападения, характеризуется выигрышем в следующих случаях:

- выигрыш субъекта нападения S_2, сделавшего первый ход, соответствует выигрышу $\xi_2(t_k, i/j) >> \xi_1(t_k, j/i)$, при этом у объекта защиты S_1 отсутствуют возможности по реализации эффективной стратегии защиты j, направленной на восстановление требуемого уровня качества функционирования СС СН из-за ограниченности ее ресурсов или отсутствия оперативной информации d_1;
- выигрыш объекта защиты S_1, когда достигается выигрыш над субъектом нападения $\xi_1(t_k, j/i) >> \xi_2(t_k, i/j)$ либо ввиду недостаточно эффективной стратегии нападения i или недостаточности ресурсов нападающей стороны, либо в связи с высокой эффективностью стратегии защиты j.

Многоэтапный конфликт (N>1) характеризуется многократной (N-кратной) сменой выигрышей ОТС S_1 и S_2 в совокупности локальных конфликтов, происходящих на всем протяжении длительности конфликта. Такой конфликт характеризуется способностью ОТС S_1 и S_2 восстанавливать требуемые уровни эффективности своего функционирования за счет реализации адаптивного управления, которое основано на анализе достигнутых выигрышей ξ_1, ξ_2, а также применяемых стратегий нападения i_{k-1} и защиты j_{k-1} на предыдущем этапе конфликта t_{k-1}, с последующем формированием решений о стратегиях нападения i_k и защиты j_k на текущем этапе t_k.

Далее, более подробно рассмотрим многоэтапный информационный конфликт.

4.6. Способы достижения выигрыша в многоэтапном информационном конфликте

Реальные информационные конфликты носят многоэтапный характер, характеризующийся поиском сторонами наиболее рациональных стратегий нападения и защиты и их применением в рамках каждого этапа. Каждый из участников конфликта (рис. 4.2) стремится оценить потенциальный исход конфликта в процессе его развития, учитывая имеющиеся у него априорные исходные данные. Конечной целью функционирования противоборствующих ОТС, как было уже отмечено, является получение выигрыша (выражаемого в матери-

альной, финансовой, информационной, моральной или др. форме) на конечной длительности конфликта $T_{ик}$.

В отсутствие угроз со стороны противника конечный выигрыш ОТС S_1 (ξ_1^0) за время длительности $T_{ик}$ может быть представлен в виде:

$$\xi_1^0 = \xi_{1\,ож}^0 T_{ик},$$

где $\xi_{1\,ож}$ – некоторый усредненный удельный (в единицу времени) ожидаемый выигрыш ОТС S_1 от применения средств связи в отсутствие дестабилизирующих воздействий на элементы СС СН.

В случае, когда нападающей ОТС S_2 реализуются угрозы элементам СС СН траектория поведения ОТС S_1 по показателю удельного выигрыша $\xi_1(t_k)$ является случайной функцией. Она может представлять собой кусочно-непрерывную функцию, имеющую скачки в точках t_0, t_1, …, t_k и непрерывную справа.

На рис. 4.3 показана итерационно-повторяющаяся последовательность чередования следующих стадий на k-ом этапе информационного конфликта:

- $\tau_2^{реак}(t_k)$ – длительность стадии реакции нападающей ОТС S_2, на которой S_2 реализует стратегию разведки $i_р$ с целью сбора данных d_2 о состоянии системы связи ОТС S_1, с учетом принятых ею мер защиты по предыдущем этапе t_{k-1} и формируется стратегия нападения $i_н$;
- $\tau_2^{нап}(t_k)$ – длительность стадии нападения, на которой ОТС S_2 осуществляется доведение до исполнителей и реализация стратегии нападения $i_н$;
- $\tau_1^{реак}(t_k)$ – длительность стадии реакции защищающейся ОТС S_1, на которой осуществляется сбор данных d_1 о состоянии системы связи ОТС S_1 и результатах нападения ОТС S_2, с учетом ранее принятых мер защиты на этапе t_{k-1}, а также формируется стратегия защиты j;
- $\tau_1^{защ}(t_k)$ – длительность стадии защиты, на которой ОТС S_1 осуществляется доведение до исполнителей и реализация стратегии защиты j.

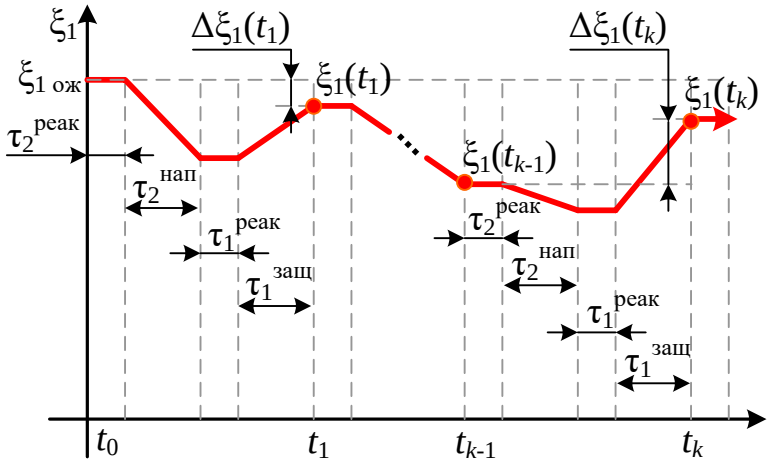

Рис. 4.3. Траектория изменения удельного выигрыша $\xi_1(t_k)$ ОТС S_1, как объекта защиты при наличии угроз нападающей ОТС S_2

Длительность реакции защищающейся ОТС $\tau_1^{реак}(t_k)$ определяется оперативностью системы управления при формировании стратегии защиты j и ее до-

ведения до управляемых средств защиты системы связи. Уровни изменения выигрыша $\Delta\xi_1$ на временной оси t соответствуют эффективности стратегий нападения $i_н$ и защиты j с учетом адекватности выбранных стратегий в соответствии со сложившейся обстановкой на момент их выбора соответствующими ОТС.

Область определения ступенчатой функции $\xi_1(t)$ на временной оси определяется суммой конкретного числа N стадий конфликта (k = 0, 1, 2, …, N), границами которых являются моменты t_k. Моменты

$$t_k + \tau_2^{реак}(t_k) \text{ и } t_k + \tau_2^{реак}(t_k) + \tau_2^{нап}(t_k) + \tau_1^{реак}(t_k),$$

соответствуют выработке новых решений, соответственно ОТС S_2 по реализации нападения и ОТС S_1 по реализации защиты. Итоговые изменения выигрыша $\Delta\xi_1(t_k)$ определяют эффективность выбранных стратегий нападения и защиты в момент t_k завершения k-го этапа информационного конфликта. Для каждой точки t_k можно определить справа приращения удельного выигрыша $\Delta\xi_1(t_k)$ как случайные величины:

$$\Delta\xi_1\left(t_k,\vec{U}\right)=\xi_1\left(t_k,\vec{U}\right)-\xi_1\left(t_{k-1},\vec{U}\right), \text{ при этом } \vec{U}=\left(U_{ад},U_{непр},U_{оп},U_{скр},U_{ус}\right),$$

где: $\vec{U}$ – вектор качества управления в ОТС S_1; $U_{ад}$ – составляющая адекватности управления; $U_{непр}$ – составляющая непрерывности управления; $U_{оп}$ – составляющая оперативности управления; $U_{скр}$ – составляющая скрытности управления; $U_{ус}$ – составляющая устойчивости управления.

Приращения $\Delta\xi_1(t_k)$ являются независимыми, т.е не зависят от номера этапа t_k. Случайный характер изменения $\Delta\xi_1(t_k)$ обусловлен, в основном, влиянием на удельную эффективность конфликтующих ОТС S_1 и S_2 таких факторов, как:

- качество стратегии защиты j, выбранной на k-ом этапе конфликта, как меры противодействия конкретной стратегии нападения i на этом же этапе;
- адекватность принятого решения об использовании конкретной стратегии защиты j из множества альтернатив J, а также соответствие этой стратегии сложившейся ситуации в момент $t_k + \tau_2^{реак}(t_k) + \tau_2^{нап}(t_k)$ и стратегии нападения i;
- скорость принятия решения $\tau_1^{реак}$ о выборе стратегии j, а также скрытность и непрерывность доведения действий в соответствии с выбранной стратегией j управляемым объектам СС СН.

Как видно из траектории поведения, приведенной на рис. 4.3, нападающая ОТС S_2 может повысить эффективность реализации нападения (измеряемого по выигрышу $\Delta\xi_2(t_k) = -\Delta\xi_1(t_k)$), либо за счет более оперативного формирования стратегии нападения i т.е. $\tau_2^{реак}\downarrow$, либо за счет повышения эффективности самой стратегии нападения $\Delta\xi_2(t_k)\uparrow$. Аналогично, защищающаяся ОТС S_1 может повысить эффективность реализации защиты $\Delta\xi_1(t_k)$ либо за счет более оперативного формирования стратегии защиты j т.е. $\tau_1^{реак}\downarrow$, либо за счет повышения эффективности самой стратегии защиты $\Delta\xi_1(t_k)\uparrow$.

Необходимо отметить, что даже своевременное и адекватное сложившейся ситуации формирование стратегии защиты j на каждом этапе конфликта не

гарантирует окончательного выигрыша для защищающейся ОТС S_1. Отсутствие таких гарантий объясняется тем обстоятельством, что нападающая сторона S_2 реализует стратегии нападения i, на принятие решения по противодействию которым защищающейся стороне S_1 требуется уже значительно меньшее время в рамках фиксированной длительности каждого конфликтного этапа. Сокращение располагаемого времени реакции, доступного обороняющейся стороне S_1 относительно нападающей стороны $\tau_1^{реак} < \tau_2^{реак}$ в рамках одного этапа конфликта, приводит к снижению выигрыша для обороняющейся ОТС $\Delta\xi_1(t_k)\downarrow$ и повышению его для нападающей ОТС $\Delta\xi_2(t_k)\uparrow$.

В многоэтапном информационном конфликте (при наличии соответствующих ресурсных возможностей у каждой из противостоящих сторон) затягивание формирования адекватных сложившейся ситуации стратегий действий и доведения их до исполнителей ($\tau^{реак}\uparrow$) приводит к снижению среднего интегрального выигрыша $\xi^{инт}$ (среднего за время конфликта $T_{ик}$). В этом случае интегральный выигрыш $\xi^{инт}$ у противоположной стороны увеличивается. Аналогичным образом, даже более оперативное формирование управляющих стратегий ($\tau^{реак}\downarrow$), которые неадекватны сложившейся ситуации (например, вследствие получения недостоверных данных d_1, d_2), приводит к выбору неверных стратегий (i, j), которые не только не обеспечивают достижение выигрыша $\Delta\xi(t_k)$ на текущем этапе, но и усугубляют проигрыш. Это также приводит к снижению среднего интегрального выигрыша $\xi^{инт}$ на длительности информационного конфликта $T_{ик}$. Таким образом, достигаемый уровень среднего интегрального выигрыша $\xi^{инт}$ на длительности конфликта $T_{ик}$ может служить мерой информационного превосходства одной стороны над другой в многоэтапном информационном конфликте (рис. 4.4).

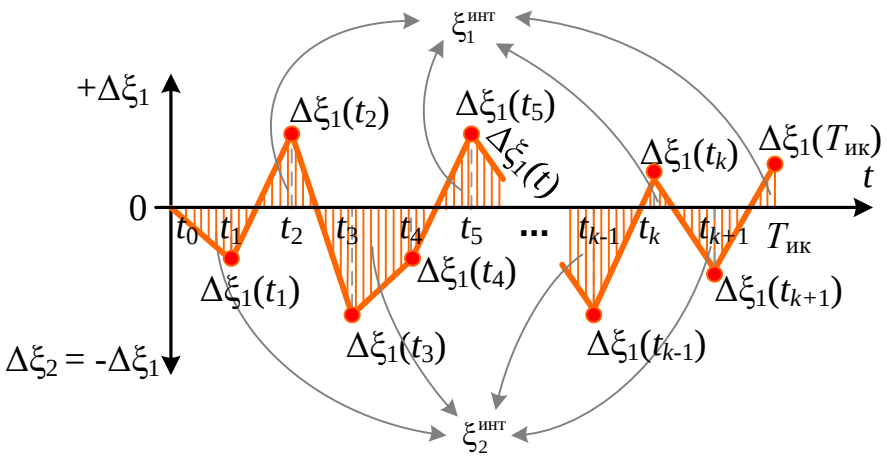

Рис. 4.4. Функция $\xi_1(t_k)$ и определение на ее основе средних интегральных выигрышей конфликтующих сторон $\xi_1^{инт}$ и $\xi_2^{инт}$, как суммы соответствующих площадей

В формальном виде уровни среднего интегрального выигрыша $\xi^{инт}$ для сторон на длительности конфликта $T_{ик}$ можно оценить следующим образом:

- для дискретных значений выигрыша $\Delta\xi(t_k)$ на каждом этапе:

$$\xi_1^{инт} = \frac{1}{T_{ик}} \sum_{i=1}^{T_{ик}} \left(\Delta\xi_1(t_i) \middle| \Delta\xi_1(t_i) > 0 \right),$$

$$\xi_2^{инт} = \frac{1}{T_{ик}} \sum_{i=1}^{T_{ик}} \left(\Delta\xi_2(t_i) \middle| \Delta\xi_2(t_i) > 0 \right)$$ при том, что $\Delta\xi_2(t_k) = -\Delta\xi_1(t_k)$;

- для непрерывной функции выигрыша $\Delta\xi(t)$:

$$\xi_1^{инт} = \frac{1}{T_{ик}} \int_{t_0}^{T_{ик}} \Delta\xi_1(t)\,dt,$$ при том, что $$\Delta\xi_1(t) = \begin{cases} \Delta\xi_1(t), \text{ если } \Delta\xi_1(t) > 0; \\ 0, \text{ если } \Delta\xi_1(t) \le 0. \end{cases}$$

$$\xi_2^{инт} = \frac{1}{T_{ик}} \int_{t_0}^{T_{ик}} \Delta\xi_2(t)\,dt$$, при том, что $$\Delta\xi_2(t) = \begin{cases} \Delta\xi_2(t), \text{ если } \Delta\xi_2(t) > 0; \\ 0, \text{ если } \Delta\xi_2(t) \le 0; \end{cases}$$ и $\Delta\xi_2(t_k) = -\Delta\xi_1(t_k)$.

Общим критерием выигрыша в информационном конфликте может являться достижение информационного преимущества по показателю среднего интегрального выигрыша на длительности конфликта $T_{ик}$:

$\xi_1^{инт} - \xi_2^{инт} > 0$ – выигрыш защищающейся ОТС S_1;

$\xi_1^{инт} - \xi_2^{инт} < 0$ – выигрыш нападающей ОТС S_2;

$\xi_1^{инт} - \xi_2^{инт} = 0$ – ничья.

4.7. Эффективность управления организационно-технической системой в условиях информационного конфликта

4.7.1. Управление организационно-технической системой в условиях информационного конфликта

Из приведенного выше содержательного описания факторов конфликтного взаимодействия ОТС S_1 и S_2 на длительности конфликта можно сделать следующие выводы.

1) Способность управляющей системы ОТС S_1 вырабатывать стратегию защиты j и управляющие воздействия на управляемые объекты после внешнего воздействия на СС СН в интересах восстановления требуемого качества функционирования ОТС S_1 зависит от показателей оперативности, устойчивости, непрерывности, скрытности и адекватности управления.

2) Управляющая система ОТС S_1, при реализации нападающей ОТС S_2 дестабилизирующих воздействий, должна обладать *устойчивостью* – способностью оперативно и непрерывно вырабатывать управляющие воздействия адекватные складывающейся ситуации, а также непрерывно и скрытно доводить их в условиях дестабилизирующих воздействий.

3) Состояние ОТС S_1 как объекта защиты на длительности конфликта при реализации угроз как системе связи, так и системе управления, должно быть конфликтно-устойчивым к соответствующей стратегии нападения i. Эта устой-

чивость обеспечивается как непосредственно устойчивостью СС СН, так и эффективностью реализации соответствующей стратегии защиты j.

4) Понятие устойчивости может относиться как к управляющей системе СС СН, так и к системе управления ОТС S_1, которая функционирует совместно с СС СН. Конфликтно-устойчивая система способна при наличии внешних дестабилизирующих воздействий различного характера, обеспечить достижение целевой функции (требуемой эффективности/качества) на длительности ее функционирования в соответствии с ее предназначением.

5) Для оценки вклада устойчивости СС СН в устойчивость системы управления ОТС S_1 целесообразно определить обобщенный показатель устойчивости управления как количественную характеристику способности ОТС S_1 обеспечивать восстановление управления в условиях информационного конфликта. Такой обобщенный показатель устойчивости должен быть чувствительным к изменению частных показателей качества управления, к которым, в первую очередь, следует отнести показатели адекватности, непрерывности, скрытности и оперативности управления.

6) Должна быть установлена взаимосвязь между обобщенным показателем устойчивости системы управления ОТС S_1 и показателем эффективности применения управляемых объектов по предназначению в соответствии с их целевой функцией, в первую очередь – с устойчивостью СС СН.

Таким образом, так как СС СН функционирует совместно с системой управления ОТС S_1, причем СС СН должна непрерывно, скрытно и своевременно передавать управляющие воздействия управляемым объектам, актуальной задачей является оценка вклада конфликтно-устойчивого функционирования СС СН в устойчивость системы управления ОТС S_1. В связи с этим, далее рассмотрим один из подходов стратифицированного описания системы показателей устойчивости системы управления ОТС S_1 с учетом конфликтно-устойчивого состояния СС СН.

В условиях реализации нападающей ОТС S_2 дестабилизирующих воздействий на СС СН, первостепенное значение имеет быстрое восстановление в короткие сроки нарушенного управления в ОТС S_1 в сложившихся условиях обстановки. Устойчивость управления в ОТС S_1 может быть достигнута в результате применения совокупности мер и контрмер по нейтрализации стратегии нападения. Будем полагать, что в рамках информационного конфликта важнейшим условием сохранения устойчивости и непрерывности управления в ОТС S_1 является реализация пассивной стратегии защиты $j_{сс}$ средств СС СН от дестабилизирующих воздействий средств разведки и нападения. Пассивная стратегия $j_{сс}$ составляет основу стратегии защиты j, а активные стратегии контратак средств разведки $j_р$ и средств нападения $j_н$ – являются вспомогательными.

Рассмотрим перечень показателей, по которым возможна оценка устойчивости системы управления ОТС S_1, так и системы связи, ее обслуживающей.

На длительности информационного конфликта $T_{ик}$ элементы ОТС S_1 должны быть управляемыми со стороны системы управления S_1, а их состояние от этапа к этапу должно изменяться при получении управляющих воздействий

в моменты времени t_k, $k = 1, 2, \ldots, N$. В этом случае качество управления (формирования и доведения управляющих воздействий до управляемых объектов) определяет способность ОТС S_1 к восстановлению требуемой удельной эффективности в динамике конфликта $\xi_1 \rightarrow \xi_{1\,ож}$.

Понятие «качество управления», применительно к ОТС S_1, характеризует совокупность ее существенных свойств как управляющей системы к сбору, хранению, передаче, обработке и представлению для лиц, принимающих решения, постоянной и текущей (оперативной) информации о состоянии ее элементов и окружающей среды, с последующей переработкой этой информации в управляющие воздействия, передаваемые на управляемые объекты с целью достижения цели функционирования.

Управляющие воздействия, представляющие собой командную (распорядительную) информацию объема $V_к$, доводимую до управляемых объектов, являются результатом преобразования постоянной ($V_{пос}$)) и текущей ($V_{тек}$) информации в процессе принятия решения органами управления. Управляющие воздействия $V_к$ указывают управляемым объектам время и способ достижения поставленной цели (выигрыша). Управляющие воздействия соответствуют конкретной стратегии конфликтного взаимодействия. При этом к частным показателям качества управления, характеризующим отдельные общесистемные свойства ОТС, относят показатели оперативности, адекватности, непрерывности, скрытности и устойчивости управления.

Вектор качества управления $\vec{U}$ может быть определен в многомерной (в данном случае – пятимерной) системе координат составляющими адекватности ($U_{ад}$), оперативности ($U_{оп}$), непрерывности ($U_{непр}$), скрытности ($U_{скр}$) и устойчивости ($U_{ус}$) управления, которые являются проекциями вектора качества управления $\vec{U}$ на соответствующие координатные оси: адекватности, непрерывности, скрытности, оперативности и устойчивости. В свою очередь, составляющие $U_{ад}$, $U_{непр}$, $U_{скр}$, $U_{оп}$, $U_{ус}$ определяются технико-эксплуатационными характеристиками элементов ОТС S_1.

Вектор качества управления $\vec{U}$ при разложении по единичным базисным составляющим $\vec{e}_{ад}$, $\vec{e}_{непр}$, $\vec{e}_{скр}$, $\vec{e}_{оп}$, $\vec{e}_{ус}$ запишется как

$$\vec{U} = |U_{ад}|\vec{e}_{ад} + |U_{непр}|\vec{e}_{непр} + |U_{скр}|\vec{e}_{скр} + |U_{оп}|\vec{e}_{оп} + |U_{ус}|\vec{e}_{ус},$$

где: $\vec{e}_{ад}$ – единица показателя (базовой вектор) адекватности управления в ОТС;
$\vec{e}_{непр}$ – единица показателя (базовой вектор) непрерывности управления в ОТС;
$\vec{e}_{скр}$ – единица показателя (базовой вектор) скрытности управления в ОТС;
$\vec{e}_{оп}$ – единица показателя (базовой вектор) оперативности управления в ОТС;
$\vec{e}_{ус}$ – единица показателя (базовой вектор) устойчивости управления в ОТС;
$|U_{ад}|$, $|U_{непр}|$, $|U_{скр}|$, $|U_{оп}|$, $|U_{ус}|$ – проекции вектора $\vec{U}$ на соответствующие координатные оси адекватности, непрерывности, скрытности, оперативности и устойчивости.

Смешанное (векторно-скалярное) произведение элементарных векторов $|U_{ад}|e_{ад}$, $|U_{непр}|e_{непр}$, $|U_{скр}|e_{скр}$, $|U_{оп}|e_{оп}$, $|U_{ус}|e_{ус}$ запишется в виде

$$U = U_{ад}U_{непр}U_{оп}U_{скр}U_{ус},$$

и представляет собой произведение показателей адекватности, непрерывности, скрытности, оперативности и устойчивости.

Для последнего произведения характерен простой физический смысл – это произведение характеризует некоторый многомерный объем, определенный численными значениями частных показателей качества управления. Объем U, при использовании нормированных составляющих $U_{ад} \leq 1$, $U_{непр} \leq 1$, $U_{скр} \leq 1$, $U_{оп} \leq 1$, $U_{ус} \leq 1$ может служить в качестве обобщенного показателя качества управления ОТС, при условии, что идеальное управление U соответствует показателям $U_{ад} = 1$, $U_{непр} = 1$, $U_{скр} = 1$, $U_{оп} = 1$, $U_{ус} = 1$, т.е. единичному объему.

Достижение конечной цели функционирования ОТС S_1 обеспечивается достижением частных целей (выполнением частных задач) при декомпозиции конечной цели на подцели разных уровней иерархии. Выполнение задач на каждом уровне иерархии определяется ответствующими показателями, совокупность которых образует систему взаимосогласованных показателей. Под системой показателей далее понимается совокупность показателей различного уровня иерархии с набором связей между ними, обладающих определенным способом их упорядочения.

4.7.2. Многоуровневая модель управления организационно-технической системой в условиях информационного конфликта

При стратифицированном подходе показатель каждого уровня иерархии имеет область своего применения и целевое назначение. В случае оценки влияния качества управления на эффективность функционирования ОТС S_1 в информационном конфликте можно выделить следующие уровни и описания, учитывая назначение и область их применения (рис. 4.5):

- *уровень конфликтного взаимодействия ОТС*, определяемый обобщенным показателем $\xi_1(T_{ик}, \vec{U})$, количественно характеризующим эффективность (результативность, качество) функционирования ОТС S_1 применительно к степени достижения цели функционирования этой ОТС в условиях информационного конфликта;
- *информационно-управленческий уровень*, определяемый системой показателей качества управления $\vec{U} = \left(U_{ад}, U_{непр}, U_{оп}, U_{скр}, U_{ус}\right)$, характеризующих способность управляющей системы ОТС адекватно, непрерывно, оперативно, скрытно и устойчиво формировать и передавать управляющие воздействия на объекты управления в ОТС S_1, которые возвращают эту ОТС в состояние $\xi_1 \rightarrow \xi_{1\,ож}$, после того, как она была выведена из устойчивого состояния $\xi_{1\,ож}$ под влиянием преднамеренных воздействий со стороны нападающей ОТС S_2;
- *информационный уровень*, определяемый частными показателями: смысловой (энтропийной) ценностью ψ информации; информационным ущербом γ; вероятностью актуальности информации ($P_{акт}$) и ее полноты ($P_{полн}$). При этом под информацией понимается либо командная ($V_к$), либо постоянная ($V_{пос}$) или текущая ($V_{тек}$) информации, кото-

рая будучи полученной и обработанной может использоваться для нужд управления ОТС S_1;

- *технический уровень*, определяемый совокупностью частных показателей Q, которые характеризуют качество формирования ($Q_{форм}$), передачи ($Q_{прд}$), хранения ($Q_{хр}$), обработки ($Q_{обр}$) и представления ($Q_{пр}$) информации в ОТС соответствующими техническими средствами ОТС S_1. Для процессов передачи информации, реализуемых СС СН, являющейся подсистемой ОТС S_1, к таким показателям относятся своевременность ($P_{св}$), достоверность ($P_{дост}$) и безопасность ($P_{без}$) связи (рис. 1.4).

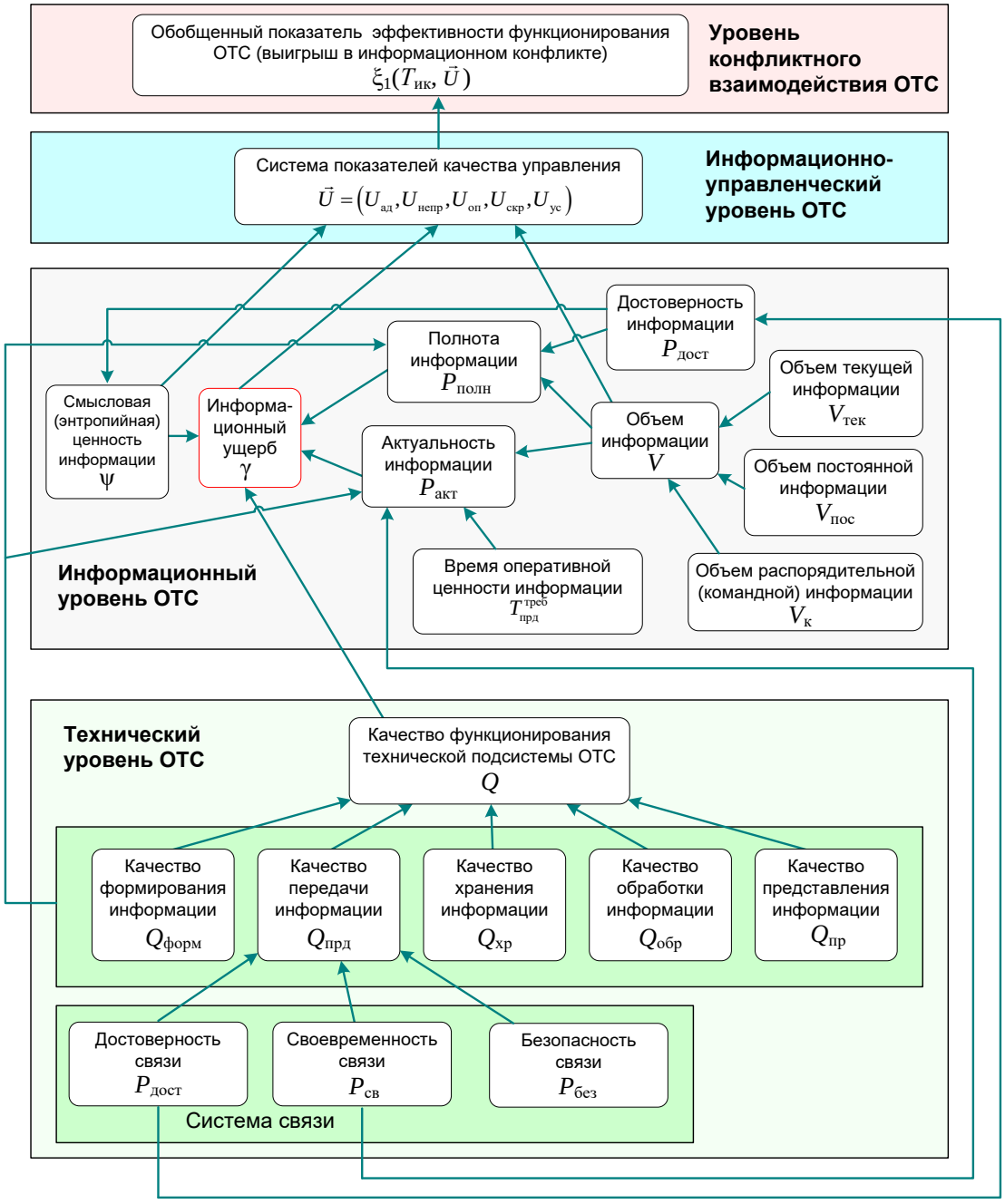

Рис. 4.5. Многоуровневая система взаимосвязанных показателей, определяющая влияние качества управления на эффективность функционирования ОТС S_1

Нужно отметить, что на техническом уровне, в отличие от информационного уровня, под информацией понимается, прежде всего, цифровая форма ее представления – данные, которые формируются, передаются, хранятся, обрабатываются и представляются (визуализируются) в ОТС S_1.

Показатели на рис. 4.5 на каждом из уровней их иерархии имеют собственные наименования, обозначения, формулировки, способы их экспериментального или расчетного определения, численные значения и различную размерность. Поэтому, при выборе и обосновании обобщенного показателя эффективности функционирования ξ_1 и обобщенного показателя качества управления $\vec{U}$, используют не абсолютные значения этих различных показателей, а нормированные, обеспечивающие приведение этих показателей к одному масштабу:

$$x^{\text{норм}} = \frac{x}{x_{\text{ид}}},$$

где: x – абсолютное значение некоторого показателя ОТС; $x^{\text{норм}}$ – нормированное значение показателя x; $x_{\text{ид}}$ – некоторое идеальное значение показателя x в условиях отсутствия дестабилизирующих воздействий на элементы ОТС S_1.

4.7.3. Понятие информационного ущерба

Наличие дестабилизирующих воздействий на СС СН в составе ОТС S_1 приводит к ухудшению способности СС СН передавать информацию, а именно, к разрушению информации (снижению ее полноты) и задержке ее передачи (снижению ее актуальности). В этом случае относительные информационные потери, превышающие некоторый допустимый уровень, который соответствует передачи информации по СС СН с требуемым уровнем достоверности ($P_{\text{дост}}^{\text{треб}}$) и в срок ее оперативной ценности ($T_{\text{прд}}^{\text{треб}}$), определяют относительный уровень информационного ущерба γ:

$$\gamma = 1 - P_{\text{полн}} P_{\text{акт}},$$

где

$$P_{\text{полн}} = \frac{V\left(P_{\text{дост}} \geq P_{\text{дост}}^{\text{треб}}\right)}{V},$$

$$P_{\text{акт}} = \frac{V\left(T_{\text{прд}} \leq T_{\text{прд}}^{\text{треб}}\right)}{V}.$$

В вышеуказанных выражениях: $P_{\text{полн}}$ – вероятность обеспечения полноты передаваемой по СС СН информации; $P_{\text{акт}}$ – вероятность обеспечения актуальности передаваемой по СС СН информации; $P_{\text{дост}}$ – вероятность обеспечения достоверности передаваемой по информации; $P_{\text{дост}}^{\text{треб}}$ – требуемый уровень достоверности передаваемой по информации; $T_{\text{прд}}$ – время передачи информации по СС СН; $T_{\text{прд}}^{\text{треб}}$ – требуемое время передачи информации по СС СН, в течение которого информация сохраняет свою актуальность (оперативную ценность); V – полный объем переданной по СС СН информации; $V(P_{\text{дост}} \geq P_{\text{дост}}^{\text{треб}})$ – объем информации принятой с требуемым уровнем достоверности; $V(T_{\text{прд}} \leq T_{\text{прд}}^{\text{треб}})$ – объем информации переданный в срок ее оперативной ценности.

Таким образом, в ОТС S_1 могут иметь место как допустимый информационный ущерб $\gamma \le \gamma(P_{дост}^{треб}, T_{прд}^{треб})$, который определяется требуемым уровнем достоверности приема актуальной информации, так и необратимый информационный ущерб, когда $\gamma > \gamma(P_{дост}^{треб}, T_{прд}^{треб})$. Именно необратимый информационный ущерб снижает качество управления, и как следствие, уменьшает выигрыш ОТС S_1 в информационном конфликте.

Наличие информационного ущерба γ приводит:

- к увеличению длительности формирования управляющих воздействий при обеспечении заданного уровня актуальности и полноты получаемой текущей информации;
- к снижению адекватности принятого решения относительно сложившейся ситуации на момент принятия решения для заданного интервала (нормативного) интервала времени, отводимого на выработку и принятие решения;
- к необходимости проведения мероприятий по повышению полноты и актуальности информации, передаваемой в СС СН, что, в свою очередь, с одной стороны, приводит к повышению объема данных, достоверности и своевременности передачи, а, с другой, к увеличению возможностей субъекта нападения S_2 в отношении ОТС S_1 в процессе ее функционирования из-за увеличения вероятности перехвата, искажения или уничтожения передаваемой информации.

Отметим, что вышеуказанный подход к расчету показателей полноты и актуальности информации, а, следовательно, и информационного ущерба является не единственным.

В стандарте [403], в предположении о пуассоновской аппроксимации потока появления новых или изменения существующих объектов или явлений реальной обстановки, о которых поступает информация, соответствующие вероятности предложено рассчитывать следующим образом.

Полнота информации [403]:

$$P_{полн} = \exp\left(-\lambda_{изм}\left(T_{форм} + T_{прд} + T_{хр} + T_{обр} + T_{пр}\right)\right);$$

где: $\lambda_{изм} = 1/T_{изм}$ – средняя интенсивность (темп) изменения реальной обстановки, появления новых или изменения существующих объектов или явлений в процессе функционирования ОТС; $T_{форм}$ – среднее время формирования информации о новых событиях и явлениях реальной обстановки; $T_{прд}$ – среднее время передачи информации по СС СН; $T_{хр}$ – среднее время хранения информации; $T_{обр}$ – среднее время обработки информации в управляющей системе; $T_{пр}$ – среднее время представления информации органу или лицу, принимающему решение.

Актуальность информации [403]:

а) для дисциплины выдачи информации от источника сразу же по происшествии значимого изменения реальной обстановки:

$$P_{акт} = \frac{T_{изм}}{T_{изм} + \left(T_{форм} + T_{прд} + T_{хр} + T_{обр} + T_{пр}\right)};$$

б) для дисциплины выдачи информации через среднее время $T_{обн}$, вне зависимости от наличия или отсутствия значимого изменения реальной обстановки:

$$P_{акт} = \frac{T_{изм}^{\ 2}}{\left(T_{изм} + \left(T_{форм} + T_{прд} + T_{хр} + T_{обр} + T_{пр}\right)\right)\left(T_{изм} + T_{обн}\right)};$$

в) для дисциплины, в которой обновление информации о реальной обстановке осуществляется через строго постоянный интервал времени $T_{обн}$:

$$P_{акт} = \frac{T_{изм}^{\ 2}}{T_{обн}\left(T_{изм} + \left(T_{форм} + T_{прд} + T_{хр} + T_{обр} + T_{пр}\right)\right)}\left(1 - \exp\left(-\frac{T_{обн}}{T_{изм}}\right)\right);$$

где: $T_{изм}$ – среднее время изменения реальной обстановки, появления новых или изменения существующих объектов или явлений, в процессе функционирования ОТС; $T_{обн}$ – среднее или фиксированное время обновления информации в системе управления.

Соответствующим образом, по выражению $\gamma = 1 - P_{полн} P_{акт}$, рассчитывается и информационный ущерб. К достоинствам расчета показателей полноты и актуальности информации, используемого в работе [403], необходимо отнести более полный учет темпа изменения реальной обстановки, а также временных параметров формирования, передачи, хранения, обработки и представления информации в управляющей системе. К недостатку – отсутствие учета передаваемых объемов информации, а также достоверности передачи.

4.8. Актуальные направления совершенствования концептуальной модели

Представленная в предыдущих подразделах концептуальная модель, может быть развита по различным направлениям, в зависимости от необходимости учета тех или иных аспектов информационного конфликта. Далее рассматриваются основные направления совершенствования концептуальной модели.

4.8.1. Модель информационного конфликта между сторонами, состоящими из систем управления и связи, системы разведки и дестабилизирующих воздействий

В работах В.Г. Радзиевского, А.А. Сироты [94, 204] представлено развитие концептуальной модели за счет представления каждой конфликтующей стороны как совокупности следующих систем (рис. 4.6):

- системы управления;
- системы связи;
- системы разведки, объединяющей средства РРТР, ОЭР, компьютерной и радиолокационной разведки;
- системы, реализующей дестабилизирующие воздействия (объединяющей средства физического поражения, ФП ЭМИ, РЭП, ИТВ).

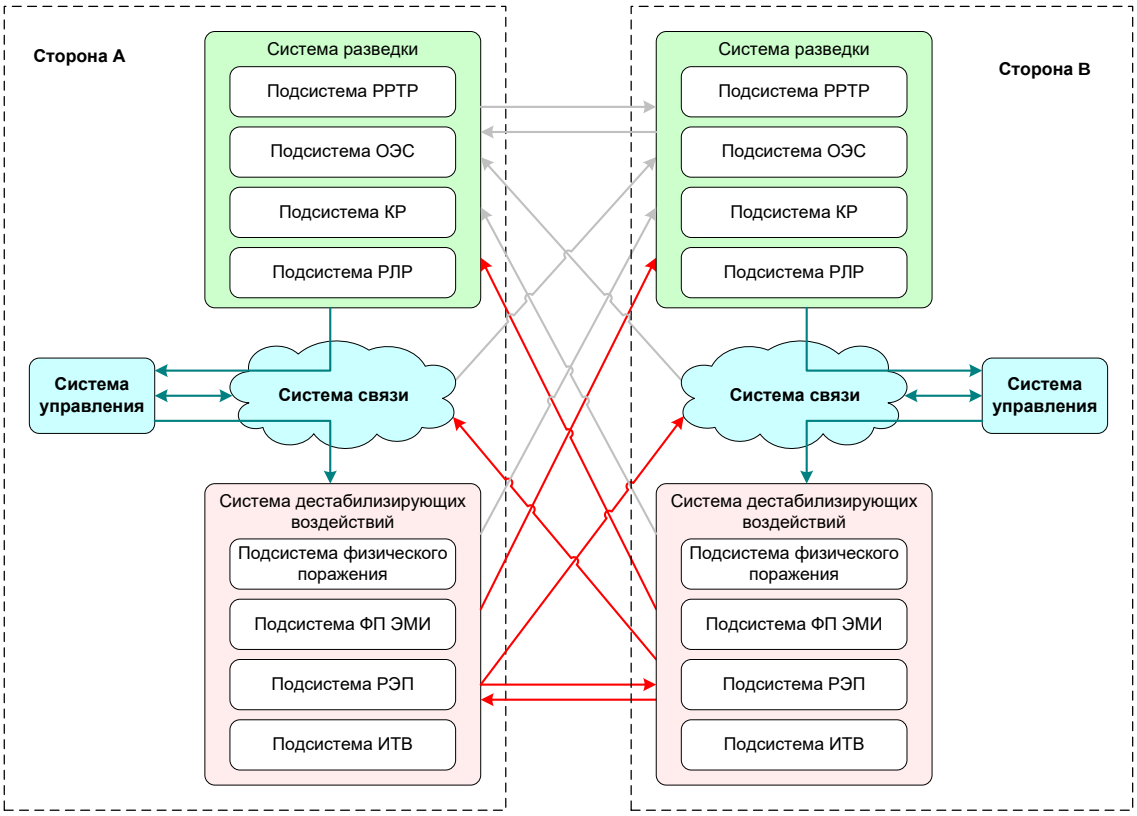

Рис. 4.6. Схема концептуальной модели информационного конфликта [94, 204]

На схеме модели (рис. 4.6) серыми стрелками обозначено вскрытие средствами разведки параметров средств нападения, средств связи и средств разведки противоположной стороны, красными – дестабилизирующие воздействия средств нападения на аналогичные средства, средства связи и средства разведки противоборствующей стороны, зеленым – направления циркуляции информационных потоков внутри контура управления своей стороны.

Аналогичная модель, представлена и в работе [6], с той разницей, что в [6] элементы противоборствующих сторон сгруппированы в группы основных элементов, атакующих элементов и обороняющихся элементов.

Отличительной особенностью модели, представленной на рис. 4.6, является то, что основное противоборство сторон сосредотачивается по направлению атак систем, которые реализуют дестабилизирующие воздействия. Именно эти системы ведут основное боевое противоборство, система разведки осуществляет их информационную поддержку, а система управления – управляет процессами. В этом случае задача системы связи – обеспечение своевременной, достоверной и безопасной связью всех участников противоборства со своей стороны. Отметим, что нарушение нормального функционирования системы связи фактически ведет к разрыву цикла управления боевыми действиями, и как следствие – к проигрышу данной стороны.

Представленная на рис. 4.6 схема конфликта является типовой схемой двустороннего симметричного информационного конфликта. Она не исчерпывает всего многообразия ситуаций. Часто, например, встречается ситуация несимметричного двустороннего конфликта, когда одна из сторон реализует

меры как активного, так и пассивного воздействия, тогда как другая сторона реализует только пассивные стратегии взаимодействия. Возможен и многосторонний конфликт, в который включается множество участников с каждой стороны. В этом плане, необходимо отметить, что в рамках конфликтующих систем может содержаться не один, а несколько разнородных по объектам и задачам информационного взаимодействия подсистем или комплексов.

4.8.2. Модель информационного конфликта с координацией конфликтующих систем

Переход к сетецентрическому управлению [10] боевыми действиями, предполагает, что все элементы систем, участвующих в конфликте, будут сопряжены через единое информационное пространство (сетецентрическую среду). При этом средства разведки и средства, реализующие дестабилизирующие воздействия, будут напрямую обмениваться информацией через систему связи, а роль системы управления сведется к координации этих средств (рис. 4.7).

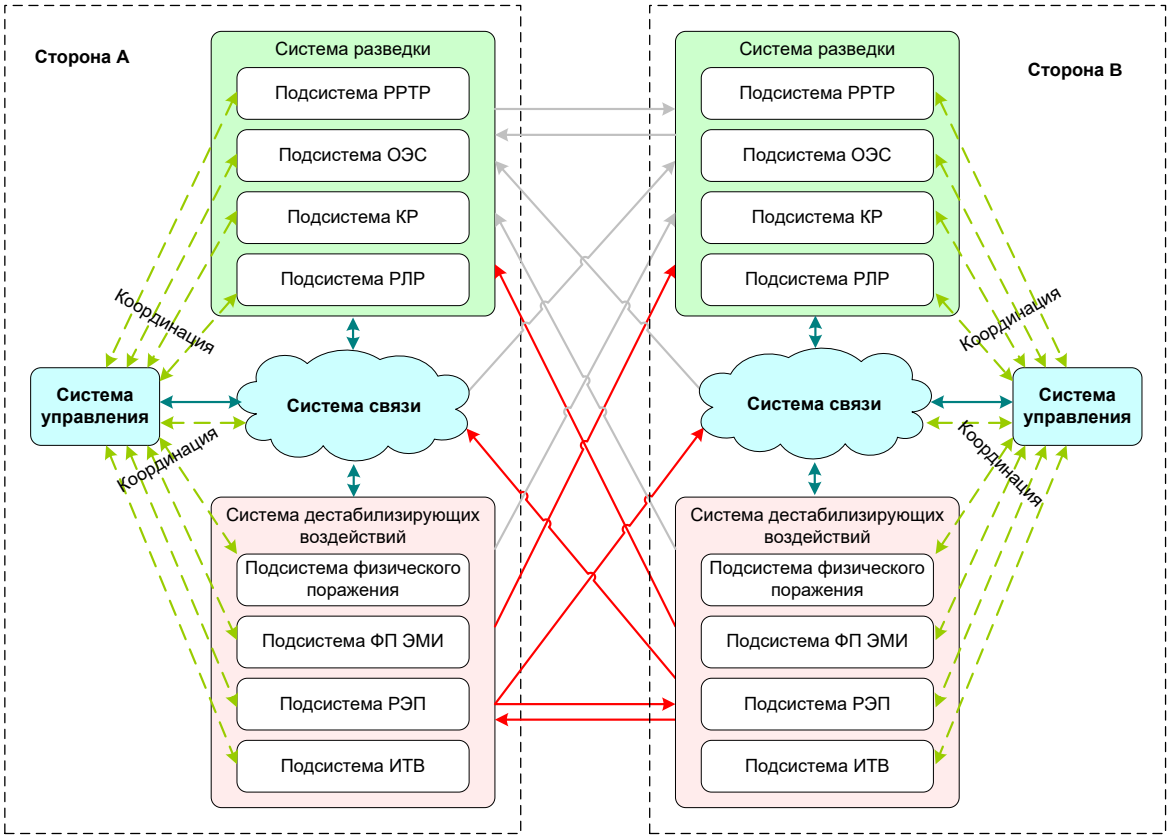

Рис. 4.7. Схема концептуальной модели информационного конфликта с координацией конфликтующих подсистем

Данный вариант информационного конфликта подробно исследован в работах Р.Л. Михайлова [198, 205-209]. Фактически, модель Р.Л. Михайлова является развитием модели В.Г. Радзиевского и А.А. Сироты с учетом современных тенденций перехода военного противоборства к сетецентрическим принципам управления. При этом надо отметить, что в работах Р.Л. Михайлова [198, 205-209] подробно рассмотрен информационный конфликт исключительно си-

стемы связи, с одной стороны, и подсистем РР и РЭП, с другой стороны. По всей видимости формирование обобщенной модели, в том виде, в котором она представлена на рис. 4.7, относится к направлению дальнейших исследований.

4.8.3. Модель информационного конфликта в глобальном инфокоммуникационном пространстве с учетом возможностей захвата информационных ресурсов и подыгрыша среды функционирования

В работах Ю.И. Стародубцева, С.С. Семенова, В.В. Бухарина [193-195, 210-212] предложена и исследована модель военного конфликта в едином общемировом информационном пространстве – техносферная война. Можно утверждать, что техносферная война является наиболее обобщенной моделью информационного конфликта и включает в себя не только военное противоборство в классических сферах войны (суша, море, воздух), но и новые тенденции перехода систем управления к сетецентрическим принципам, а также усиливающуюся роль информационного противоборства, ареной может является все мировое инфокоммуникационное пространство (рис. 4.8).

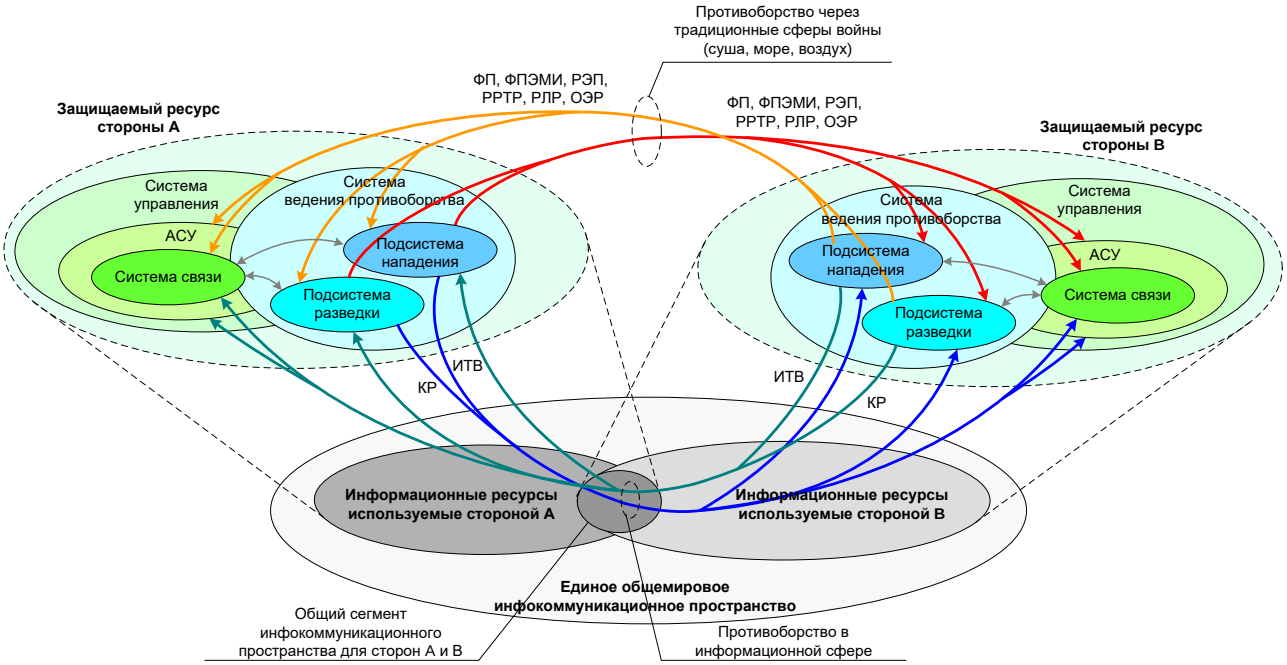

Рис. 4.8. Модель информационного конфликта в глобальном инфокоммуникационном пространстве с учетом возможностей захвата информационных ресурсов и подыгрыша среды функционирования

Оригинальными особенностями данной модели является учет следующих факторов:

- насыщение средств разведки, поражения, систем управления войсками и оружием, аппаратно-программными средствами, которые, в соответствии с сетецентрической концепцией, включены в единую сетецентрическую среду;

- сетецентрические среды современных вооруженных сил, существуют не изолированно, а напротив – основаны на системах связи, включенных в состав единого общемирового инфокоммуникационного пространства. Более того, существенные части мирового инфокоммуникационного пространства в случае военных конфликтов становятся частью сетецентрической среды (например, ВС США арендуют значительную часть пропускной способности отдельных коммерческих ССС для информационного обеспечения удаленных ТВД [383]);
- с информатизацией средств вооружения растет доля операций, проводимых в рамках военного конфликта не через традиционные сферы войны (суша, море, воздух), а через мировое инфокоммуникационное пространство. При этом ввиду сопряженности сетей связи военного и гражданского назначения для ИТВ через совместно используемые сетевые ресурсы оказываются доступными фактические любые средства вооружения и системы управления ими;
- масштабность и эффективность проведения ИТВ против противоборствующей стороны зависит от объема совместно используемых и располагаемых ресурсов в мировом инфокоммуникационном пространстве. В связи с этим к отдельной задаче, обеспечивающей наращивание возможностей конкретной стороны в плане эффективности своих ИТВ, является захват как можно большего количества ресурсов инфокоммуникационного пространства с целью увеличения своих возможностей, а также точек сопряжения с системой связи противника через которые осуществляются ИТВ;
- мировое инфокоммуникационное пространство не принадлежит ни одной из сторон, однако, вместе с тем, играет важную роль разделяемого ресурса, необходимого каждой стороне для эффективного ведения информационного противоборства. В связи с этим каждая из сторон будет проводить мероприятия по реализации обеспечивающих ИТВ с целью скрытного «захвата» имеющихся в инфокоммуникационном пространстве ресурсов. Под захватом понимается внедрение в ресурс, вирусов, закладок, либо некоторое другое ИТВ, которое позволит использовать данный информационный ресурс во время начала активной фазы информационного противоборства в интересах захватившей его стороны, причем, как правило, скрытно для владельца данного ресурса;
- широкое распространение в мировом инфокоммуникационном пространстве технических средств, производящихся какой-либо одной стороной, фактически, ведет к получению этой стороной подавляющего преимущества, т.к. при равенстве боевых потенциалов в традиционных сферах войны, эта сторона может получать неограниченные возможности в инфокоммуникационном пространстве за счет подыгрыша ей со стороны произведенных ею технических средств связи и обработки информации.

Вышеуказанные факторы составляют новизну модели техносферной войны [193-195, 210-212]. При этом такие факторы как рассмотрение мирового единого инфокоммуникационном пространства и борьба сторон за ее ресурсы, как одного из важнейших составляющих войны в современных условиях, а также преимущества, получаемые стороной производителем инфокоммуникационных средств, – ранее не встречались в других работах и являются важными направлениями развития теории информационных конфликтов.

4.8.4. Модель информационного конфликта с учетом многоуровневого построения системы связи

В большинстве работ по информационному конфликту рассмотрение процесса противоборства сторон ведется, как правило, без учета воздействия отдельных деструктивных факторов на конкретные процессы в СС СН на различных уровнях ее функционирования в соответствии с моделью взаимодействия открытых систем Open Systems Interconnect (OSI). В известных работах отсутствуют системные исследования эффектов от преднамеренных деструктивных воздействий (средств физического поражения, средств РЭП, средств ФП ЭМИ и ИТВ) с учетом их отображения на процессы отдельных уровней модели OSI. Не учитывается влияние преднамеренных деструктивных воздействий на процессы маршрутизации информационных потоков в распределенных сетях, а также в сетях с динамически изменяемой топологией. Как правило, не рассматриваются вопросы обеспечения заданного качества обслуживания в распределенных сетях, находящихся под воздействием территориально-распределенной группировки средств дестабилизирующих воздействий.

Имеются отдельные работы в области анализа функционирования комплексов связи и управления как многоуровневых иерархических систем А.М. Чуднова [1], И.М. Гуревича [212-216], А.А. Вакуленко, В.И. Шевчука [217], Ю.И. Маевского [218], В.В. Поповского, А.В. Лемешко, О.Ю. Евсеевой [219]. Однако за исключением работ А.М. Чуднова [1] и Ю.И. Маевского [218], в этих работах не рассматриваются конфликтные ситуации, характерные для многоуровневого информационного конфликта.

В интересах устранения вышесказанных недостатков в работах А.В. Паршуткина [3, 4] представлено развитие модели «классического» информационного конфликта системы связи в направлении повышения «многоуровневости» конфликта и согласования его с эталонной моделью OSI (рис. 4.9).

В этой модели предлагается учесть специфику различных типов дестабилизирующих воздействий за счет декомпозиции информационного конфликта системы связи с соответствующими средствами на отдельные конфликтные ситуации на каждом из уровней эталонной модели OSI. Таким образом, предложенный в работах А.В. Паршуткина [3, 4] новый концептуальный подход к моделированию информационного конфликта с одной стороны органично развивает существующие работы в области многоуровневого информационного конфликта радиоэлектронных систем [5, 6, 204, 334], а с другой – формализует конфликтное взаимодействие в соответствии с уровнями эталонной модели OSI. Данная концептуальная модель, названная автором эталонной моделью взаимо-

действия конфликтующих систем CSI (Conflict System Interconnection Reference Model), формализует объекты и общие подходы к описанию локальных информационных конфликтов в системе связи на каждом из уровней модели OSI (рис. 4.9). В рамках модели CSI средствами наблюдения и вскрытия протоколов, используемых в системах связи, останутся «классические» средства радио- и компьютерной разведки, а средствами воздействия – как «традиционные» средства РЭП, так и новые виды ИТВ.

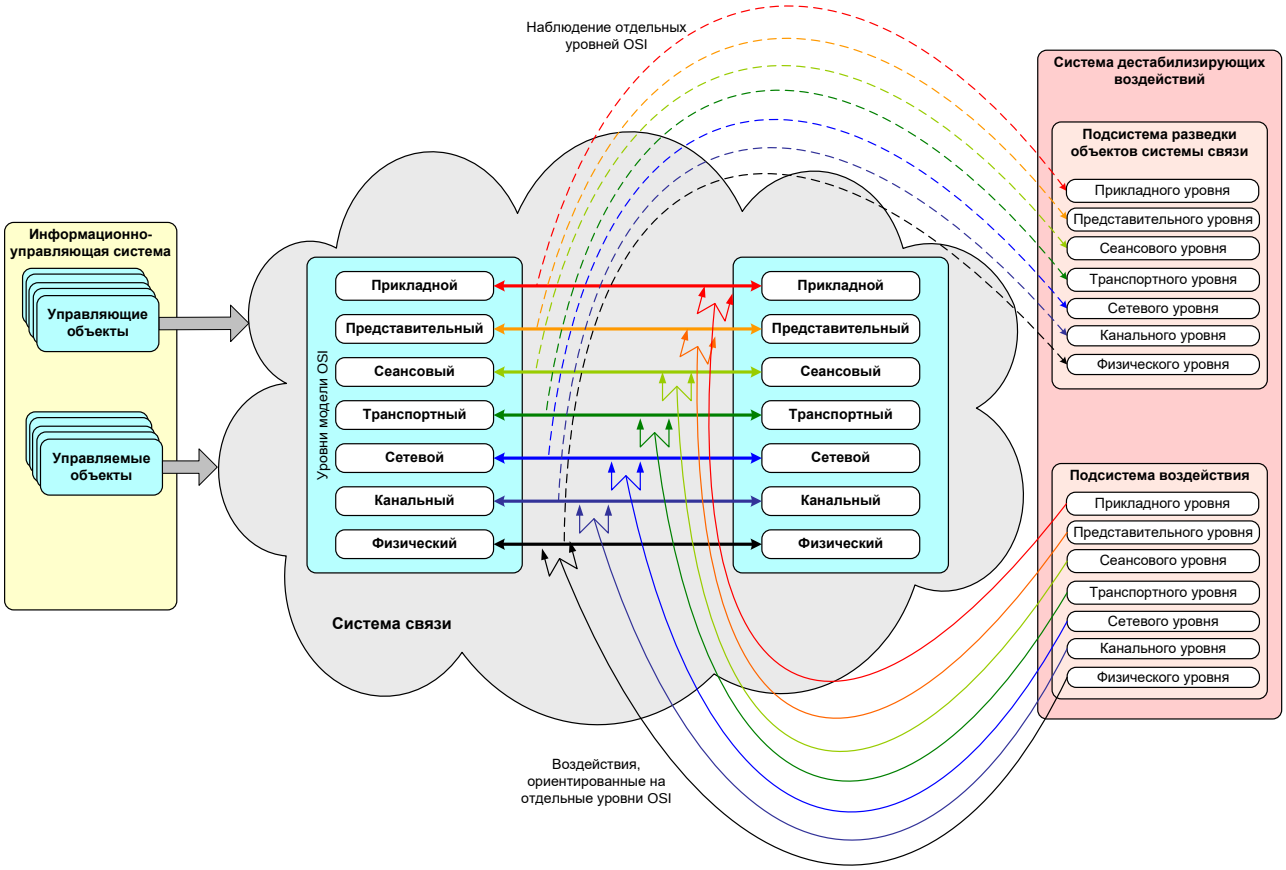

Рис. 4.9. Модель CSI [3, 4]

В дальнейшем, в следующей главе, в качестве конкретизации модели CSI представлена динамическая многоуровневая модель системы связи в условиях информационного конфликта.

Выводы по четвертой главе

Процесс конфликтного взаимодействия СС СН со средствами разведки и дестабилизирующих воздействий может быть формализован в виде концептуальной модели информационного конфликта (рис. 4.2). Данная модель описывает противоборство двух сторон, представленных соответствующими ОТС – нападающей ОТС (включающей в себя подсистему разведки, подсистему нападения и подсистему управления) и защищающейся ОТС (включающей в себя подсистему связи (непосредственно СС СН), подсистему управления и подсистему защиты).

Целью формирования концептуальной модели СС СН в условиях информационного конфликта является представление структурных схем, конфликтующих ОТС, в самом общем абстрактном варианте их формализации, анализ путей реализации стратегий разведки, нападения и защиты, а также направлений реализации угроз для каждой из сторон. При этом предполагается, что концептуальная модель послужит основой, в которой каждый рассмотренный процесс, стратегия или режим функционирования будет более подробно формализован в виде частных моделей в дальнейших исследованиях.

Развитие данной концептуальной модели предлагается вести за счет декомпозиции СС СН, на отдельные уровни в соответствии с моделью OSI и рассмотрения ее как сложной многоуровневой системы, находящейся в условиях информационного конфликта со средствами разведки и дестабилизирующих воздействий, а также конкретизации процессов функционирования отдельных протоколов СС СН. Данное развитие концептуальной модели представлено в следующей главе.

5. Динамическая многоуровневая модель системы связи в условиях дестабилизирующих воздействий и ведения разведки

5.1. Постановка задачи на моделирование

Развивая концептуальную модель СС СН, представленную в предыдущей главе, рассмотрим информационный конфликт СС СН, формализованный на основе теории динамических систем в терминологии работ [220-222] и представленный в виде динамической многоуровневой иерархической модели. При этом ее отдельные уровни соответствуют модели CSI, предложенной А.В. Паршуткиным [3, 4], а за концептуальную основу модели системы связи взята двухуровневая модель, представленная в работе [1]. В качестве более ранних работ, которые частично послужили прототипами общего подхода к моделированию иерархического динамического конфликта в системах связи, относятся работы П.А. Будко [22], К.Е. Легкова [36], И.М. Гуревича [212-216], А.А. Вакуленко, В.И. Шевчука [217], Ю.И. Маевского [218], В.В. Поповского, А.В. Лемешко, О.Ю. Евсеевой [219].

Для формализации модели введем следующие обозначения.

1) Элементы системы:

$|\cdot|$ – количество элементов в множестве $(\cdot)$;

a – алгоритм, как часть элемент математического обеспечения системы связи;

$A=\bigcup_{l} A_l$ – множество элементов алгоритмов, составляющих математическое обеспечение системы связи;

$A_l=\bigcup_{\Pi_l} A_{l,\pi}$ – множество алгоритмов, являющихся частью математического обеспечения, реализующих функционирование протоколов Π_l на l-ом уровне системы связи;

$A_{l,\pi}=\{a \mid a\in D(\pi_l)\}$ – множество алгоритмов, являющихся частью математического обеспечения, реализующих функционирование π-го протокола на l-ом уровне функционирования системы связи;

$D(\cdot)$ – область определения $(\cdot)$;

$E=\{e_i\}$ – множество средств связи, установленных на узлах сети связи;

$K=\{k_{ij}\}$ – множество каналов связи, соединяющих узлы связи (средства связи). Предполагается, что канал k_{ij} соединяет узлы z_i и z_j в случае, если средства связи e_i и e_j, размещенные на этих узлах, используют совместный протокол связи $\pi_{l.k}$;

$l=1\ldots7$ – номер уровня функционирования системы связи в соответствии с моделью OSI;

r – отдельный тип ресурса системы связи;

$R=\bigcup_{l} R_l$ – ресурс системы связи на всех уровнях ее функционирования;

$R_l = \bigcup_{\Pi_l} R_{l,\pi}$ – ресурс системы связи на l-ом уровне ее функционирования, используемый для функционирования протоколов Π_l и организации связи;

$R_{l,V} = \{r \mid r \in D(V_l),\ r \in R_l\}$ – ресурс на l-ом уровне функционирования системы связи, используемый системой дестабилизирующих воздействий для V_l-го воздействия на протоколы связи Π_l;

$R_{l,\pi} = \{r \mid r \in D(\pi_l)\}$ – ресурс системы связи на l-ом уровне ее функционирования, используемый для функционирования π-го протокола;

$S = \{t_0, t, \{S_l\}, X, U, A, \Theta, Z, E, K, \Lambda\}$ – множество состояний системы связи;

$S_{\text{conf}} = \{t, R, \Omega, A, \Theta, Z, K, \Lambda\}$ – конфигурация системы связи, определяющая ее текущую структуру и множество функциональных связей;

$S_{\text{conf}}^{\text{набл}} = \{t, R, \Omega, A, \Theta, Z, K, \Lambda\} \in M$ – конфигурация системы связи, наблюдаемая по каналу разведки со стороны системы дестабилизирующих воздействий;

$S_l = \{S_{l,\pi}\} \cup \Theta_l$ – множество состояний l-ого уровня функционирования системы связи, определяемое состояниями протоколов и связями между ними;

$S_{l,\pi} = \{s_\pi\}$ – множество состояний π_l-го протокола связи на l-ом уровне функционирования системы связи;

s_π – состояние π-го протокола связи;

$Z = \{z_i\}$ – множество узлов системы связи;

$\Theta = \{(\pi_{l1,i}, \pi_{l2,j})\},\ i, j = 1 \ldots |\Pi_l|,\ l_1, l_2, = 1 \ldots 7$ – множество функциональных связей между протоколами $\pi \in \Pi$ в системе связи на различных ее уровнях;

$\Theta_l = \{(\pi_{l,i}, \pi_{l,j})\},\ i, j = 1 \ldots |\Pi_l|$ – множество функциональных связей между протоколами $\pi_l \in \Pi_l$ на l-ом уровне системы связи;

$\Theta_{l,\pi} = \{(a_{l,,\pi,i}, a_{l,,\pi,j})\},\ i, j = 1 \ldots |A_{l,\pi}|$ – множество функциональных связей между алгоритмами $A_{l,\pi}$ в протоколе π_l на l-ом уровне системы связи;

Λ – информационная структура системы связи, определяющая маршруты циркуляции информационных потоков;

π – протокол связи;

π_l – протокол на l-ом уровне функционирования системы связи;

$\pi_{l,i}$ – i-ый протокол на l-ом уровне функционирования системы связи;

$\Pi = \bigcup_l \Pi_l$ – множество протоколов, используемых в системе связи на всех уровнях ее функционирования;

$\Pi_l = \bigcup_i \{\pi_{l,i}\}$ – множество протоколов, используемых в системе связи, на l-ом уровне ее функционирования;

ω – параметр алгоритма a;

$\Omega = \bigcup_l \Omega_l$ – множество параметров алгоритмов на всех уровнях системы связи;

$\Omega_l = \bigcup_{\Pi_l} \Omega_{l,\pi}$ – множество параметров алгоритмов протоколов Π_l на l-ом уровне системы связи;

$\Omega_{l,\pi} = \bigcup_\pi \Omega_{l,\pi,a}$ – множество параметров алгоритмов π-го протокола связи на l-ом уровне системы связи;

$\Omega_{l,\pi,a} = \{\omega \mid \omega \in D(a),\ a \in D(\pi_l)\}$ – множество параметров a-го алгоритма π-го протокола на l-ом уровне системы связи;

$\Pi_{l,v} = \bigcup_i \{\pi_{l,i} \mid V_l \in X_{l,\pi}\}$ – множество протоколов, используемых на l-ом уровне системы связи и подвергающихся преднамеренному дестабилизирующему воздействию V_l;

2) Параметры и показатели системы:

$\mathbb{E}(\cdot)$ – область значений $(\cdot)$;

k_u – индикатор устойчивости системы связи;

q – отдельный показатель качества QoS функционирования системы связи;

$Q = \bigcup_l Q_l$ – множество показателей QoS системы связи на всех ее уровнях;

$Q_l = \bigcup_{\Pi_l} Q_{l,\pi}$ – множество показателей QoS системы связи на l-ом уровне;

$Q_{l,M} = \bigcup_{\Pi_l} Q_{l,\pi,M}$ – множество показателей QoS системы связи на l-ом уровне, наблюдаемых системой дестабилизирующих воздействий по каналу разведки M_l;

$Q_{l,N} = \bigcup_{\Pi_l} Q_{l,\pi,N}$ – множество показателей QoS системы связи на l-ом уровне, наблюдаемых системой управления связи по каналу наблюдения N_l;

$Q_{l,\pi} = \{q \mid q \in \mathbb{E}(\pi_l)\}$ – множество показателей QoS системы связи на l-ом уровне, которые обеспечивает π_l-ый протокол связи;

$Q_{l,\pi,M} = \{q \mid q \in Q_{l,\pi},\ q \in M_{l,\pi}\}$ – множество показателей QoS системы связи на l-ом уровне, которые обеспечивает π_l-ый протокол связи, наблюдаемых системой дестабилизирующих воздействий по каналу разведки $M_{l,\pi}$;

$Q_{l,\pi,N} = \{q \mid q \in Q_{l,\pi},\ q \in N_{l,\pi}\}$ – множество показателей QoS системы связи на l-ом уровне, которые обеспечивает π_l-ый протокол связи, наблюдаемых системой управления связи по каналу наблюдения $N_{l,\pi}$;

$Q_{l,\pi,v} = \{q_{l,\pi} \mid q_{l,\pi} < q_{l,\pi}^{\text{треб}}\}$ – множество показателей QoS системы связи на l-ом уровне, которые обеспечивает π_l-ый протокол связи и которые снижаются в результате преднамеренных дестабилизирующих воздействий $V_{l,\pi}$;

$Q_M = \bigcup_l Q_{l,M}$ – множество показателей QoS системы связи на всех ее уровнях, наблюдаемых системой дестабилизирующих воздействий по каналу разведки M;

$Q_N = \bigcup_l Q_{l,N}$ – множество показателей QoS системы связи на всех ее уровнях, наблюдаемых системой управления связи по каналу наблюдения N;

t – время функционирования системы связи;

t_0 – начальный момент функционирования системы связи;

$t_{\text{набл}}$ – интервал времени наблюдения;

$t_{\text{тек}}$ – текущий момент функционирования системы связи;

T – множество моментов времени функционирования системы связи (непрерывных или дискретных);

T_U – множество моментов времени выдачи управляющих воздействий на элементы системы связи со стороны системы управления связью;

T_V – время, в течении которого осуществляются дестабилизирующие воздействия на элементы системы связи со стороны противника;

T_η – множество моментов времени наблюдения элементов системы связи со стороны системы управления связью;

3) Связи внутри системы:

η – параметр, наблюдаемый со стороны системы управления связью;

$N_{l,\pi}=\{\eta \mid \eta\in \mathbb{E}(\pi_l),\ \eta\in Q_{l,\pi}\times Y_{l,\pi}\}$ – канал наблюдения выходных параметров $Y_{l,\pi}$ и показателей QoS $Q_{l,\pi}$, которые обеспечиваются протоколом π_l на своем l-ом уровне системы связи со стороны системы управления связью;

$N_l=\bigcup\limits_{\Pi_l} N_{l,\pi}$ – канал наблюдения параметров Y_l и показателей QoS Q_l на l-ом уровне системы связи со стороны системы управления связью;

$N=\bigcup\limits_{l} N_l$ – канал наблюдения параметров Y и показателей QoS Q на всех уровнях системы связи со стороны системы управления связью;

μ – параметр, наблюдаемый по каналу разведки со стороны системы управления воздействиями противника;

$M_{l,\pi}=\{\mu \mid \mu\in \mathbb{E}(\pi_l),\ \mu\in Q_{l,\pi}\times Y_{l,\pi}\}$ – канал разведки выходных параметров $Y_{l,\pi}$ и показателей QoS $Q_{l,\pi}$, которые обеспечиваются протоколом π_l на своем l-ом уровне системы связи со стороны системы дестабилизирующих воздействий;

$M_l=\bigcup\limits_{\Pi_l} M_{l,\pi}$ – канал разведки параметров Y_l и показателей QoS Q_l на l-ом уровне системы связи со стороны системы дестабилизирующих воздействий;

$M=\bigcup\limits_{l} M_l$ – канал разведки параметров $\{Y_l\}$ и показателей QoS Q на всех уровнях системы связи со стороны системы дестабилизирующих воздействий;

v – отдельное воздействие со стороны системы дестабилизирующих воздействий;

$V_{l,\pi}=\{v \mid v\in D(\pi_l),\ v\in R_{l,\pi}\times\Omega_{l,\pi}\times A_{l,\pi}\times\Theta_{l,\pi}\}$ – множество воздействий со стороны системы дестабилизирующих воздействий на протокол π_l, функционирующий на l-ом уровне системы связи;

$V_l=\bigcup\limits_{\Pi_l} V_{l,\pi}$ – множество воздействий, осуществляемых на l-ый уровень системы связи со стороны системы дестабилизирующих воздействий;

$V=\bigcup\limits_{l} V_l$ – множество воздействий, осуществляемых на все уровни системы связи со стороны системы дестабилизирующих воздействий;

$\chi_{l,\pi}$ – множество параметров естественной среды функционирования системы связи (без преднамеренных дестабилизирующих воздействий), определяющие параметрическое пространство для протокола π_l на l-ом уровне;

$\chi_l=\bigcup\limits_{\Pi_l} \chi_{l,\pi}$ – множество параметров естественной среды функционирования системы связи, определяющие параметрическое пространство для протоколов Π_l на l-ом уровне;

$\chi=\bigcup\limits_{l} \chi_l$ – множество параметров естественной среды функционирования системы связи;

$X_{l,\pi} = \chi_{l,\pi} \times R_{l,\pi} \times V_{l,\pi}$ – множество параметров среды, определяющих параметрическое пространство для протокола π_l системы связи на l-ом уровне функционирования с учетом выделяемых протоколу на l-ом уровне ресурсов $R_{l,\pi}$, параметров естественной среды $\chi_{l,\pi}$ и множества $V_{l,\pi}$ преднамеренных дестабилизирующих воздействий на этот протокол;

$X_l = \bigcup_{\Pi_l} X_{l,\pi} = \chi_l \times R_l \times V_l$ – множество параметров среды, определяющих параметрическое пространство для протоколов системы связи Π_l на l-ом уровне функционирования, с учетом ресурсов l-ого уровня R_l, параметров естественной среды χ_l и множества V_l дестабилизирующих воздействий на этом уровне;

$X = \bigcup_{l} X_l = \chi \times R \times V$ – множество параметров среды, определяющих параметрическое пространство для системы связи на всех ее уровнях, с учетом ее ресурсов R, параметров естественной среды χ и всего множества дестабилизирующих воздействий V;

u – управляющее воздействие на элемент системы связи со стороны системы управления связью;

$u_{l,\pi}$ – управляющее воздействие на протокол π_l системы связи со стороны системы управления связью на l-ом уровне функционирования;

$U_{l,\pi} = u_{l,\pi} \times T$ – функционал, задающий множество управляющих воздействий (управление) на протокол π_l, со стороны системы управления связью на l-ом уровне с целью обеспечения протоколом требуемых показателей QoS $Q_{l,\pi}$;

$U_l = \bigcup_{\Pi_l} U_{l,\pi}$ – функционал, задающий множество управляющих воздействий (управление) на протоколы Π_l l-ого уровня со стороны системы управления связью на этом уровне с целью обеспечения требуемых показателей QoS Q_l;

$U = \bigcup_{l} U_l$ – функционал, задающий множество управляющих воздействий (управление) на протоколы Π всех уровней со стороны системы управления связью с целью обеспечения требуемых показателей QoS Q;

y – выходной параметр протокола системы связи;

$Y_{l,\pi} = \{y \mid y \in \mathbb{E}(\pi_l)\}$ – множество выходных параметров π_l-го протокола на l-ом уровне системы связи;

$Y_{l,\pi,N} = \{y \mid y \in Y_{l,\pi},\ y \in N_{l,\pi}\}$ – множество выходных параметров π_l-го протокола на l-ом уровне, наблюдаемых системой управления связью по каналу наблюдения $N_{l,\pi}$;

$Y_{l,\pi,M} = \{y \mid y \in Y_{l,\pi},\ y \in M_{l,\pi}\}$ – множество выходных параметров π_l-го протокола на l-ом уровне, наблюдаемых системой дестабилизирующих воздействий по каналу разведки $M_{l,\pi}$;

$Y_l = \bigcup_{\Pi_l} Y_{l,\pi}$ – множество выходных параметров l-го уровня системы связи;

$Y_{l,N} = \bigcup_{\Pi_l} Y_{l,\pi,N}$ – множество выходных параметров l-го уровня системы связи, наблюдаемых системой управления связи по каналу наблюдения N_l;

$Y_{l,M} = \bigcup_{\Pi_l} Y_{l,\pi,M}$ – множество выходных параметров l-го уровня системы связи, наблюдаемых системой дестабилизирующих воздействий по каналу разведки M_l;

$Y_N = \bigcup_l Y_{l,N}$ – множество выходных параметров всех уровней системы связи, наблюдаемых системой управления связи по каналу наблюдения N;

$Y_M = \bigcup_l Y_{l,M}$ – множество выходных параметров всех уровней системы связи, наблюдаемых системой дестабилизирующих воздействий по каналу разведки M;

$Y = \bigcup_l Y_l$ – множество выходных параметров системы связи;

Y_7 – конечные выходные параметры системы связи;

$\psi_{l,\pi}$ – отображение, задающее смену состояний $s_{l,\pi} \in S_{l,\pi}$ протокола π_l на l-ом уровне функционирования;

ψ_l – отображение, задающее смену состояний $s_l \in S_l$ l-го уровня системы связи;

ψ – отображение, задающее смену состояний $s \in S$ системы связи;

$f_{l,\pi}$ – отображение, определяющее выходные показатели качества обслуживания $Q_{l,\pi}$, которые обеспечивает протокол π_l на своем l-ом уровне функционирования;

f_l – отображение, определяющее выходные показатели качества обслуживания Q_l, которые обеспечивают множество протоколов Π_l на l-ом уровне функционирования;

f – отображение, определяющее выходные показатели качества обслуживания Q системы связи;

$\gamma_{l,\pi}$ – отображение, определяющее выходные параметры Y_π протокола π_l на l-ом уровне;

γ_l – отображение, определяющее выходные параметры Y_l множества протоколов Π_l на l-ом уровне;

γ – отображение, определяющее выходные параметры Y системы связи;

$\varphi_{l,\pi}$ – отображение, определяющее параметрическое множество среды функционирования протоколов более высокого уровня X_{l+1}, зависимое от протокола π_l на l-ом уровне;

φ_l – отображение, определяющее параметрическое множество среды функционирования X_{l+1} протоколов более высокого уровня Π_{l+1};

$\varphi = \bigcup_l \varphi_l$ – множество отображений, определяющих межиерархические связи между уровнями системы связи.

Целью моделирования является формализация информационного конфликта системы связи со средствами разведки и дестабилизирующих воздействий как для отдельных протоколов на конкретных уровнях модели OSI, так и для системы связи в целом, путем ее представления в виде динамической многоуровневой иерархической модели.

5.2. Динамическая модель протокола системы связи

В отличие от известных моделей, представленных в работах [1, 2], в данной модели в качестве основного элемента системы связи выбран протокол связи π как ее функционально-простейший элемент.

При этом под *протоколом* понимается формализованный набор правил, задаваемых алгоритмами его функционирования, а также их параметрами, ко-

торые позволяют осуществлять соединение и обмен данными между двумя или более функциональными элементами системы связи. Функционально протоколы классифицируются в соответствии с уровнями модели OSI. При этом протоколы, как правило, физического уровня реализуются аппаратно, протоколы канального и сетевого уровня – аппаратно-программными средствами, а протоколы транспортного уровня и выше – программно.

Рассмотрим общую динамическую модель протокола (рис. 5.1), построенную на основе теории систем [220-222].

5.2.1. Схема модели

В общем случае модель протокола π_l в виде динамической системы (рис. 5.1) описывается следующими параметрами и отображениями.

1) Входные параметры:

- множество обобщенных параметров среды $X_{l,\pi} = R_{l,\pi} \times \chi_{l,\pi} \times V_{l,\pi}$, в которой функционирует протокол π_l на l-ом уровне, включающие в себя:
  - множество параметров естественной среды l-го уровня $\chi_{l,\pi}$, значимые для протокола π_l (при этом $\chi_{l,\pi} \subseteq \chi_l \subseteq \chi$);
  - множество ресурсов связи l-го уровня $R_{l,\pi}$, используемых протоколом π_l (при этом $R_{l,\pi} \subseteq R_l \subseteq R$);
  - множество преднамеренных воздействий $V_{l,\pi}$ реализуемых системой дестабилизирующих воздействий на l-ом уровне и влияющих на функционирование протокола π_l ($V_{l,\pi} \subseteq V_l \subseteq V$);
- множество управляющих воздействий $U_{l,\pi} = u_{l,\pi} \times T$ ($U_{l,\pi} \subseteq U_l \subseteq U$) на протокол π_l, со стороны системы управления связью на l-ом уровне, заключающиеся в рациональном распределении ресурсов l-го уровня ($u_{l,\pi}: R_l \rightarrow \{R_{l,\pi}\}$) и в управлении параметрами $\Omega_{l,\pi}$ функционирования протокола π_l с целью обеспечения требуемого качества обслуживания:

  $$u_{l,\pi}: \Omega_{l,\pi,a} \rightarrow Q_{l,\pi} \mid \{q_{l,\pi} \geq q_{l,\pi}^{\text{треб}}\} \in Q_{l,\pi};$$
- множество моментов времени функционирования системы связи T.

2) Внутренние параметры протокола π_l на l-ом уровне:

- множество алгоритмов $A_{l,\pi}$, реализующих функционал протокола π_l и связанных между собой в соответствии со структурой $\Theta_{l,\pi}$:

  $$A_{l,\pi} = \{a \mid a \in D(\pi_l)\};$$

  $$\pi_l = A_{l,\pi} \cup \Theta_{l,\pi}; \qquad (5.1)$$
- множество параметров $\Omega_{l,\pi,a}$ алгоритмов $A_{l,\pi}$, реализующих функционал протокола π_l:

  $$\Omega_{l,\pi,a} = \{\omega \mid \omega \in D(a),\ a \in D(\pi_l)\}; \qquad (5.2)$$

3) Отображения, определяющие общую динамическую модель протокола π_l на l-ом уровне:

- отображение $\psi_{l,\pi}$, задающее смену состояний s_π ($s_\pi \in S_{l,\pi}$) протокола π_l:

  $$s_\pi = \psi_{l,\pi}(t_0,\ t,\ s_\pi(t_0),\ S_{l,\pi},\ X_{l,\pi},\ U_{l,\pi},\ A_{l,\pi})\ ; \qquad (5.3)$$

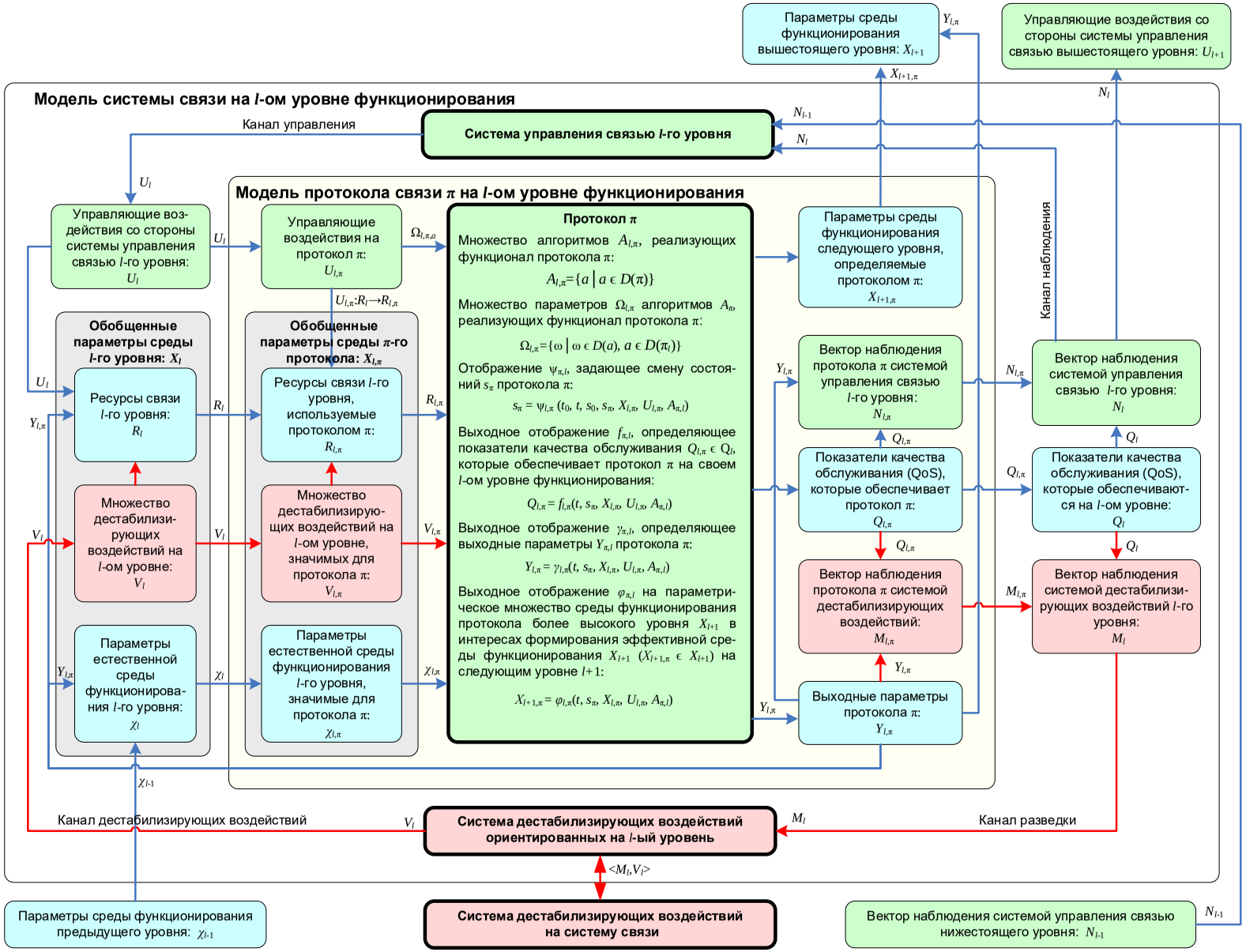

Рис. 5.1. Динамическая модель отдельного протокола системы связи

- отображение $f_{l,\pi}$, определяющее выходные показатели качества обслуживания $Q_{l,\pi} \in Q_l$,, которые обеспечивает протокол π_l на l-ом уровне функционирования:

$$Q_{l,\pi} = f_{l,\pi}(t, s_\pi, X_{l,\pi}, U_{l,\pi}, A_{l,\pi}); \quad (5.4)$$

- отображение $\gamma_{l,\pi}$, определяющее выходные параметры $Y_{l,\pi}$ протокола π_l:

$$Y_{l,\pi} = \gamma_{l,\pi}(t, s_\pi, X_{l,\pi}, U_{l,\pi}, A_{l,\pi}); \quad (5.5)$$

- отображение $\varphi_{l,\pi}$, определяющее параметрическое множество среды функционирования протоколов более высокого уровня X_{l+1}:

$$X_{l+1,\pi} = \varphi_{l,\pi}(t, s_\pi, X_{l,\pi}, U_{l,\pi}, A_{l,\pi}). \quad (5.6)$$

4) Выходные параметры:

- множество выходных параметров $Y_{l,\pi}$ протокола π_l;
- множество показателей качества обслуживания $Q_{l,\pi} \in Q_l$, которые обеспечивает протокол π_l на l-ом уровне функционирования;
- множество параметров среды функционирования протоколов более высокого уровня $X_{l+1,\pi}$ ($X_{l+1,\pi} \subseteq X_{l+1}$). Фактически данный выходной параметр определяет возможности протокола текущего уровня по исправлению ошибок и негативных воздействий входного параметра предыдущего уровня (например, система радиоэлектронной защиты на 1-ом (физическом) уровне OSI при приеме сигналов X_1 осуществляет фильтрацию помех и преобразовывает сигналы в двоичный код X_2, а далее на 2-ом (канальном) уровне OSI битовый поток X_2 объединяется в блоки, в которых на основе схемы помехоустойчивого кодирования исправляются ошибки, и исправленный блок передается на 3-ий (сетевой) уровень OSI X_3 и т.д.).
- канал наблюдения $N_{l,\pi}$ выходных параметров $Y_{l,\pi}$ и показателей QoS $Q_{l,\pi}$, которые обеспечиваются протоколом π_l на l-ом уровне системы связи со стороны системы управления связью:

  $N_{l,\pi}=\{\eta \mid \eta \in \mathbb{E}(\pi_l), \eta \in Q_{l,\pi} \times Y_{l,\pi}\}$, где $\mathbb{E}(\cdot)$ – область значений $(\cdot)$;
- канал разведки $M_{l,\pi}$, по которому системой дестабилизирующих воздействий наблюдаются выходные параметры $Y_{l,\pi}$ и показатели QoS $Q_{l,\pi}$, которые обеспечиваются протоколом π_l на l-ом уровне системы связи. с целью обоснованного принятия решений по применению воздействий $V_{l,\pi}$:

  $M_{l,\pi}=\{\mu \mid \mu \in \mathbb{E}(\pi_l), \mu \in Q_{l,\pi} \times Y_{l,\pi}\}$.

Параметры $R_{l,\pi}$, $V_{l,\pi}$, $U_{l,\pi}$ представляют собой конечномерные векторные функции от времени t, $t \in T$. Множество параметров естественной среды $\chi_{l,\pi}$ может быть как функциями от времени t (например, медленные или быстрые замирания при распространении радиосигналов коротких волн, зависящие от времени суток или сезона), так и случайными параметрами, как правило, с нормальным или экспоненциальным распределением.

Таким образом, модель протокола π_l представляет собой конечномерную динамическую систему, определенную на параметрическом пространстве $R_{l,\pi} \times \chi_{l,\pi} \times V_{l,\pi} \times U_{l,\pi} \times T$ и заданную отображениями $\psi_{l,\pi}$, $f_{l,\pi}$, $\gamma_{l,\pi}$, $\varphi_{l,\pi}$. Далее рассмотрим отдельные аспекты формализации функционирования протокола более подробно.

5.2.2. Формализация процесса функционирования протокола

Процесс функционирования протокола π_l определяется отображением $\gamma_{l,\pi}$:$\{t, s_\pi, X_{l,\pi}, U_{l,\pi}, A_{l,\pi}\} \rightarrow Y_{l,\pi}$ задаваемым выражением (5.5), в процессе которого производится выработка множества выходных параметров $Y_{l,\pi}$, которые соответствуют целевому назначению протокола π_l, в зависимости от его текущего состояния s_π и входных воздействий $\{X_{l,\pi}, U_{l,\pi}\}$.

Выполнение функций по целевому назначению протокола π_l ведется по заложенному в него множеству алгоритмов $A_{l,\pi}=\{a \mid a \in D(\pi_l)\}$, взаимоувязанных в единую систему в соответствии со структурой связей $\Theta_{l,\pi}$. Функционирование алгоритмов $A_{l,\pi}$, в свою очередь, зависит от их собственных параметров $\Omega_{l,\pi,a}=\{\omega \mid \omega \in D(a), a \in D(\pi_l)\}$ и параметров среды $X_{l,\pi} = R_{l,\pi} \times \chi_{l,\pi} \times V_{l,\pi}$. Для выполнения целевых задач протоколу π_l выделяются ресурсы $R_{l,\pi}$. Контроль качества функционирования ведется по значениям показателей QoS $\{q_{l,\pi}\} \in Q_{l,\pi}$, которые обеспечивает этот протокол.

Оценкой качества функционирования протокола π_l является множество показателей QoS $Q_{l,\pi}$, которые определяются в соответствии с выражением (4). В интересах обеспечения заданного уровня показателей QoS $\{q_{l,\pi}^{\text{треб}}\}$, на протокол π_l со стороны системы управления связью оказывается множество управляющих воздействий $U_{l,\pi}$, которые, как правило, связаны или с распределением ресурсов $R_{l,\pi}$, доступных протоколу π_l, или с изменением параметров $\Omega_{l,\pi,a}$ алгоритмов $A_{l,\pi}$.

Например, протокол детектирования и помехоустойчивого приема сигналов может обеспечивать в качестве множества $Y_{l,\pi}$ следующие сигнальные параметры: вероятность правильного обнаружения сигнала, мощность сигнала, вид модуляции, цифровая последовательность, соответствующая принятому сигналу и т.д. Для этого протокола, под множеством $A_{l,\pi}$ можно рассматривать алгоритм обнаружения сигнала, а также алгоритмы когерентного и некогерентного приема, а под множеством параметров $\Omega_{l,\pi,a}$ алгоритмов $A_{l,\pi}$ – критерий обнаружения и пороговое значение для него, время накопления сигнала, пороговое значение автокорреляционной функции и др. В качестве ресурса $R_{l,\pi}$ можно рассматривать частотно-временную область, в которой ведется прием сигналов. В качестве параметров естественной среды $\chi_{l,\pi}$ – значение отношения мощности сигнала к мощности шума (ОСШ) на входе приемника в условиях отсутствия помех и энергетически-временные параметры принимаемого сигнала. В качестве дестабилизирующего воздействия $V_{l,\pi}$ – воздействие средств РЭП, снижающее значение ОСШ и, как следствие, понижающее показатели QoS $Q_{l,\pi}$ протокола приема. В качестве элементов множества показателей QoS $Q_{l,\pi}$ могут выступать вероятность правильного обнаружения сигнала, вероятность ошибочного приема сигнала, вероятность ошибки на бит, пропускная способность канала и др.

5.2.3. Формализация критерия эффективного функционирования протокола

Качество функционирования протокола определяется соответствием всех показателей QoS из множества $Q_{l,\pi}$ критерию эффективности (5.7).

Протокол является эффективно функционирующим в случае, если все его показатели качества $\forall\{q_{l,\pi}\}\in Q_{l,\pi}$, которые он обеспечивает, имеют значения не ниже требуемого, то есть выполняется критерий:

$$\forall\{q_{l,\pi}\geq q_{l,\pi}^{\text{треб}}\}\in Q_{l,\pi}. \qquad (5.7)$$

Функционирование протокола π_l, как правило, сопровождается динамическим или стохастическим изменением значений параметров среды функционирования $X_{l,\pi}=R_{l,\pi}\times\chi_{l,\pi}\times V_{l,\pi}$, которые в условиях конфликта, в первую очередь, определяются множеством дестабилизирующих воздействий $V_{l,\pi}$.

Условимся называть множество входных параметров $X_{l,\pi}\times U_{l,\pi}$ *эффективным*, если оно позволяет обеспечить выполнение критерия эффективного функционирования протокола (5.7) и *неэффективным* – если не позволяет (рис. 5.2).

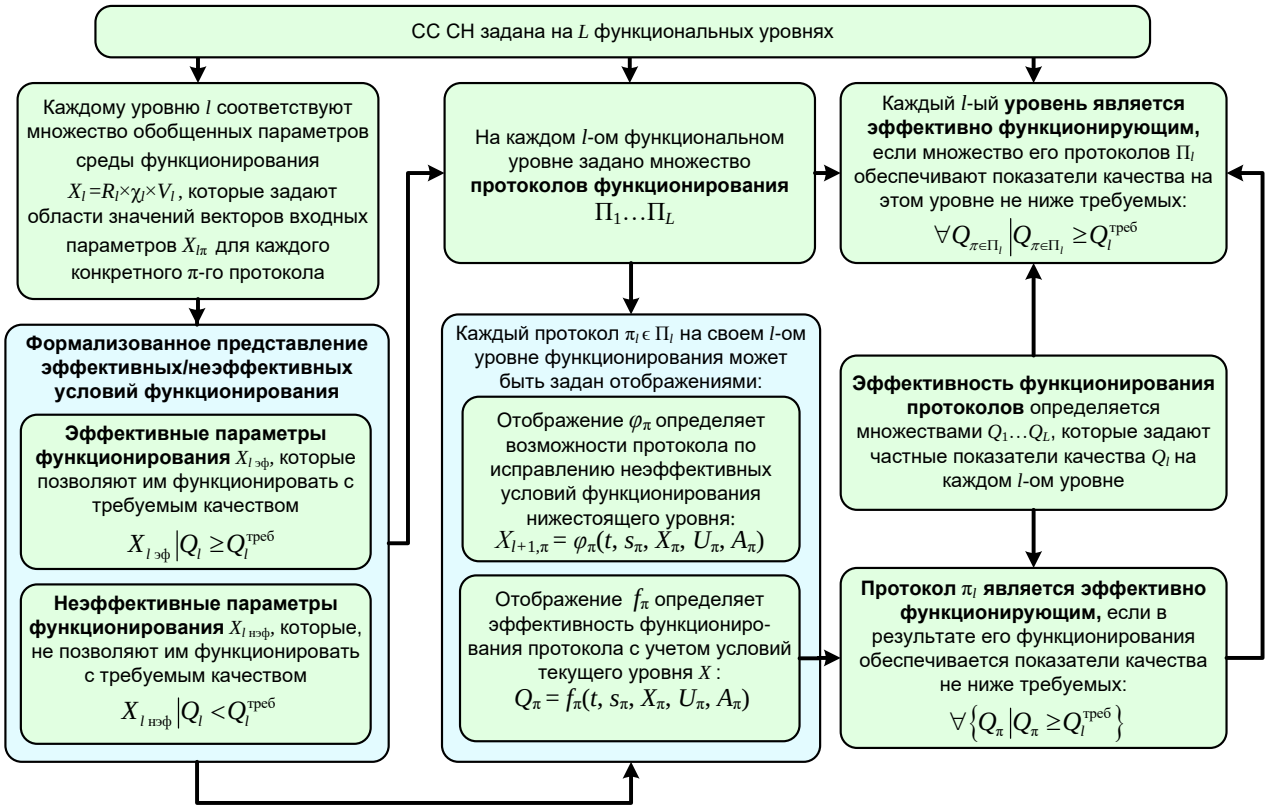

Рис. 5.2. Схема, поясняющая понятие эффективности протокола связи

Для обеспечения выполнения критерия (5.7) на протокол π_l со стороны системы управления связью оказывается множество управляющих воздействий $U_{l,\pi}$, которые, как правило, связаны или с распределением ресурсов $R_{l,\pi}$, доступных протоколу π_l, или с изменением параметров $\Omega_{l,\pi}$ алгоритмов $A_{l,\pi}$, на основе которых функционирует протокол.

Разные протоколы могут обеспечивать один и тот же показатель качества ($q_{l,\pi1}\cap q_{l,\pi2}\neq\varnothing$). Более того, как правило, в системе связи на одном уровне функ-

ционирования могут организовываться каскадные схемы протоколов, нацеленные на последовательное улучшение одного и того же показателя качества.

В качестве такого примера может выступать показатель качества – достоверность приема сигнала, для обеспечения которого последовательно применяются протокол приема антенной системы, протокол помехоустойчивого приема и протокол фильтрации помех (рис. 5.3):

$f_{\pi 1}$: $\{t, s_\pi, X_{l,\pi 1}, U_{l,\pi 1}, A_{\pi 1}\} \rightarrow q_{l,дост1}$, $q_{l,дост1} \in q_{l,\pi 1} \subseteq Q_l$,
$\gamma_{\pi 1}$: $\{t, s_\pi, X_{l,\pi 1}, U_{l,\pi 1}, A_{\pi 1}\} \rightarrow Y_{l,\pi 1}$;

$f_{\pi 2}$: $\{t, s_\pi, Y_{l,\pi 1}, U_{l,\pi 2}, A_{\pi 2}\} \rightarrow q_{l,дост2}$, $q_{l,дост2} \in q_{l,\pi 2} \subseteq Q_l$,
при этом $q_{l,дост2} > q_{l,дост1}$,
$\gamma_{\pi 2}$: $\{t, s_\pi, Y_{l,\pi 1}, U_{l,\pi 2}, A_{\pi 2}\} \rightarrow Y_{l,\pi 2}$;

$f_{\pi 3}$: $\{t, s_\pi, Y_{l,\pi 2}, U_{l,\pi 3}, A_{\pi 3}\} \rightarrow q_{l,дост3}$, $q_{l,дост3} \in q_{l,\pi 3} \subseteq Q_l$,
при этом $q_{l,дост3} > q_{l,дост2}$,
$\gamma_{\pi 3}$: $\{t, s_\pi, Y_{l,\pi 2}, U_{l,\pi 3}, A_{\pi 3}\} \rightarrow Y_{l,\pi 3}$.

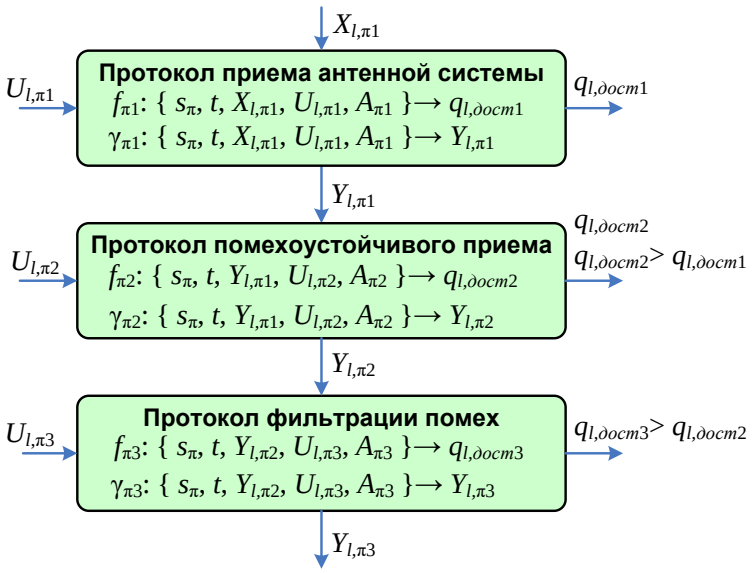

Рис. 5.3. Пример каскадной схемы протоколов, функционирующих на одном уровне

5.2.4. Формализация канала наблюдения протокола со стороны системы управления связью

Канал наблюдения $N_{l,\pi}$ протокола π_l со стороны системы управления связью обеспечивает сбор сведений о состоянии протокола s_π за счет наблюдений $\eta_{l,\pi}$ всех или части выходных параметров $Y_{l,\pi}$ и показателей QoS $Q_{l,\pi}$, которые обеспечиваются протоколом π_l. Целью наблюдения $\eta_{l,\pi}$ является определение состояния s_π протокола π_l и принятие решений о выработке управляющих воздействий $U_{l,\pi}$ на протокол. С учетом этого, наблюдение $N_{l,\pi}$ представляется вектором, составляющие которого являются соответственно наблюдениями эле-

ментов множеств $Y_{l,\pi}$ и $Q_{l,\pi}$. Данные компоненты образуют множество наблюдаемых параметров:

$$N_{l,\pi} = Y_{l,\pi,N} \times Q_{l,\pi,N}, \qquad (5.8)$$

где $Y_{l,\pi,N} \subseteq Y_{l,\pi}$ и $Q_{l,\pi,N} \subseteq Q_{l,\pi}$ – компоненты множеств $Y_{l,\pi}$ и $Q_{l,\pi}$, наблюдаемые системой управления связью.

Определение текущего состояния протокола s_π в условиях параметрического сужения $s_\pi \to \{\{q_{l,\pi}\},\{y_{l,\pi}\}\} \to \{\{q_{l,\pi,N}\},\{y_{l,\pi,N}\}\} \to N_{l,\pi}$, и сужения реакции, связанные с ограничением на время наблюдения $0 \le T \le t_{набл}$, в выражении (5.8), является предметом приложения теории наблюдения динамических систем [220-222] к исследованию систем управления связью и рассмотрено в работе [1]. Как показано в этой работе, основными особенностями наблюдения протоколов в системе связи являются:

- дискретность процесса наблюдения: $T_\eta = \{t_1, t_2, \ldots, t_n, \ldots\}$ в течении времени $t_{набл}$;
- временные задержки процессов сбора сведений о значениях компонент множеств $Y_{l,\pi,N}$ и $Q_{l,\pi,N}$;
- потери сведений об отдельных наблюдениях $\eta_{l,\pi} \in N_{l,\pi}$ в процессе передачи по сети связи;
- ситуации нарушения порядка следования результатов наблюдения (в сети связи возможны ситуации, когда информация более позднего наблюдения $\eta_{l,\pi}(t_2)$ поступает раньше, чем информация предыдущего наблюдения $\eta_{l,\pi}(t_1)$, $t_2 > t_1$);
- наблюдение группы протоколов Π_l^* l-го уровня по их общим показателям качества Q_l^* и выходным параметрам Y_l^*, являющихся общими для всей группы:

$$\begin{cases} \Pi_l^* = \bigcup\left(\pi_l \left| \left(\bigcap\limits_{\Pi_l} Q_{l,\pi} = Q_l^* \neq \varnothing\right) \wedge \left(\bigcap\limits_{\Pi_l} Y_{l,\pi} = Y_l^* \neq \varnothing\right)\right.\right); \\ N_{l,\Pi_l^*} = Q_l^* \times Y_l^* = \left(\bigcap\limits_{\forall \pi_l \in \Pi_l^*} q_{l,\pi}\right) \bigcup \left(\bigcap\limits_{\forall \pi_l \in \Pi_l^*} Y_{l,\pi}\right), \end{cases}$$

  что существенно затрудняет идентификацию состояния s_π каждого из протоколов π_l, входящих в группу Π_l^*;
- наличие преднамеренных дестабилизирующих воздействий $V_{l,\pi}$, связанных с нарушением функционирования канала наблюдения ($N_{l,\pi}=0$) или подменой сведений о наблюдаемых показателях, входящих в множества $Y_{l,\pi,N}$ и $Q_{l,\pi,N}$.

С учетом данных особенностей, наблюдение $N_{l,\pi}$ протокола π_l можно отнести к одному из двух видов наблюдения [221]:

1) *наблюдаемость по направлению*, связанная с оценкой изменения показателей, входящих в множества $Y_{l,\pi,N}$ и $Q_{l,\pi,N}$, во времени:

$$\left[\begin{array}{l} \eta_{l,\pi} = \dfrac{d\left\{q_{l,\pi,N}\right\}}{dt}; \\ \eta_{l,\pi} = \dfrac{d\left\{y_{l,\pi,N}\right\}}{dt}, \end{array}\right.$$

где $\eta_{l,\pi} \in N_{l,\pi}$;

2) *локальная наблюдаемость*, связанная с фиксацией события $\eta_{l,\pi} \in N_{l,\pi}$, состоящего в изменении значения одного или нескольких наблюдаемых показателей $q_{l,\pi,N} \in N_{l,\pi}$ или $y_{l,\pi,N} \in N_{l,\pi}$ ниже некоторых граничных значений $q_l^{\text{треб}}$, $y_{l,\pi}^{\text{треб}}$:

$$\eta_{l,\pi} = \begin{cases} q^*_{l,\pi,\eta}, \text{ если } \exists\left\{q^*_{l,\pi,\eta} \middle| q^*_{l,\pi,\eta} < q_{l,\pi}^{\text{треб}}\right\} \in Q_{l,\pi,N}; \\ y^*_{l,\pi,\eta}, \text{ если } \exists\left\{y^*_{l,\pi,\eta} \middle| y^*_{l,\pi,\eta} < y_{l,\pi}^{\text{треб}}\right\} \in Y_{l,\pi,N}; \\ 0, \text{ если } \forall\left(\left\{q_{l,\pi,\eta} \middle| q_{l,\pi,\eta} \geq q_{l,\pi}^{\text{треб}}\right\} \in Q_{l,\pi,N}\right) \wedge \left(\left\{y_{l,\pi,\eta} \middle| y_{l,\pi,\eta} \geq y_{l,\pi}^{\text{треб}}\right\} \in Y_{l,\pi,N}\right). \end{cases}$$

5.2.5. Формализация канала управления протоколом со стороны системы управления связью

Опишем канал $U_{l,\pi}$ управления протоколом π_l со стороны системы управления связью. По наблюдению $N_{l,\pi}$, система управления связью вырабатывает множество управляющих воздействий $U_{l,\pi}$, которые по каналу управления воздействуют на протокол π_l. С учетом конечности множества состояний S_π и последовательности моментов $T_U=\{t_1, t_2, \ldots, t_n, \ldots\}$ принятия решений по выдаче управляющих воздействий $U_{l,\pi}=\{U_{l,\pi}(t_1), U_{l,\pi}(t_2), \ldots, U_{l,\pi}(t_n), \ldots\}$ такое управление $U_{l,\pi}$ можно назвать *программой управления*. Программа управления при любом начальном состоянии протокола $s_\pi(t_0)$ и наличии преднамеренных дестабилизирующих воздействий $V_{l,\pi}$ должна обеспечивать выполнение критерия (5.7), т.е. существование предела (в первом уравнении системы)

$$\begin{cases} Q_{l,\pi} = \lim\limits_{\substack{t\to\infty \\ U_{l,\pi}(t)}} f_{l,\pi}\left(t,\ s_\pi,\ X_{l,\pi},\ U_{l,\pi},\ A_{l,\pi}\right); \\ \forall\left\{q_{l,\pi} \geq q_{l,\pi}^{\text{треб}}\right\} \in Q_{l,\pi}; \\ X_{l,\pi} = R_{l,\pi} \times \chi_{l,\pi} \times V_{l,\pi}; \\ U_{l,\pi} = u_{l,\pi} \times T_U. \end{cases}$$

Необходимо отметить, что ввиду особенностей наблюдения $N_{l,\pi}$, изложенных выше, в контуре управления всегда присутствует неопределенность в определении текущего состояния протокола s_π. Еще одной чертой, характерной для протокола π_l, как для динамической системы, является наличие множества дестабилизирующих воздействий $V_{l,\pi}$. Эти аспекты позволяют отнести задачу разработки программы управления системой связи к задачам синтеза адаптивной робастной системы управления.

Наличие программы управления $U_{l,\pi}$ должно предусматривать план управления $U_{l,\pi}^{\text{план}}=\{U_{l,\pi}(t_{\text{тек}+1}), U_{l,\pi}(t_{\text{тек}+2}), \ldots, U_{l,\pi}(t_{\text{тек}+n}), \ldots\}$ по обеспечению достижения выполнения критерия

$$\forall\ \{q_{l,\pi} \geq q_{l,\pi}^{\text{треб}}\} \in Q_{l,\pi},$$

за счетное число шагов n в будущие моменты времени $t_{\text{тек}+n}$. На план управления накладываются ограничения, что управление $U_{l,\pi}^{\text{план}}$ должно переводить протокол π_l в состояние s_π, которое является допустимым для этого протокола:

$$\begin{cases} s_\pi \in S_{l,\pi}; \\ s_\pi = \psi_{l,\pi}\left(t_0,\ t_{\text{тек}+n},\ s_\pi(t_0),\ S_{l,\pi}, X_{l,\pi},\ U_{l,\pi}^{\text{план}},\ A_{l,\pi}\right); \\ X_{l,\pi} = R_{l,\pi} \times \chi_{l,\pi} \times V_{l,\pi}; \\ U_{l,\pi}^{\text{план}} = u_{l,\pi} \times T_U. \end{cases}$$

План управления должен предусматривать формирование управляющих воздействий $U_{l,\pi}^{\text{план}}$ в зависимости от текущего наблюдения $N_{l,\pi}(t_{\text{тек}})$ и подчиняться определенной стратегии управления, связанной с реализацией цели управления $\forall\ \{q_{l,\pi} \geq q_{l,\pi}^{\text{треб}}\} \in Q_{l,\pi}$.

Как правило, для системы связи можно рассмотреть две основные стратегии управления при допущении о том, что принятие решения по выработке управления $U_{l,\pi}^{\text{план}}(t_{\text{тек}+1})$ осуществляется на каждом шаге независимо от предыдущих управлений и основано на результатах текущего наблюдения $N_{l,\pi}(t_{\text{тек}})$ [1]:

1) *вероятностная стратегия*, когда в условиях текущего наблюдения $N_{l,\pi}(t_{\text{тек}})$ в следующий момент времени осуществляется выбор такого управляющего воздействия $U_{l,\pi}^{\text{план}}(t_{\text{тек}+1})$ из имеющегося множества альтернатив $\{U_{l,\pi}(t_{\text{тек}+1})\}$, которое с наибольшей вероятностью ведет к выполнению выбранного критерия эффективности $q_{l,\pi} \geq q_{l,\pi}^{\text{треб}}$ ($q_{l,\pi} \in Q_{l,\pi}$):

$$U_{l,\pi}^{\text{план}} :< \frac{\left\{U_{l,\pi}^{\text{план}}\left(t_{\text{тек}+1}\right)\right\}}{N_{l,\pi}\left(t_{\text{тек}}\right)} > \to U_{l,\pi}\left(t_{\text{тек}+1}\right) \Big| P\left(q_{l,\pi}(t_{\text{тек}+1}) \geq q_{l,\pi}^{\text{треб}}\right) \to \max; \qquad (5.9)$$

2) *стратегия максимального приближения*, когда в условиях текущего наблюдения $N_{l,\pi}(t_{\text{тек}})$ осуществляется выбор такого управляющего воздействия $U_{l,\pi}^{\text{план}}(t_{\text{тек}+1})$, которое минимизирует отклонение выбранного показателя $q_{l,\pi}$ ($q_{l,\pi} \in Q_{l,\pi}$) от его требуемого значения $q_{l,\pi}^{\text{треб}}$:

$$U_{l,\pi}^{\text{план}} :< \frac{\left\{U_{l,\pi}^{\text{план}}\left(t_{\text{тек}+1}\right)\right\}}{N_{l,\pi}\left(t_{\text{тек}}\right)} > \to U_{l,\pi}\left(t_{\text{тек}+1}\right) \Big| \left(q_{l,\pi}(t_{\text{тек}+1}) - q_{l,\pi}^{\text{треб}}\right) \to \min. \qquad (5.10)$$

План управления при вероятностной стратегии может быть формализован на основе теории марковских и полумарковских процессов, а задача управления протоколом π_l может быть сведена к оптимизации семейства вероятностей вида (5.9). План управления при стратегии максимального приближения может быть формализован на основе теории адаптивного управления, при этом задача управления протоколом π_l может быть сведена к оптимизации траектории воздействий, минимизирующих последовательность шагов, на каждом из которых реализуется управление (5.10).

Конкретизация плана управления $U_{l,\pi}^{\text{план}}$ может состоять в выделении отдельных объектов управления для протокола π_l, управление которыми планируется на очередном шаге $t_{\text{тек}+1}$. В зависимости от объекта управления по отношению к произвольному протоколу l-го уровня можно выделить:

1) самонастраивающиеся управление:

- управление ресурсами $R_{l,\pi}$, выделяемыми протоколу π_l из общего пула ресурсов l-го уровня:
  $U_{l,\pi}: R_l \to \{R_{l,\pi}\}$;
- управление параметрами $\Omega_{l,\pi,a}$ отдельных алгоритмов $a \in A_{l,\pi}$:
  $U_{l,\pi}: \{\Omega_{l,\pi}\} \to \arg A_{l,\pi}$.

2) самоорганизующиеся управление:

- управление алгоритмами $A_{l,\pi}$, используемыми протоколом π_l из совокупности математического обеспечения $\{A_{l,\pi}\}$, и последовательностью их выполнения $\Theta_{l,\pi}$:

  $U_{l,\pi}$:$\{\{A_{l,\pi}\}, \{\Theta_{l,\pi}\}\} \rightarrow (A_{l,\pi}, \Theta_{l,\pi})$;
- управление структурой функционального взаимодействия протоколов Π_l между собой на одном и том же уровне функционирования системы связи (отображение множества выходов $Y_{l,\pi}$ одних протоколов на множество входов $X_{l,\pi}$ других):

  U_l: $\{\Theta_l\} \rightarrow \Theta_l$, где $\Theta_l=(X_l, Y_l)$.

Ввиду ограниченности ресурсов R_l конкретного уровня задача их распределения между множеством протоколов Π_l формализуется на основе теории комбинаторной оптимизации и, как правило, формулируется в виде задачи о ранце, или в виде задачи оптимизации расписания [223, 224]. Задачи выбора алгоритмов $A_{l,\pi}$ и их параметров $\{\Omega_{l,\pi,a}\}$, как правило, решаются на основе методов линейного или динамического программирования с целью оптимизации выбранных показателей QoS: $\{q_{l,\pi} \rightarrow \max \mid q_{l,\pi} \geq q_{l,\pi}^{\text{треб}}\}$, $q_{l,\pi} \in Q_{l,\pi}$. Ввиду множественности показателей $q_{l,\pi}$, входящих в $Q_{l,\pi}$, для перехода от множества локальных экстремумов $\{q_{l,\pi} \rightarrow \max\}$ к глобальному максимуму по интегральному показателю $Q_{l,\pi} \rightarrow \max$, как правило, вводят дополнительные весовые коэффициенты для отдельных показателей q_l и применяют метод многокритериальной оптимизации по Парето [225].

Управление $U_{l,\pi}$, в общем случае, должно соответствовать принципу компенсации из теории управления по отношению к дестабилизирующим воздействиям $V_{l,\pi}$ и условиям естественной среды $\chi_{l,\pi}$. При этом компенсация может быть:

- *активной*, за счет формирования управляющих воздействий $U_{l,\pi}$ на соответствующие объекты управления (см. выше);
- *пассивной*, за счет внесения некоторой избыточности (количественной, функциональной или временной) в математическое обеспечение $A_{l,\pi}$, в параметры $\Omega_{l,\pi}$ протокола π_l, в структуру взаимодействия протоколов Θ_l, а также в распределяемый протоколу ресурс $R_{l,\pi}$. Это позволит обеспечить выполнение требований по QoS $\forall \{q_{l,\pi} \geq q_{l,\pi}^{\text{треб}}\} \in Q_{l,\pi}$ в более широком диапазоне параметров среды $X_{l,\pi} = R_{l,\pi} \times \chi_{l,\pi} \times V_{l,\pi}$.

Управляющие воздействия $U_{l,\pi}$ поступают по каналу управления, который представляет собой служебный канал в составе сети связи или в отдельной управляющей сети. Этим фактом, а также общей спецификой функционирования системы связи определяются основные особенности процесса управления протоколами в ней:

- дискретность процесса управления: $T_U=\{t_1, t_2, \ldots, t_n, \ldots\}$;
- случайные задержки в передаче управляющих воздействий $U_{l,\pi}$;
- потери сообщений содержащих управляющие воздействия $U_{l,\pi}$ в процессе их передачи;
- ситуации нарушения причинности процесса управления (в пакетной сети связи возможны ситуации, когда более позднее сообщение с

управляющим воздействием $U_{l,\pi}(t_2)$ поступает управляемому объекту раньше, чем предыдущее сообщение $U_{l,\pi}(t_1)$, $t_2>t_1$);

- наличие дестабилизирующих воздействий $V_{l,\pi}$, связанных с нарушением функционирования канала управления ($u_{l,\pi}=0$, $u_{l,\pi}\in U_{l,\pi}$) или подменой сообщений с управляющими воздействиями ($u_{l,\pi}=v_{l,\pi}$, где $u_{l,\pi}\in U_{l,\pi}$, $v_{l,\pi}\in V_{l,\pi}$).

5.2.6. Формализация канала разведки протокола со стороны системы дестабилизирующих воздействий

Опишем в формальном виде канал разведки $M_{l,\pi}$ протокола π со стороны системы дестабилизирующих воздействий. Канал разведки $M_{l,\pi}$, функционирует аналогично каналу наблюдения $N_{l,\pi}$ со стороны системы управления связью:

$$M_{l,\pi} = Y_{l,\pi,M} \times Q_{l,\pi,M},$$

где $Y_{l,\pi,M} \subseteq Y_{l,\pi}$ и $Q_{l,\pi,M} \subseteq Q_{l,\pi}$ – элементы множеств $Y_{l,\pi}$ и $Q_{l,\pi}$ наблюдаемые по отдельным наблюдениям $\mu_{l,\pi}$ системой управления воздействиями противника.

Вместе с тем, каналу разведки $M_{l,\pi}$ свойственна одна принципиальная особенность. Ввиду того, что возможности разведки противника $M_{l,\pi}$ ниже возможностей канала наблюдения системы связи $N_{l,\pi}$, противник не может получить доступ ко всем наблюдаемым параметрам $Y_{l,\pi,N}$ и $Q_{l,\pi,N}$ вектора $N_{l,\pi}$. Таким образом, количество параметров протокола π_l, наблюдаемых противником по каналу разведки $M_{l,\pi}$, как правило, меньше, чем количество параметров $N_{l,\pi}$, наблюдаемых системой управления связью, т.е.:

$$M_{l,\pi} \subseteq N_{l,\pi} \subseteq Y_{l,\pi} \times Q_{l,\pi}, \qquad (5.11)$$

при этом равенство $M_{l,\pi}=N_{l,\pi}$ обеспечивается только в случаях, когда система разведки противника получила полный доступ к каналу наблюдения системы управления связью (например, путем перехвата сообщений канала наблюдения $N_{l,\pi}$).

Целью наблюдения $\mu_{l,\pi}$, производимого по каналу разведки $M_{l,\pi}$, является определение текущего состояния протокола s_π и принятие решения о выработке преднамеренных воздействий $V_{l,\pi}$ на протокол π_l. С учетом выражения (5.11), можно сделать вывод о том, что система воздействия всегда наблюдает протокол π_l с меньшей степенью полноты и достоверности, чем система управления связью.

При разведке системы связи противником на первом этапе необходимо решить задачу идентификации множества конкретных протоколов $\{\pi_l\}$, используемых на l-ом уровне, среди множества протоколов Π_l по каналу разведки $M_{l,\pi}$. Как правило, данная задача решается на основе теории идентификации и теории классификации. На втором этапе решается задача определения состояния s_π для каждого конкретного протокола π_l. Как правило, задачи обоих этапов решаются за счет формирования признакового пространства и построения в нем траекторий наблюдения показателей $\{\mu_{l,\pi}(t)\} \in M_{l,\pi}$, в течение некоторого промежутка времени $t_{\text{набл}}$, достаточным для накопления данных и идентификации конкретных протоколов $\{\pi_l\} \in \Pi_l$ и их состояний $\{s_\pi\}$.

Основными проблемными аспектами, связанными с каналом разведки протокола со стороны противника, являются:

- наличие временной задержки, связанной с накоплением данных наблюдения в течении $t_{набл}$;
- наблюдение группы протоколов Π_l^* l-го уровня по их общим показателям качества Q_l^* и выходным параметрам Y_l^*, являющимися общими для всей группы:

$$\begin{cases} \Pi_l^* = \bigcup\left(\pi_l \left| \left(\bigcap_{\Pi_l} Q_{l,\pi,M} = Q_{l,M}^* \neq \varnothing\right) \wedge \left(\bigcap_{\Pi_l} Y_{l,\pi,M} = Y_{l,M}^* \neq \varnothing\right)\right.\right); \\ M_{l,\Pi_l^*} = Q_{l,M}^* \times Y_{l,M}^* = \left(\bigcap_{\forall \pi_l \in \Pi_l^*} Q_{l,\pi,M}\right) \bigcup \left(\bigcap_{\forall \pi_l \in \Pi_l^*} Y_{l,\pi,M}\right); \end{cases}$$

  что существенно затрудняет идентификацию состояния s_π каждого из протоколов $\pi_l \in \Pi_l^*$, входящих в группу;
- сложность достоверного определения состояния протокола s_π в условиях параметрического сужения:

  $\{s_\pi\} \to \{\pi_l\} \to \Pi_l \to Y_l \times Q_l \to Y_{l,M} \times Q_{l,M} \to M_l \to \{M_{l,\pi}\}$,

  а также сужения реакции, в связи с ограничениями на дискретность $T_\mu = \{t_1, t_2, \ldots, t_n, \ldots\}$ и общую длительность времени наблюдения $t_{набл}$;
- возможности системы связи по активному противодействию каналу разведки противника за счет выполнения мероприятий по противодействию средствам разведки ($\mu_{l,\pi} = 0$), а также за счет создания ложных систем и средств связи, реализующих внедрение в канал разведки противника $M_{l,\pi}$ дезинформации об истинных режимах работы и об используемых в системе связи протоколах;
- наличие требований по скрытности ведения разведки, которые ограничивает возможности по активному сбора данных о состоянии протоколов системы связи.

Для повышения уровня достоверности разведки системой дестабилизирующих воздействий могут выдаваться тестовые воздействия $V_{l,\pi}^{тест}$, которые соответствуют однозначно идентифицируемой траектории изменения параметров $Q_{l,\pi,M}(t)$ и $Y_{l,\pi,M}(t)$, наблюдаемых в канале $M_{l,\pi}$. Бескомпроматное использование таких тестовых воздействий $V_{l,\pi}^{тест}$, подобранных специально для идентификации протоколов π_l, а также их состояний $\{s_\pi\}$ на начальном этапе конфликта, позволит собрать сведения о составе и функциональной структуре l-го уровня системы связи, а на этапах развития конфликта – контролировать эффективность воздействия.

5.2.7. Формализация канала воздействия на протокол со стороны системы дестабилизирующих воздействий

Опишем в формальном виде канал воздействия $V_{l,\pi}$ на протокол π со стороны системы дестабилизирующих воздействий. По итогам наблюдения в канале разведке $M_{l,\pi}$ система дестабилизирующих воздействий принимает решение о выборе и осуществлении воздействия $V_{l,\pi} = \{v_{l,\pi}\}$ из множества воздействий V_l, которые могут быть осуществлены на l-ом уровне функционирования

системы связи. Выбор воздействия $V_{l,\pi}$ должен учитывать совокупность факторов естественной среды $\chi_{l,\pi}$, выделенный протоколу ресурс $R_{l,\pi}$, а также состав математического обеспечения протокола π: его алгоритмы $A_{l,\pi}$ и их параметры $\Omega_{l,\pi}$. Фактически, совокупность протокола π и системы дестабилизирующих воздействий образуют как бы еще один контур управления с антагонистическим критерием достижения цели воздействия – снижения заданного или всех показателей качества протокола $q_{l,\pi}$ ниже требуемых значений $q_{l,\pi}^{\text{треб}}$:

$$\left[\begin{array}{l} \exists\left\{q_{l,\pi} < q_{l,\pi}^{треб}\right\} \in Q_{l,\pi}; \\ \forall\left\{q_{l,\pi} < q_{l,\pi}^{треб}\right\} \in Q_{l,\pi}. \end{array}\right. \qquad (5.12)$$

Конечное множество воздействий $V_{l,\pi}=\{v_{l,\pi}\}$ на интервале времени T_V образует программу воздействий. Программа воздействий может реализоваться:

- в дискретном времени

  $V_{l,\pi}=\{V_{l,\pi}(t_1), V_{l,\pi}(t_2), \ldots, V_{l,\pi}(t_n), \ldots\}$, $T_V=\{t_1, t_2, \ldots, t_n, \ldots\}$;
- в непрерывном времени

  $V_{l,\pi}=V_{l,\pi}(t)$, $t \in T_V$.

Программа воздействий $V_{l,\pi}$ при любом начальном состоянии протокола $s_\pi(t_0)$ и наличии управляющих воздействий $U_{l,\pi}$ должна обеспечивать выполнение критерия (5.12), т.е. обеспечивать существование предела (в первом уравнении системы)

$$\begin{cases} q_{l,\pi} = \lim\limits_{\substack{t \to T_V \\ V_{l,\pi}(t)}} f_{l,\pi}\left(t,\ s_\pi,\ X_{l,\pi},\ U_{l,\pi},\ A_{l,\pi}\right); \\ \exists\left\{q_{l,\pi} < q_{l,\pi}^{\text{треб}}\right\} \in Q_{l,\pi}; \\ X_{l,\pi} = R_{l,\pi} \times \chi_{l,\pi} \times V_{l,\pi}; \\ V_{l,\pi}(t) = \left\{v_{l,\pi}\right\} \times T_U. \end{cases}$$

Наличие программы воздействий $V_{l,\pi}$ должно предусматривать план воздействий $V_{l,\pi}^{\text{план}}=\{V_{l,\pi}(t_{\text{тек}+1}), V_{l,\pi}(t_{\text{тек}+2}), \ldots, V_{l,\pi}(t_{\text{тек}+n}), \ldots\}$, который бы обеспечил достижение критерия $\exists\{q_{l,\pi} < q_{l,\pi}^{\text{треб}}\} \in Q_{l,\pi}$ за счетное число шагов n в будущие моменты времени $t_{\text{тек}+n}$.

План воздействия должен предусматривать формирование воздействий $V_{l,\pi}^{\text{план}}(t_{\text{тек}+1})$ в зависимости от текущего наблюдения $M_{l,\pi}(t_{\text{тек}})$, и подчиняться определенной стратегии, связанной с реализацией цели воздействия, а именно – снижения показателей QoS системы связи ($\exists\{q_{l,\pi} < q_{l,\pi}^{\text{треб}}\}$). Как правило, можно рассмотреть следующие основные стратегии воздействий на отдельный протокол π_l при допущении о том, что принятие решения о выработке воздействия $V_{l,\pi}^{\text{план}}(t_{\text{тек}+1})$ осуществляется на каждом шаге независимо от предыдущих воздействий и основано на результатах наблюдения состояния системы связи в канале разведки $M_{l,\pi}(t_{\text{тек}})$:

1) *вероятностная стратегия*, когда при текущем наблюдении в канале разведки $M_{l,\pi}(t_{\text{тек}})$, в следующий момент времени осуществляется выбор такого воздействия $V_{l,\pi}^{\text{план}}(t_{\text{тек}+1})$ из имеющегося множества альтернатив $\{V_{l,\pi}(t_{\text{тек}+1})\}$, которое с наибольшей вероятностью ведет к выполнению критерия эффективности воздействия (5.12) по одному или не-

скольким показателям качества $q_{l,\pi}$, входящим в множество $Q_{l,\pi,v}=\{q_{l,\pi} \mid q_{l,\pi}<q_{l,\pi}^{\text{треб}}\}$ ($Q_{l,\pi,v}\in Q_{l,\pi}\in Q_l$) т.е.

$$V_{l,\pi}^{\text{план}}:\frac{\left\{V_{l,\pi}^{\text{план}}\left(t_{\text{тек}+1}\right)\right\}}{M_{l,\pi}\left(t_{\text{тек}}\right)}\to V_{l,\pi}\left(t_{\text{тек}+1}\right)\Big|P\left(q_{l,\pi}(t_{\text{тек}+1})<q_{l,\pi}^{\text{треб}}\right)\to\max\,; \qquad (5.13)$$

2) *стратегия максимального отклонения*, когда при текущем наблюдении в канале разведки $M_{l,\pi}(t_{\text{тек}})$ осуществляется выбор такого воздействия $V_{l,\pi}^{\text{план}}(t_{\text{тек}+1})$, которое максимизировало бы отклонение показателей $q_{l,\pi}\in Q_{l,\pi,v}$ от их требуемых значений $q_{l,\pi}^{\text{треб}}$:

$$V_{l,\pi}^{\text{план}}:\frac{\left\{V_{l,\pi}^{\text{план}}\left(t_{\text{тек}+1}\right)\right\}}{M_{l,\pi}\left(t_{\text{тек}}\right)}\to V_{l,\pi}\left(t_{\text{тек}+1}\right)\Big|\left(q_{l,\pi}^{\text{треб}}-q_{l,\pi}(t_{\text{тек}+1})\right)\to\max\,. \qquad (5.14)$$

Ввиду сложности организации воздействий $V_{l,\pi}$, ориентированных на конкретный протокол π_l, и с учетом их интегрального характера целесообразно рассмотреть стратегии воздействий V_l, ориентированные на весь l-ый уровень функционирования. В этом случае стратегии (5.13) и (5.14) могут быть модифицированы с учетом максимизации числа поражаемых протоколов и уровней:

1) *вероятностная стратегия максимизации количества пораженных протоколов*, когда при текущем наблюдении в канале разведки $M_l(t_{\text{тек}})$ осуществляется выбор такого воздействия $V_l^{\text{план}}(t_{\text{тек}+1})$ из имеющегося множества альтернатив $\{V_l(t_{\text{тек}+1})\}$, которое с наибольшей вероятностью ведет к выполнению критерия эффективности воздействия $\{q_{l,\pi}<q_{l,\pi}^{\text{треб}}\}$ по выбранным показателям качества $q_{l,\pi}$, входящим в множество $Q_{l,v}=\cup Q_{l,\pi,v}$, в максимальном числе протоколов $\Pi_{l,v}$ из множества Π_l

$$V_l^{\text{план}}:\frac{\left\{V_l^{\text{план}}\left(t_{\text{тек}+1}\right)\right\}}{M_l\left(t_{\text{тек}}\right)}\to V_l\left(t_{\text{тек}+1}\right)\Big|\left(P\left(\left|\Pi_{l,v}\right|\right)\to\max\right)\wedge\left(\left|\Pi_{l,v}\right|\to\max\right), \qquad (5.15)$$

где: $\left|\Pi_{l,v}\right|$ – число элементов множества протоколов Π_l, поражаемых воздействием V_l; $P\left(\left|\Pi_{l,v}\right|\right)$ – вероятность успешного поражения множества протоколов Π_l воздействием V_l;

2) *стратегия максимального интегрального отклонения*, когда при наблюдении по каналу разведки $M_l(t_{\text{тек}})$ осуществляется выбор такого воздействия $V_l^{\text{план}}(t_{\text{тек}+1})$, которое максимизировало бы отклонение показателей $q_{l,\pi}\in Q_{l,v}$ от их требуемых значений $q_{l,\pi}^{\text{треб}}$ в максимальном числе протоколов $\Pi_{l,v}$ из множества Π_l:

$$V_l^{\text{план}}:\frac{\left\{V_l^{\text{план}}\left(t_{\text{тек}+1}\right)\right\}}{M_l\left(t_{\text{тек}}\right)}\to V_l\left(t_{\text{тек}+1}\right)\Big|\left(\left|\Pi_{l,v}\right|\to\max\right)\wedge$$

$$\wedge\left(\sum_{\pi\in\Pi_{l,v}}\left(q_{l,\pi}^{\text{треб}}-q_{l,\pi}\left(t_{i+1}\right)\right)\to\max\right). \qquad (5.16)$$

В случае наличия единственного показателя качества $\left|Q_{l,\pi,v}\right|=1$, по которому оценивается эффективность воздействия $V_{l,\pi}$ (или V_l). Выражения (5.13-5.16) будут напрямую определять стратегию очередного шага в плане $V_{l,\pi}^{\text{план}}$ (или в $V_l^{\text{план}}$). Если в множество $Q_{l,\pi,v}$ входит несколько показателей качества ($\left|Q_{l,\pi,v}\right|>1$), то для перехода от множества локальных экстремумов к глобаль-

ному максимуму по интегральному показателю необходимо ввести дополнительные весовые коэффициенты для отдельных показателей $q_{l,\pi} \in Q_{l,v}$ или использовать метод многокритериальной оптимизации по Парето [225].

Анализ отличительных особенностей стратегий (5.13, 5.14) и (5.15, 5.16) позволяет сделать следующий вывод. Использование стратегий (5.13, 5.14), а также воздействий, ориентированных на подавление отдельных протоколов π_l, целесообразно, в случае высокой степени наблюдаемости протокола по каналу разведки $M_{l,\pi}$, когда возможно параметрическое выделение состояния s_π каждого из протоколов π_l множества Π_l:

$$M_l \rightarrow M_{l,\pi} \rightarrow Y_{l,\pi,M} \times Q_{l,\pi,M} \rightarrow \{\pi_l\} \rightarrow \{s_\pi\}.$$

Стратегии (5.15, 5.16) и воздействия V_l, обладающие максимальным «площадным эффектом» $|\Pi_{l,v}| \rightarrow \max$, целесообразно использовать, когда по наблюдению в канале разведки M_l сложно осуществить параметрическое выделение состояния s_π каждого из протоколов π_l, а возможно только определение общего направления функционирования множества протоколов Π_l:

$$M_l \rightarrow Y_{l,M} \times Q_{l,M} \rightarrow \Pi_l.$$

План воздействий $V_{l,\pi}^{\text{план}}$ при вероятностных стратегиях (5.13, 5.15) может быть формализован на основе теории марковских и полумарковских процессов, а задача управления воздействием на протокол π_l или на их множество Π_l может быть сведена к оптимизации семейства вероятностей вида (5.13). План воздействий $V_{l,\pi}^{\text{план}}$ и $V_l^{\text{план}}$ при стратегиях (5.14, 5.16), основанных на максимальном отклонении, может быть формализован на основе теории адаптивного управления. при этом задача воздействия на протокол π_l или на их множество Π_l может быть сведена к оптимизации траектории воздействий $V_l(t_{\text{тек}+1})$, $V_l(t_{\text{тек}+2})$, …, …, $V_{l,\pi}(t_{\text{тек}+n})$, минимизирующих число шагов n, на каждом из которых реализуется управление воздействиями (5.14) или (5.16) для достижения условия (5.12).

В работах [1, 5, 226] вводится понятие «ресурса воздействия» $R_V=\{r_{l,v}\}$ как совокупности временных, энергетических и вероятностных параметров, описывающих одно или несколько воздействий V_l с целью дестабилизирующего влияния на элементы системы связи. В тех же работах показано, что система воздействий должна минимизировать расход своего ресурса при одновременном рациональном его распределении между отдельными воздействиями $\{V_{l,\pi}\}$. С учетом вышеуказанного, целесообразно дополнить стратегии (5.13-5.16) дополнительным критерием выбора воздействий: по итогам наблюдения в канале разведки $M_l(t_{\text{тек}})$ на следующем шаге $t_{\text{тек}+1}$ целесообразно выбирать такое воздействие $V_l(t_{\text{тек}+1})$, которое минимизирует суммарный расход ресурса воздействия $R_{l,V}$ на l-ом уровне функционирования:

$$V_l^{\text{план}} : \frac{\left\{V_l^{\text{план}}\left(t_{\text{тек}+1}\right)\right\}}{M_l\left(t_{\text{тек}}\right)} \rightarrow V_l\left(t_{\text{тек}+1}\right)\Big| R_{l,V} \rightarrow \min, \qquad (5.17)$$

при этом возможно выделить отдельную подзадачу – рациональное распределение общего ресурса воздействия $R_{l,V}$ по отдельным подресурсам $\{R_{l,\pi,V}\}$, выделяемых каждому воздействию $V_{l,\pi}$ на отдельные протоколы $\{\pi_l\}$, с целью реализации стратегий (5.13-5.16) и выполнения критерия $R_{l,V} \rightarrow \min$.

Конкретизация плана воздействия $V_{l,\pi}^{план}$ будет состоять в выделении отдельных объектов, воздействие на которые планируется на очередном шаге $t_{тек+1}$.

В зависимости от объекта воздействия, по отношению к произвольному протоколу l-го уровня, можно выделить:

1) воздействия на входные данные:

- ограничение как общего ресурса l-го уровня R_l, так и ресурсов отдельных протоколов $R_{l,\pi}$

  $V_l : R_l \rightarrow R_{l,v} \mid \exists \{R_{l,v} < R_l\}$,

  $V_{l,\pi} : R_{l,\pi} \rightarrow R_{l,\pi,v} \mid \exists \{R_{l,\pi,v} < R_{l,\pi}\}$;
- усугубление последствий воздействия дестабилизирующих факторов естественной среды $\chi_{l,\pi}$ функционирования протокола π_l

  $V_{l,\pi} : (X_{l,\pi} = R_{l,\pi} \times \chi_{l,\pi}) \rightarrow (X_{l,\pi} = R_{l,\pi} \times (\chi_{l,\pi} \times V_{l,\pi}))$;
- ограничение или подмена входных параметров $X_{l,\pi}$ протокола

  $V_{l,\pi} : X_{l,\pi} \rightarrow X_{l,\pi,v} \mid \exists \{x_{l,\pi,v}=0\}$, при условии $|X_{l,\pi}| = |X_{l,\pi,v}|$,

  $V_{l,\pi} : X_{l,\pi} \rightarrow X_{l,\pi,v} \mid \exists \{x_{l,\pi}=v_{l,\pi}\}$, при условии $|X_{l,\pi}| = |X_{l,\pi,v}|$.

2) воздействия на функционал протокола:

- функциональная блокировка за счет ограничения параметров $\omega \in \Omega_{l,\pi}$ в алгоритмах $A_{l,\pi}$ протокола π_l

  $V_{l,\pi} : \Omega_{l,\pi} \rightarrow \Omega_{l,\pi,v} \mid \exists \{\omega=0 \mid \omega \in \Omega_{l,\pi,v}\}$, при $|\Omega_{l,\pi}| = |\Omega_{l,\pi,v}|$;
- функциональная блокировка за счет ограничения исполнения алгоритмов $A_{l,\pi}$ в протоколе π_l

  $V_{l,\pi} : A_{l,\pi} \rightarrow A_{l,\pi,v} \mid \exists \{a=\varnothing \mid a \in A_{l,\pi,v}\}$, при $|A_{l,\pi}| = |A_{l,\pi,v}|$;
- функциональная блокировка за счет ограничения функциональных связей $\Theta_{l,\pi}$ алгоритмов $A_{l,\pi}$ в протоколе π_l

  $V_{l,\pi} : \{A_{l,\pi}, \Theta_{l,\pi}\} \rightarrow \Theta_{l,\pi,v} \mid \exists (\{\theta=\varnothing \mid \theta \in \Theta_{l,\pi,v}\} \wedge \{\theta \neq \varnothing \mid \theta \in \Theta_{l,\pi}\}_i)=1$,

  где $\wedge$ – знак конъюнкции (логическое «и»), $\theta \in \Theta_{l,\pi}$;
- навязывание ложной логики функционирования за счет подмены или искажения параметров алгоритмов $\Omega_{l,\pi}$ в множестве алгоритмов $A_{l,\pi}$ протокола π_l

  $V_{l,\pi} : \Omega_{l,\pi} \rightarrow \Omega_{l,\pi,v} \mid \exists \{\omega=v_{l,\pi,a} \mid \omega \in \Omega_{l,\pi,v}\}$, при $|\Omega_{l,\pi}| = |\Omega_{l,\pi,v}|$;
- навязывание ложной логики функционирования за счет подмены или искажения отдельных алгоритмов a в множестве алгоритмов $A_{l,\pi}$ протокола π_l

  $V_{l,\pi} : A_{l,\pi} \rightarrow A_{l,\pi,v} \mid \exists \{a=v_{l,\pi,a} \mid a \in A_{l,\pi,v}\}$, при $|A_{l,\pi}| = |A_{l,\pi,v}|$;
- навязывание ложной логики функционирования за счет нарушения функциональных связей $\Theta_{l,\pi}$ алгоритмов $A_{l,\pi}$ протокола π_l

  $V_{l,\pi} : \{A_{l,\pi}, \Theta_{l,\pi}\} \rightarrow \Theta_{l,\pi,v} \mid \exists (\{\theta=v_{l,\pi} \mid \theta \in \Theta_{l,\pi,v}\} \wedge \{\theta \neq \varnothing \mid \theta \in \Theta_{l,\pi}\})=1$,

  где $\theta \in \Theta_{l,\pi}$.

Как правило, воздействия, ориентированные на входные данные, реализуются внешними по отношению к протоколу средствами и способами (воздействие физических и радиоэлектронных средств подавления, подмена или искажение передаваемых по системе связи пакетов, DOS и DDOS атаки и т.д.). Воздействия, ориентированные на функциональную блокировку или навязывание ложной логики, требуют глубокого знания функционирования атакуемого про-

токола и реализуются программными и аппаратными закладками, а также с помощью деструктивных программных средств (компьютерных вирусов).

Воздействие $V_{l,\pi}$, в общем случае, должно соответствовать принципу компенсации из теории управления по отношению к управлению $U_{l,\pi}$ и условиям среды $\chi_{l,\pi}$. При этом, такое компенсационное воздействие может быть:

- *активным* за счет непосредственных воздействий $V_{l,\pi}$ на соответствующие объекты (см. выше);
- *пассивным* за счет внесения в математическое обеспечение $A_{l,\pi}$ и параметры $\Omega_{l,\pi}$ протокола π_l, а также в структуру взаимодействия протоколов Θ_l специализированных «закладок». Их наличие позволит реализовать режимы снижения быстродействия, появление квазислучайных вычислительных ошибок, переход в ложные режимы функционирования, а также режимы «внутреннего благоприятствования» воздействиям $V_{l,\pi}$. Это обеспечит выполнение критерия эффективности воздействия $\exists\{q_{l,\pi}<q_{l,\pi}^{\text{треб}}\}$ в более широком диапазоне воздействий $V_{l,\pi}$ и для большего числа показателей качества $\{q_{l,\pi}\}\in Q_{l,\pi,v}$.

Специфика конфликтного взаимодействия с системой связи формирует основные особенности процесса воздействий на протоколы:

- управление выдачей воздействий $V_{l,\pi}$ и V_l ведется в условиях ограниченной наблюдаемости протоколов l-го уровня;
- стратегии воздействий $V_{l,\pi}$ и V_l, а также выбор конкретных способов воздействий на l-ом уровне зависит от степени наблюдаемости этого уровня;
- любые воздействия $V_{l,\pi}$ и V_l реализуют интегральный эффект поражения, так как протоколы взаимосвязаны при решении задач l-го уровня функционирования;
- воздействия $V_{l,\pi}$ и V_l на l-ом уровне могут быть ориентированы на входные параметры или на функционал протокола(ов), и при этом могут носить как пассивный, так и активный характер;
- воздействиям $V_{l,\pi}$ и V_l свойственна инертность реакции на наблюдение в канале разведки $M_{l,\pi}$.

Данные особенности процессов воздействия, а также особенности разведки $M_{l,\pi}$, изложенные выше, позволяют сделать вывод, что в контуре управления воздействиями всегда присутствует неопределенность определения состояний как отдельных протоколов, так и их множества на l-ом уровне. Эти аспекты позволяют отнести задачу разработки системы воздействия к задачам робастного анализа с целью поиска неустойчивых режимов функционирования протокола системы связи как динамической системы.

5.2.8. Итоговые выводы

Таким образом, любой протокол π_l может быть описан как динамическая система, функционирующая в сложной параметрической среде, при этом сам протокол, фактически, является частью двух органов управления – системы управления связью и системы управления воздействиями, которые преследуют антагонистические цели функционирования. Такая функциональная дуальность

определяет информационный конфликт вышеуказанных систем управления, который происходит и развивается в приложении к конкретному протоколу. Дополнительно к вышеуказанному следует отметить, что протокол является частью сложной функционально-взаимосвязанной структуры как в горизонтальной области – в соответствии задачами отдельного уровня OSI, так и в вертикальной – в соответствии с задачами межуровневого протокольного взаимодействия. В связи с этим, целесообразно на основе представленной модели протокола, функционирующего на отдельном уровне OSI, рассмотреть функционирование всей функционально-взаимосвязанной протокольной структуры системы связи, с учетом ее многоуровневого иерархического конфликтного взаимодействия с системой дестабилизирующих воздействий.

5.3. Динамическая многоуровневая модель системы связи

5.3.1. Схема модели

Особенность системы связи состоит в том, что она, в соответствии с моделью OSI, функционирует на семи иерархических уровнях. При этом на каждом из этих уровней имеется множество функционально-связанных протоколов, решающих задачи связи данного уровня (рис. 5.4). Несмотря на то, что эталонная модель OSI постулирует независимость отдельных уровней и необходимость решения задач каждого уровня самостоятельно и независимо, на самом деле уровни OSI являются функционально вложенными «снизу-вверх». Таким образом, отказ на нижних уровнях ведет к изменению показателей качества связи на более высоких уровнях. В связи с этим, целесообразно дополнить «принцип независимости уровней системы связи», рассматриваемый в модели OSI, учетом функционально-иерархической вложенности нижестоящих уровней в вышестоящие за счет использования методов теории сложных иерархических систем.

Каждый l-ый уровень системы связи решает свои функциональные задачи. При этом, непосредственно сам уровень, образован совокупностью функционально-взаимодействующих протоколов $\Pi_l=\cup\pi_l$, которые функционируют в параметрическом пространстве среды $X_l=R_l\times\chi_l\times V_l$ (где $\chi_l=\cup\chi_{l,\pi}$, $R_l=\cup R_{l,\pi}$, $V_l=\cup V_{l,\pi}$). В соответствии с этими особенностями, каждому уровню присущи специфические для него параметры естественной среды χ_l, ресурсы R_l и воздействия V_l, при этом эффективность функционирования нижних уровней напрямую определяет эффективность функционирования более верхних уровней.

Рассмотрим модель системы связи как обобщение модели протокола, рассмотренной выше. Как показано на рис. 5.4, система связи состоит из семи уровней, которые соответствуют модели OSI, и каждому из уровней соответствует собственная совокупность протоколов. С учетом формального описания протокола, представленного выше, каждый l-ый уровень в составе иерархической модели сети будет описываться следующими параметрами и отображениями.

1) Входные параметры l-го уровня:

- множество обобщенных параметров среды $X_l = R_l \times \chi_l \times V_l$ (где $\chi_l = \cup \chi_{l,\pi}$, $R_l = \cup R_{l,\pi}$, $V_l = \cup V_{l,\pi}$), в которой функционирует множество протоколов Π_l ($\Pi_l = \cup \pi_l$) на l-ом уровне, включающее в себя:
  - множество параметров естественной среды l-го уровня χ_l ($\chi_l \subseteq \chi$);
  - множество ресурсов связи l-го уровня R_l ($R_l \subseteq R$);
  - множество преднамеренных воздействий V_l, реализуемых системой дестабилизирующих воздействий на l-ом уровне и влияющих на функционирование протоколов Π_l ($V_l \subseteq V$);
- множество управляющих воздействий $U_l = \{U_{l,\pi}\} \times T$ (где $U_l \subseteq U$) на протоколы Π_l со стороны системы управления связи на l-ом уровне;
- множество моментов времени функционирования системы связи T.

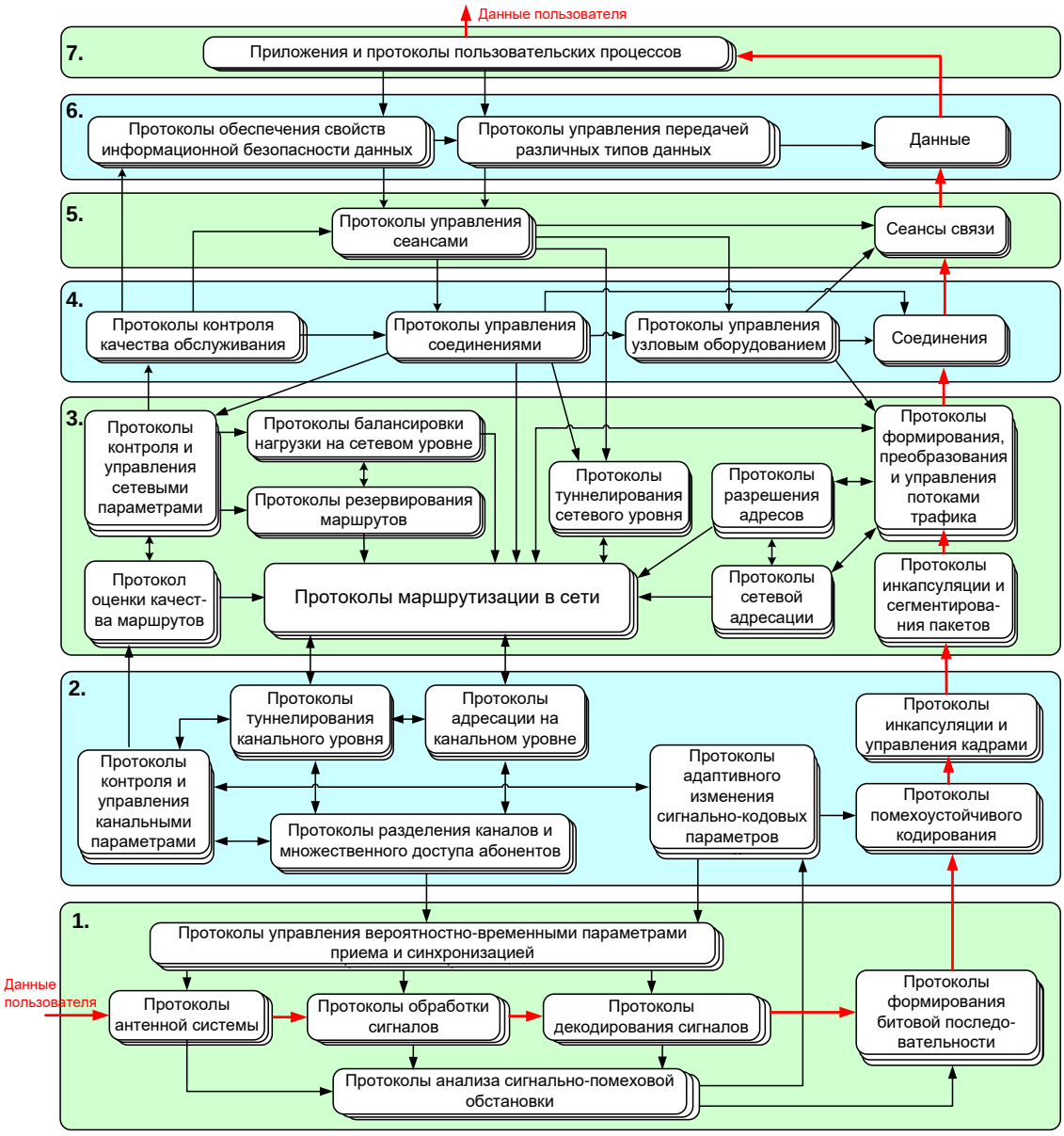

Рис. 5.4. Функциональная связь протоколов системы связи на различных уровнях модели OSI

2) Внутренние параметры l-го уровня:

- множество алгоритмов A_l протоколов Π_l на l-ом уровне системы связи:

$$A_l = \bigcup_{\Pi_l} A_{l,\pi}; \qquad (5.18)$$

- множество параметров Ω_l алгоритмов A_l протоколов Π_l на l-ом уровне системы связи:

$$\Omega_l = \bigcup_{\Pi_l} \Omega_{l,\pi}; \qquad (5.19)$$

3) Отображения, определяющие общую динамическую модель l-го уровня системы связи:

- отображение ψ_l, задающее смену состояний s_l l-го уровня системы связи:

$$s_l = \{s_\pi\} \cup \Theta_l = \psi_l(t_0, t, \{\pi\}, \{S_\pi\}, X_l, U_l, A_l, \Theta_l), \qquad (5.20)$$

  при этом состояние l-го уровня определяется как объединение множества состояний всех протоколов этого уровня $\{s_\pi\}$ и состояния функционально-структурных связей между протоколами Θ_l;
- отображение f_l, определяющее выходные показатели качества обслуживания Q_l, которые обеспечивают протоколы Π_l на l-ом уровне функционирования:

$$Q_l = f_l(t, s_l, X_l, U_l, A_l); \qquad (5.21)$$

- отображение γ_l, определяющее выходные параметры Y_l протоколов Π_l на l-ом уровне:

$$Y_l = \gamma_l(t, s_l, X_l, U_l, A_l); \qquad (5.22)$$

- отображение φ_l, определяющее параметрическое множество среды X_{l+1} функционирования протоколов более высокого уровня Π_{l+1}:

$$X_{l+1} = \varphi_l(s_\pi, t, X_l, U_l, A_l). \qquad (5.23)$$

4) Выходные параметры:

- множество выходных параметров l-го уровня Y_l;
- множество показателей качества обслуживания Q_l, которые обеспечиваются на l-ом уровне функционирования;
- множество параметров среды функционирования протоколов более высокого уровня X_{l+1};
- канал наблюдения $N_l = \cup N_{l,\pi} = Y_{l,N} \times Q_{l,N}$ со стороны системы управления связью в интересах принятия решений по управлению связью;
- канал наблюдения $M_l = \cup N_{l,\pi} = Y_{l,M} \times Q_{l,M}$ со стороны системы дестабилизирующих воздействий в интересах принятия решений по целесообразному применению воздействий V_l.

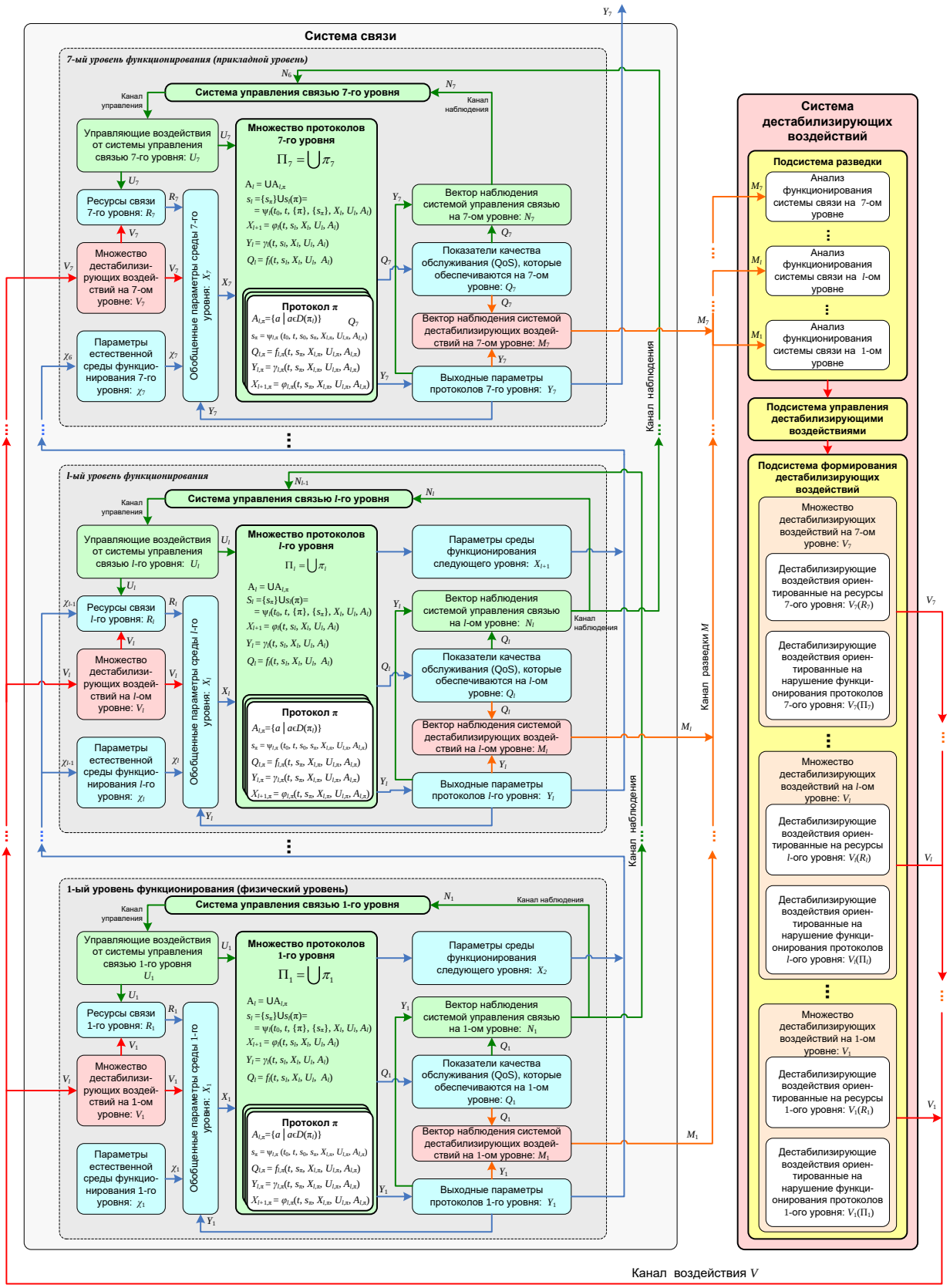

Рис. 5.5. Динамическая многоуровневая модель системы связи

С учетом вышеизложенного, иерархическая модель системы связи как совокупности уровней модели OSI (рис. 5.5) будет определяться следующими параметрами и отображениями.

1) Входные параметры системы связи:

- множество обобщенных параметров среды $X=\cup X_l$, включающие в себя:
  - множество параметров естественной среды $\chi=\cup\chi_l$;
  - множество ресурсов связи $R=\cup R_l$;
  - множество воздействий $V=\cup V_l$, реализуемых системой дестабилизирующих воздействий на l-ых уровнях функционирования;
- множество управляющих воздействий $U=\cup U_l$ со стороны систем управления связью на l-ых уровнях функционирования;
- множество моментов времени функционирования системы связи T.

2) Внутренние параметры системы связи:

- множество алгоритмов A системы связи:

$$A=\cup A_l; \tag{5.24}$$

- множество параметров Ω алгоритмов A системы связи:

$$\Omega=\cup\Omega_l; \tag{5.25}$$

- множество протоколов Π системы связи:

$$\Pi=\cup\Pi_l; \tag{5.26}$$

- множество средств связи, множество средств связи, установленных на узлах сети, при этом каждое средство поддерживает множество протоколов $\{\pi_i\}$, т.е. $e_i=\{\pi_i\}$:

  $E=\{e_i\}$;
- множество узлов сети, при этом каждый узел содержит множество средств связи $\{e_i\}$, т.е. $z_i=\{\{e_i\}, \{\pi_i\}, \{k_{ij}\}\}$:

  $E=\{e_i\}$;
- множество каналов связи, соединяющих узлы:

  $K=\{k_{ij}\}$;

  при этом предполагается, что канал связи $k_{ij}=\{z_i, z_j, e_i, e_j, \pi_{l,k}\}$ соединяет узлы z_i и z_j в случае, если средства связи $e_i\in z_i$ и $e_j\in z_j$, размещенные на этих узлах, используют один и тот же протокол связи $\pi_{l,k}$;
- матрица распределения информационных потоков между абонентами и узлами сети (матрица тяготения):

  Λ;
- текущая конфигурация системы связи, описывающее распределение ресурса R на всех ее уровнях L, состава и взаимного расположения каналов и узлов $\{Z, K\}$, оборудования узлов $E\in Z$, протоколов Π, алгоритмов A и их параметров Ω и характеризующее множество информационных структур Λ, которые могут быть реализованы в системе связи:

  $S_{conf}=\{t, Z, K, R, \Pi, A, \Omega, \Lambda\}$;

3) Отображения, определяющие динамическую модель системы связи:

- отображение ψ, задающее смену состояний S системы связи:

$$S = \{S_l\} \cup \Theta = \psi(t_0, t, \{S_l\}, X, U, A, Z, E, K, \Lambda, \Theta); \quad (5.27)$$

- множество отображений f, определяющих выходные показатели качества обслуживания Q системы связи:

$$Q = f(t, S, X, U, A),\ f = \cup f_l,\ Q = \cup Q_l; \quad (5.28)$$

- множество отображений γ, определяющих выходные параметры Y системы связи:

$$Y = \gamma(t, S, X, U, A),\ \gamma = \cup \gamma_l,\ Y = \cup Y_l; \quad (5.29)$$

- множество отображений φ, определяющих межиерархические связи между уровнями системы связи:

$$\varphi = \cup \varphi_l. \quad (5.30)$$

Фактически, множество отображений φ определяет отличие данной модели от классической модели OSI, которая в явном виде не задает межуровневые отображения.

4) Выходные параметры:

- множество выходных параметров системы связи Y;
- итоговые выходные параметры системы связи Y_7;
- множество показателей качества обслуживания Q системы связи;
- канал наблюдения $N = \cup N_l = Y_N \times Q_N$ со стороны системы управления связью в интересах принятия решений по управлению связью;
- канал наблюдения $M = \cup M_l = Y_M \times Q_M$ со стороны системы дестабилизирующих воздействий в интересах принятия решений по применению многоуровневых воздействий V.

Рассмотрим особенности функционирования системы связи более подробно. Основные особенности системы связи как динамической системы в аспектах ее функционирования, управления, наблюдения и конфликтного взаимодействия с системой дестабилизирующих воздействий могут быть рассмотрены, по аналогии с вышерассмотренной моделью отдельного протокола, в связи с чем, их рассматривать далее в том же ключе, на взгляд автора, не имеет смысла. В связи с этим, при моделировании системы связи, далее акцентируем внимание на основных отличительных, от модели протокола, и эмерджентных свойствах, с учетом ее многоуровневого иерархического построения.

5.3.2. Формализация пространственно-распределенной структуры системы связи

В общем случае процессы функционирования системы связи задаются отображениями (5.26-5.30) и аналогичны процессу функционирования отдельного протокола, рассмотренному выше. Отличительные особенности иерархического построения системы связи и ее специфика заключаются в следующем. Основу системы связи составляет пространственно-распределенная транспортная сеть, состояние элементов которой и определяет состояние S системы связи в целом:

$$S = \psi(t_0, t, \{S_l\}, X, U, A, Z, E, K, \Lambda, \Theta). \quad (5.31)$$

где: $E=\{e_i\}$ – множество средств связи, установленных на узлах сети, при этом каждое средство поддерживает множество протоколов $\{\pi_i\}$, т.е. $e_i=\{\pi_i\}$;

$Z=\{z_i\}$ – множество узлов сети, при этом каждый узел содержит множество средств связи $\{e_i\}$, т.е. $z_i=\{\{e_i\}, \{\pi_i\}, \{k_{ij}\}\}$;

$K=\{k_{ij}\}$ – множество каналов связи, соединяющих узлы. При этом предполагается, что канал связи $k_{ij}=\{z_i, z_j, e_i, e_j, \pi_{l,k}\}$ соединяет узлы z_i и z_j в случае, если средства связи $e_i \in z_i$ и $e_j \in z_j$, размещенные на этих узлах, используют один и тот же протокол связи $\pi_{l,k}$;

Λ – матрица распределения информационных потоков между абонентами и узлами сети (матрица тяготения).

Параметры $Z \times K$ фактически задают граф сети, а отдельные воздействия $V_{l,\pi}$, за счет нарушения функционирования или блокировки протоколов, используемых как в канале связи $k_{ij}=\{z_i, z_j, e_i, e_j, \pi_{l,k}\}$, так и в узле $z_i=\{\{e_i\}, \{\pi_i\}, \{k_{ij}\}\}$, приводят к изменению данной топологии.

Введем понятия физической и информационной структуры сети.

Физическая структура сети – это формализованное представление сети $\{Z, K\}$, характеризующее связи, реализованные каналообразующей аппаратурой между узлами системы связи [1].

Информационная структура сети – это формализованное представление наложенной сети Λ, которая образуется множеством путей передачи сообщений между узлами в физической сети $\{Z, K\}$ [1].

Кроме того, целесообразно ввести понятие конфигурации системы связи.

Конфигурация системы связи – это формализованное представление текущего состояния системы связи $S_{\text{conf}}=\{t, Z, K, R, \Pi, A, \Omega, \Lambda\}$, описывающее распределение ресурса R на всех ее уровнях L, состава и взаимного расположения узлов и каналов $\{Z, K\}$, оборудования узлов $E \in Z$, протоколов Π, алгоритмов A и их параметров Ω, а также множество информационных структур Λ, которые в настоящий момент реализованы в системе связи [1].

5.3.3. Формализация процесса функционирования системы связи

Процесс функционирования системы связи определяется отображением $\gamma:\{t, S, X, U, A\} \rightarrow Y$, задаваемым выражением (5.29). В процессе функционирования системы связи производится доставка сообщений Y_7 с показателями качества Q, что соответствуют целевому назначению системы связи в зависимости от ее текущего состояния S, а также множества входных воздействий X и управления U. Качество выполнения функций по целевому назначению для системы связи определяется показателями Q, которые зависят от множества используемых протоколов Π, функционирующих в соответствии с алгоритмами A и их параметрами Ω, а также зависят от параметров среды $X=R \times \chi \times V$.

5.3.4. Формализация показателей качества функционирования системы связи

Качество функционирования системы связи является ее интегральным свойством, характеризующим способность обеспечивать своевременную, до-

стоверную и безопасную передачу сообщений в интересах информационно-управляющей системы более высокого уровня.

Качество функционирования определяется как свертка отдельных показателей эффективности системы связи из множества Q на различных уровнях ее функционирования.

В общем случае показатели качества можно классифицировать следующим образом [1]:

1) по характеризуемым качественным сторонам системы связи:
- показатели, характеризующие СС как материальный объект:
  а) готовность;
  б) устойчивость, определяемая живучестью, помехоустойчивостью и надежностью;
  в) пропускная способность;
  г) мобильность;
  д) безопасность, включающая в себя разведзащищенность и имитостойкость;
- показатели, характеризующие процессы передачи информации в системе связи:
  а) своевременность;
  б) достоверность;
  в) скрытность;
- показатели, характеризующие сложность планирования, развертывания и эксплуатации системы связи, отдельных средств связи, средств обеспечения, а также обслуживающего персонала;
- показатели, характеризующие влияние системы связи на другие смежные системы и метасистему более высокого уровня (определяются задачами системы связи, решаемыми ею в структуре информационно-управляющей системы);

2) по масштабности характеризуемых подсистем:
- элементарные, характеризующие наименьший элемент системы связи, к которому они могут быть применены;
- локальные, характеризующие совокупность элементов системы связи или качество отдельного уровня OSI;
- глобальные, характеризующие отдельные качественные аспекты всей системы связи в целом;

3) по длительности временного интервала, на котором оценивается система:
- текущие или точечные, определяемые на элементарном интервале времени;
- интегральные, характеризующие поведение системы на некотором множестве моментов времени (как правило, при $t \to t_{набл}$ или $t \to \infty$);

4) по роли в решаемой задаче анализа (синтеза):
- первичные, задаваемые в виде исходных данных;
- вторичные – искомые или анализируемые;
- нейтральные, инвариантные к решаемой задаче;

5) по характеризуемому элементу динамической модели:

- состояние системы связи, узлов связи или вышестоящей информационно-управляющей системы в целом;
- состояние системы управления системы связи;
- состояние системы дестабилизирующих воздействий.

Помимо отдельных показателей качества, для системы связи, как сложной иерархической системы, используют интегральные и обобщенные показатели. Интегральные показатели качества вводятся путем свертки отдельных показателей в один. Обобщенные показатели качества характеризуют предпочтительность того или иного состояния в данный момент времени, независимо от состояния системы в другой момент времени, а также ее поведения в целом.

Конкретизируем основные показатели качества системы связи, на основе работы [1].

1) Общие показатели эффективности системы связи:

- состояния: $q(S)$;
- точечные: $q(t)=m_t(q(t))$, где m_t – математическое ожидание показателя q для состояния системы в конкретный момент времени t;
- интегральные: $q=m(q(t))$, где m – математическое ожидание показателя q, усредненное по анализируемому интервалу времени. Интегральные показатели представляются через точечные на основе их усреднения по анализируемому интервалу времени.

2) Показатели готовности системы связи:

- состояния – индикаторы готовности:

$$q_{\text{г}}\left(q,T_{\text{г}}\right)=\begin{cases}1, \text{ при } \forall\left\{q(t\geq T_{\text{г}})\geq q^{\text{треб}}\right\};\\ 0, \text{ при } \exists\left\{q(t\geq T_{\text{г}})< q^{\text{треб}}\right\};\end{cases}$$

- точечные – вероятность готовности к моменту времени t:

  $q(t) = m_t(q(t)) = P(q(S, t)\geq q^{\text{треб}})$;
- интегральные – вероятность готовности в случайно выбранный момент t:

  $q = m(q(t)) = P(q(S)\geq q^{\text{треб}})$.

3) Показатели пропускной способности системы связи:

- состояния:
  а) связность направления связи;
  б) пропускная способность направления связи;
  в) коэффициент реализации требований информационно-управляющей системы более высокого уровня по пропускной способности и связности направления связи;
- точечные:
  а) математическое ожидание пропускной способности и связности направления в момент времени t;
  б) математическое ожидание коэффициента реализации требований по пропускной способности и связности направления в момент времени t;

- интегральные:
  а) математическое ожидание пропускной способности и связности направления за наблюдаемый период времени $t_{набл}$;
  б) математическое ожидание коэффициента реализации требований по пропускной способности и связности направления за наблюдаемый период $t_{набл}$.

4) Показатели устойчивости системы определяются на основе введения функций, характеризующих случайные изменения среды (χ) или преднамеренные воздействия (V), обуславливающие ухудшение показателей качества системы связи: $q_1(X) \rightarrow q_2(X, V)$, $q_1 \geq q_2$:

- показатели устойчивости состояния:
  а) коэффициент, определяющий уменьшение показателей качества состояния системы при наихудшем воздействии V:

$$k_u(q,V) = \inf\left(\frac{q}{q(V)}\right);$$

  б) величина, определяющая уровень воздействия V, необходимого для изменения показателей качества системы ниже требуемого значения:

$$\Delta V = \inf V \mid \exists \{q(X, V) < q^{треб}\};$$

  в) индикатор устойчивости состояния – определяет вероятность соответствия всех показателей качества системы связи $Q=\{q\}$ требуемым значениям:

$$k_u = P(\forall\{q \geq q^{треб}\}). \qquad (5.30)$$

  В более простом случае в качестве индикатора устойчивости можно использовать признак снижения любого из показателей качества ниже требуемого значения:

$$k_u = \begin{cases} 1, \text{ при } \forall\{q \geq q^{треб}\}; \\ 0, \text{ при } \exists\{q < q^{треб}\}. \end{cases}$$

  С учетом того, что для различных уровней функционирования системы связи свойственна свертка показателей качества:

$$Q_1 \rightarrow Q_2 \rightarrow \ldots \rightarrow Q_i \rightarrow \ldots \rightarrow Q_7,$$

  то при рассмотрении индикатора устойчивости системы связи конкретного l-го уровня можно ограничиться сверткой до этого уровня:

$$k_{u\,l} = P(\forall\{Q_l \geq Q_l^{треб}\}); \qquad (5.31)$$

- точечные показатели устойчивости:
  а) определяются и интерпретируются аналогично рассмотренным выше, в соответствии с выражениями (5.30), (5.31);
  б) среднеожидаемое в момент t значение коэффициента потери качества за время Δt (математическое ожидание вычисляется по совместному распределению показателей $q(t)$, $q(t+\Delta t)$ системы в моменты времени t и $t+\Delta t$)

$$\Delta k_u(\Delta t) = (q(t) - q(t+\Delta t))/q(t);$$

в) время Δt, через которое ожидаемое значение показателей качества снизится ниже требуемого значения

$$\Delta t \mid q(t+\Delta t) < q^{\text{треб}}.$$

Интегральные показатели устойчивости. К основным показателям устойчивости, представляющим интерес, можно отнести зависимости конкретных показателей качества q от преднамеренных воздействий V при управлении U. Такая оценка позволяет вывести следующие показатели:

- устойчивость системы связи к воздействиям V;
- устойчивость системы связи к случайным возмущениям среды функционирования χ;
- устойчивость системы связи к нарушению функционирования некоторого конкретного протокола связи π;

Показатели полноты наблюдаемости, скрытности и разведзащищенности как свойств, определяющих возможности по наблюдению со стороны противника, анализируются при формализации конфликта системы связи и системы воздействия. Показатели мобильности, своевременности и достоверности являются внутренними показателями системы связи и учитываются в векторе параметров Q.

В составе показателей качества, применяемых в математических моделях для описания структуры и процесса функционирования системы связи, наряду с вышеуказанными показателями могут выделяться и описываться показатели, соответствующие взаимодействию системы, среды функционирования и других объектов (систем наблюдения и воздействия противника). При этом задача анализа системы связи на ее динамической модели сводится к нахождению временной зависимости показателей эффективности, заданных на состоянии исследуемого объекта, и определению по ним точечных и интегральных показателей системы [1].

Система связи является эффективно функционирующей, в случае, если ее показатели качества верхнего (прикладного) уровня Q_7, получаемые в результате свертки

$$Q_1 \to Q_2 \to \ldots \to Q_i \to \ldots \to Q_7,$$

имеют значения не ниже требуемого, то есть выполняется критерий

$$\forall \{q_7 \geq q_7^{\text{треб}}\},\ q_7 \in Q_7. \qquad (5.32)$$

При этом особое значение имеют четыре нижних уровня модели OSI – физический, канальный, сетевой и транспортный, которые соответствуют телекоммуникационному оборудованию системы связи и в большей степени уязвимы для преднамеренных воздействий. Поэтому, в качестве частного случая, можно рассматривать систему связи как пространственно-распределенную транспортную сеть, ограниченную четырьмя нижними уровнями модели OSI.

В этом случае критерий (5.32) может быть представлен в виде

$$\forall \{q_4 \geq q_4^{\text{треб}}\},\ q_4 \in Q_4. \qquad (5.33)$$

5.3.5. Формализация каналов наблюдения и разведки

Применительно к системе связи в целом, канал наблюдения N со стороны системы управления связью должен включать в себя не только наблюдаемые параметры Q и Y ($N=\cup N_l=Q_N\times Y_N$), но и наблюдаемые данные о конфигурации системы связи $S_{\text{conf}}=\{t, Z, K, R, \Pi, A, \Omega, \Lambda\}$, включающие в себя протоколы Π, алгоритмы A и их параметры Ω, топологию системы связи $Z\times K$, структуру передачи информационных потоков Λ и распределение ресурсов R. Фактически, полную формализацию канала наблюдения можно представить в виде

$$N\times S_{\text{conf}},$$

где: N – наблюдаемые показатели качества и выходные апапметры; S_{conf} – управляемые параметры системы связи, причем управляемые как со стороны системы управления связью, так и со стороны системы дестабилизирующих воздействий.

По аналогии с каналом N, канал разведки со стороны противника M также должен включать в себя помимо показателей Q и Y ($M=\cup M_l= Q_M\times Y_M$) показатели, характеризующие вскрытие и идентификацию протоколов функционирования системы связи $\Pi=\cup\Pi_l$, ее транспортной структуры $\{Z, K\}$, а также информационной структуры Λ, определяемой маршрутами передачи информационных потоков. Идеальным вариантом для противника является полное наблюдение конфигурации системы связи $S_{\text{conf}}=\{t, Z, K, R, \Pi, A, \Omega, \Lambda\}$. Однако в реальности наблюдаемая конфигурация $S_{\text{conf}}^{\text{набл}}$ будет неполной $S_{\text{conf}}^{\text{набл}}\subset S_{\text{conf}}$.

В таком случае канал разведки системы воздействий формально можно представить в виде

$$M\times S_{\text{conf}}^{\text{набл}}.$$

В процессе функционирования канала разведки формируется, так называемая «картина наблюдения» (процесс $M\times S_{\text{conf}}^{\text{набл}}\times t_{\text{набл}}$), идентифицирующая с определенной вероятностью (достоверностью) элементы S_{conf}. Идентификация, как правило, ведется по признаковому пространству каждого объекта. В соответствии с наблюдаемыми признаками, каждый элемент конфигурации $S_{\text{conf}}^{\text{набл}}$ относится к некоторому заранее заданному классу с определенной степенью достоверности. Процесс такого сопоставления, а также задачи выбора множества признаков и методики классификации объектов $S_{\text{conf}}^{\text{набл}}$ за время $t_{\text{набл}}$ относятся к самостоятельным научным задачам, решаемым на основе теорий кластеризации и классификации.

5.3.6. Формализация системы управления связью и системы дестабилизирующих воздействий

Функционирование системы связи, как правило, сопровождается динамическим или стохастическим изменением значений множества входных параметров на различных ее уровнях $X=\cup X_l$, $X_l = R_l\times\chi_l\times V_l$, которые в условиях информационного конфликта, в первую очередь, определяются множеством преднамеренных воздействий на различных уровнях $V=\cup V_l$.

Для обеспечения выполнения критерия (5.32) по соответствию качества связи заданным значениям, на протоколы П со стороны системы управления связью оказывается множество управляющих воздействий $U=\cup U_l$, которые, как правило, связаны или с распределением ресурсов R_l на различных уровнях, или с изменением параметров Ω алгоритмов A, на основе которых функционируют протоколы системы связи.

Управление системой связи характеризуется рядом особенностей. Для динамической модели системы связи наиболее существенными из них являются [1]:

- наличие совокупности направлений связи, в которых обеспечивается обмен сообщениями абонентов и узлов;
- возможность использования различных путей прохождения сообщений в рамках одного направления связи;
- зависимость множества реализуемых информационных путей передачи информации Λ от транспортной структуры $\{Z, K\}$ и конфигурации системы связи S_{conf};
- инерционность процессов управления состояниями транспортной и информационной структур, а также процессов изменения конфигурации системы связи.

Множество управляющих воздействий U направляется на перестройку топологии системы связи $Z\times K$, преобразование структур транспортной S и информационной Λ сетей, управление резервами R, протоколами средств связи П (режимами помехозащиты, рабочими частотами, мощностью передачи, видом формируемых сигналов и способом их обработки) и т.д.

Особенностью построения системы управления связью является то, что она, с одной стороны, функционально разобщена по уровням OSI (что приводит к тому, что система управления каждого уровня стремится обеспечить выполнение только своих задач), а, с другой стороны, она должна обеспечивать требуемое качество связи $Q^{\text{треб}}$ в интересах информационно-управляющей системы более высокого уровня. Иерархический характер управления означает, что в рамках одного состояния системы связи, определяемого старшим элементом подсистемы управления (высшего уровня иерархии), допускается управление младшими элементами и состояниями системы связи на более низких уровнях иерархии. Процессы управления различных уровней иерархии различаются по масштабности и сложности решаемых задач, по степени их влияния на систему связи и информационно-управляющую систему в целом, по динамичности, уровню автоматизации и другим показателям. Все вышеуказанное, а также принцип функциональной независимости уровней, введенный моделью OSI, позволяют для широкого спектра случаев, рассматривать управление ресурсами отдельного уровня независимо от других.

5.3.7. Формализация особенностей управления системой связи и воздействия на нее как на многоуровневую систему

Традиционно процессы функционирования системы связи, управления ее ресурсами и конфликт с системой дестабилизирующих воздействий рассматри-

ваются на каком-либо одном из уровней модели OSI. Анализ особенностей дестабилизирующих воздействий на систему связи [9, 10] показал, что преднамеренным воздействиям, в основном, подвергаются четыре нижних уровня транспортной подсистемы модели OSI.

Как правило, для системы связи рассматривают либо одноуровневый информационный конфликт (рис. 5.6 а, б), либо многоуровневые эффекты на различных уровнях системы связи в условиях одноуровневого воздействия (рис. 5.6 в). Вместе с тем, для перспективных систем дестабилизирующих воздействий нельзя исключать применения разноуровневого комплексного воздействия (рис. 5.6 г). При этом наиболее вероятным сценарием, на взгляд автора, является использование на нижних уровнях некритичных динамических воздействий ($Q_1(V_1)>Q_1^{треб}$), эффект от которых отображается на более верхние уровни ($V_1 \to X_1 \to П_1 \to Y_1 \to X_2 \to П_2 \to \ldots$) и «раскачивает» систему связи, переводя ее в погранично-устойчивое состояние. Одновременно, на верхних уровнях (например, на сетевом или на транспортном) используются точечные воздействия V_i, ориентированные на блокировку или нарушение функционирования критических протоколов связи, что приводит к потере устойчивости всей системы $Q(V_1, V_i)<Q^{треб}$ (рис. 5.6 б).

Наличие одновременных разноуровневых воздействий, а также глубокая функциональная взаимосвязь между уровнями OSI в системе связи требует реализации единой стратегии управления $U=\cup U_l$ на различных уровнях модели OSI. Реализация такого управления требует создания системы управления, которая бы обеспечивала управление каждым из уровней с квазиоптимальной стратегией суммарных затрат ресурсов всех уровней $R(U, V)\to\min$. Причем данное управление должно быть адаптивным к преднамеренным воздействиям V.

Примерами такого многоуровневого управления ресурсами могут быть: применение корректирующего кодирования с целью избегания многократного повышения полосы частот канала в алгоритмах с адаптивным ШПС для обеспечения заданной достоверности приема сигналов; изменение маршрутов передачи в сети для избегания передачи данных по каналам, на которые оказываются преднамеренные воздействия, с целью исключить растрату частотно-временных и энергетических ресурсы физического и канального уровня на обеспечение требуемой помехозащищенности подавляемых каналов и т.д.

Управление U, в общем случае, должно соответствовать принципу компенсации из теории управления по отношению к преднамеренным воздействиям V и условиям среды χ. При этом компенсация может быть:

- *активной* за счет непосредственной выдачи управляющих воздействий U_l на соответствующие объекты управления (см. выше);
- *пассивной* за счет внесения некоторой избыточности (количественной, функциональной или временной) в алгоритмы A или в их параметры Ω протоколов П, в структуру взаимодействия протоколов, а также в ресурсы системы связи R. Это позволит обеспечить выполнение требований $Q \geq Q^{треб}$ в более широком диапазоне входных параметров

$X=R\times\chi\times V$ и сократить интенсивность выдачи управляющих воздействий U.

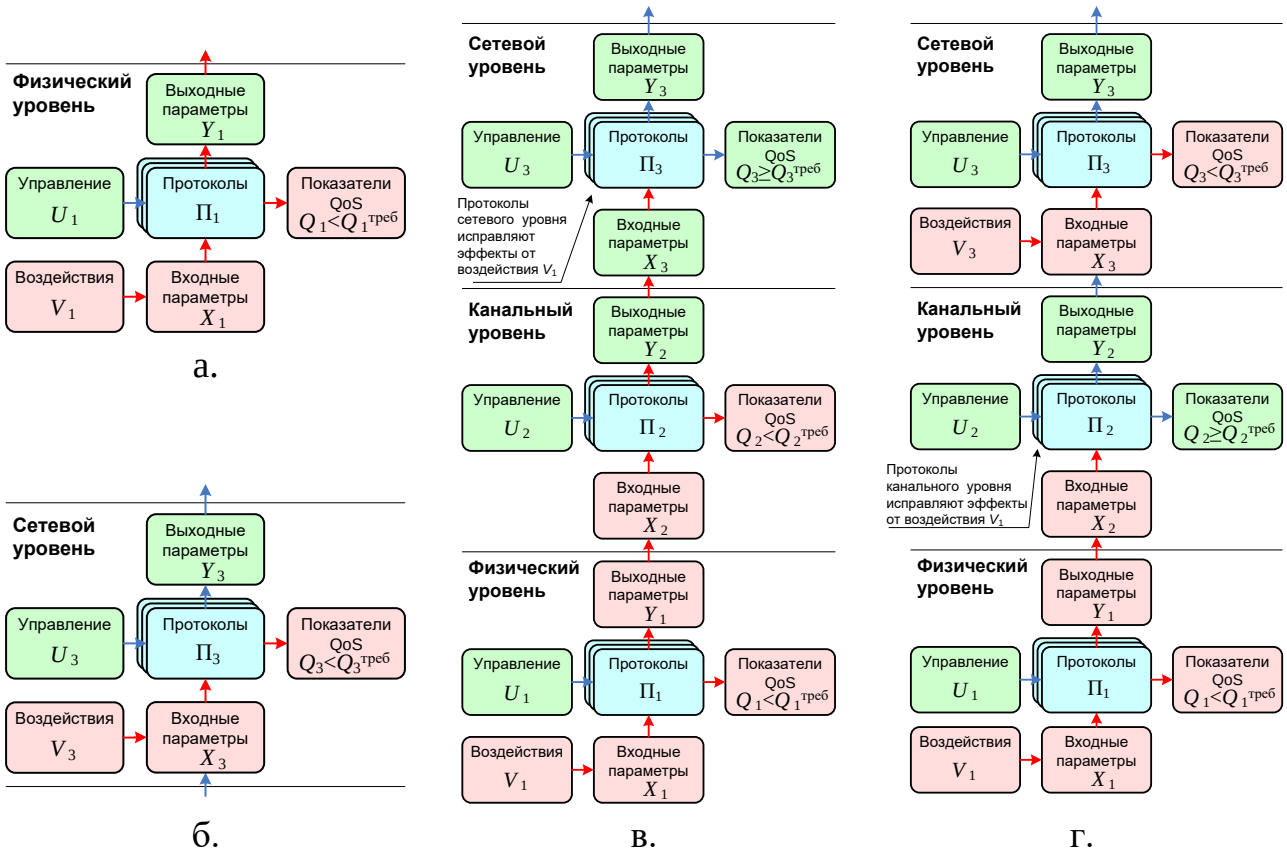

Рис. 5.6. Информационный конфликт по уровням воздействия:
а) воздействие только на физическом уровне (например, РЭП);
б) воздействие только на сетевом уровне (например, DDOS-атаки);
в) оценка эффектов от одноуровневого воздействия на физическом уровне (например, эффекты от РЭП приводят к потери достоверности приема, которую не способны исправить протоколы физического и канального уровня, но за счет перемаршрутизации на сетевом уровне эффекты от воздействия исправляются);
г) разноуровневое комплексное воздействие (по аналогии с предыдущим случаем, только дополнительное использование ИТВ на сетевом уровне приводит к нестабильному функционированию протоколов маршрутизации, при этом доставка пакетов становится невозможна).

Как показано в работе [227], эффективность управления многоуровневой системы, каковой является система связи, зависит от соотношений между глобальной и локальными целями функционирования на каждом из уровней. В самом деле, стремление локальных систем управления каждого уровня OSI минимизировать свои собственные целевые функции $R_l(U_l)\rightarrow\min \mid Q_l\geq Q_l^{треб}$ может не приводить к достижению глобального оптимума $R(U)\rightarrow\min$. В связи с этим, может возникнуть межуровневая несогласованность (конфликт) между локально принимаемыми решениями. Принципы координации иерархических

систем, представленные в работе [227], показывают, что при принятии локальных решений необходимо выполнение условий координируемости.

В общем случае в многоуровневой системе возникают два вида конфликтов [227]:

- межуровневые;
- внутриуровневые.

Межуровневый конфликт есть конфликт между двумя различными уровнями в многоуровневой системе, который характеризуется невозможностью достижения глобальной цели за счет реализации локальных задач уровней. Например, если глобальной целью является максимизация пропускной способности системы, а локальной цель – минимизация затрат ресурса на всех уровнях, то возникает конфликт между уровнями [227].

Внутриуровневый конфликт представляет собой конфликт в пределах отдельного уровня. Данный конфликт возникает, когда достижению локальной цели уровня препятствует некоторый элемент [227]. Особенности таких конфликтов рассмотрены в работах Г.А. Угольницкого [228], А.Б. Усова [229] и У. Деттмера [265].

В связи с указанными особенностями управления в системе связи к перспективным способам преднамеренного воздействия можно отнести многоуровневые или одноуровневые воздействия, ориентированные на:

- порождение или развитие межуровневых конфликтов в системе связи;
- порождение или развитие внутриуровневых конфликтов в системе связи.

Воздействия, ориентированные на внутриуровневые конфликты в системе связи, могут быть реализованы за счет нарушения логики работы или функциональной блокировки отдельных «ключевых» протоколов или элементов системы связи на данном уровне. Воздействия, ориентированные на межуровневые конфликты, могут быть реализованы за счет учета отображений эффекта от воздействия на вышестоящие уровни системы или с использованием многоуровневых воздействий, ориентированных на «ключевые» протоколы системы связи.

Как показано выше, система связи является *эффективной* в случае, если ее показатели качества верхнего (прикладного) уровня Q_7, получаемые в результате свертки

$$Q_1 \to Q_2 \to \ldots \to Q_i \to \ldots \to Q_7,$$

имеют значения не ниже требуемого, то есть выполняется критерий $\forall \{q_7 \geq q_7^{\text{треб}}\}$, $q_7 \in Q_7$.

По аналогии, введем понятие *эффективных условий функционирования* – условий $X_{\text{эф}} = \cup X_l$ ($X_l = R_l \times \chi_l \times V_l$), которые при управлении системой связи $U = \cup U_l$ обеспечивают выполнение критерия эффективности функционирования $\forall \{q_7 \geq q_7^{\text{треб}}\}$.

Существование таких эффективных условий определяет область *неэффективных воздействий* – то есть воздействий $V_{нэф} = \cup V_l$, которые при управлении $U = \cup U_l$ не способны вывести систему за пределы эффективного функционирования, то есть $Q(U, X_{эф}(V_{\text{нэф}})) \geq Q^{\text{треб}}$. Другими словами, эффективные усло-

вия функционирования системы связи соответствуют условию неэффективных воздействий.

В настоящее время в модели OSI принят *классический принцип независимости протоколов системы связи на различных уровнях ее функционирования*. В основу классического принципа многоуровневого функционирования, в соответствии с моделью OSI, положены два положения (рис. 5.7).

1) Протоколы вышестоящих уровней $П_l$ и система управления ими U_l должны обеспечивать исправление неэффективных выходных параметров (выходных условий) нижестоящих уровней $Y_{l\text{-}1\ нэф} \rightarrow X_{l\ эф}$

$$\varphi_l : Y_{l-1\,нэф} \xrightarrow{П_l} \left[\begin{array}{l} X_{l\,эф}; \\ X_{l\,нэф}. \end{array} \right. \qquad (5.34)$$

где $X_{l\ эф}$ – соответствует случаю, когда протоколы $П_l$ исправляют неэффективные условия функционирования предыдущего уровня; $X_{l\ нэф}$ – когда не исправляют. При этом:

$$X_{l\,нэф} = \bigcup_{П_l} X_{l,\pi\,нэф}, \quad X_{l\,эф} = \bigcup_{П_l} X_{l,\pi\,эф}, \text{ и в итоге } X_l = X_{l\,эф} \bigcup X_{l\,нэф}.$$

2) На своем уровне функционирования протоколы $П_l$ функционально независимы от нижестоящих уровней $П_{l\text{-}1}$ и должны обеспечивать требуемую эффективность функционирования:

$$f_l : \{t,\ s_l, X_{l\,эф},\ U_l,\ A_l\} \xrightarrow{П_l} Q_l \,|\, Q_l \geq Q_l^{треб}. \qquad (5.35)$$

Выражение (5.34) позволяет сформировать следствие, на первый взгляд кажущееся логичным – если выходные параметры протоколов нижестоящего уровня $Y_{l\text{-}1\ нэф}$ являются эффективными $Y_{l\text{-}1}=Y_{l\text{-}1\ эф}$, то и условия функционирования протокола вышестоящего уровня являются эффективными:

$$Y_{l-1\,эф} \Rightarrow X_{l\,эф}, \qquad (5.36)$$

откуда, распространяя данный вывод на все уровни системы связи, получаем, что эффективные условия 1-го уровня служат причиной эффективных условий всех последующих уровней.

$$X_{1\,эф} \Rightarrow Y_{1\,эф} \Rightarrow \ldots \Rightarrow Y_{l-1\,эф} \Rightarrow X_{l\,эф} \Rightarrow \ldots \Rightarrow Y_{7\,эф}. \qquad (5.37)$$

Вместе с тем, из практики связи известно, что существуют режимы функционирования протоколов связи, которые являются неэффективными, но при этом соблюдаются условия эффективного функционирования 1-го уровня: $X_{1\ эф} \Rightarrow X_{i\ нэф}$. Таким образом, следствие (5.37) – не выполняется.

Как правило, объяснение наличия таких условий лежит в области независимости функциональных уровней системы связи и, якобы, невозможности формирования отдельных условий текущего уровня из условий функционирования предыдущего уровня. Однако, по мнению автора, это не совсем верно.

Введем *принцип оценивания устойчивости системы связи на основе многоуровневой функциональной взаимосвязи ее элементов*, который направлен на разрешение сформулированного выше противоречия (рис. 5.7).

Для устранения данного противоречия необходимо изменить строгость допущений (5.34), и ввести условия, когда эффективные выходные параметры

протоколов нижестоящих уровней $Y_{l\text{-}1\,эф}$ могут определять неэффективные условия функционирования протоколов вышестоящего уровня $X_{l\,нэф}$:

$$\begin{cases} \varphi_l : Y_{l-1\,нэф} \xrightarrow{\Pi_l} \left[\begin{array}{l} X_{l\,эф}; \\ X_{l\,нэф}; \end{array} \right. \\ \varphi_l : Y_{l-1\,эф} \xrightarrow{\Pi_l} \left[\begin{array}{l} X_{l\,эф}; \\ X_{l\,нэф}. \end{array} \right. \end{cases} \tag{5.38}$$

Отсюда следует оригинальный вывод о существовании эффективных выходных параметров $Y_{l\text{-}1\,эф}$ и условий функционирования $X_{l\text{-}1\,эф}$ нижестоящих уровней, которые являются причиной неэффективных условий $X_{l\,нэф}$ на вышестоящих уровнях системы связи:

$$\begin{aligned} &\exists Y_{l-1\,эф} \Rightarrow X_{l\,нэф}, \\ &\exists X_{l-1\,эф} \Rightarrow Y_{l\,эф} \Rightarrow X_{l\,нэф}. \end{aligned} \tag{5.39}$$

Распространяя данный вывод на все L уровни системы связи получаем, что существуют такие эффективные условия функционирования любого из уровней $X_{i\,эф}$, которые могут служить причиной неэффективных условий функционирования $X_{j\,эф}$ ($j>i$) любого из последующих уровней. В случае, если эти неэффективные условия не исправляются вышестоящим уровнем функционирования, система связи оказывается функционально подавленной:

$$\exists X_{1\,эф} \Rightarrow Y_{1\,эф} \Rightarrow X_{2\,эф} \Rightarrow ... \Rightarrow X_{l\,нэф} \Rightarrow Y_{l\,нэф} \Rightarrow ... \Rightarrow X_{7\,нэф}. \tag{5.40}$$

Наличие такого эффекта для сетевого уровня проиллюстрировано на рис. 5.7. В общем случае причиной создания таких неэффективных условий могут быть как внутрисистемные конфликты в системе связи, так и преднамеренные воздействия на систему связи.

Для преднамеренной реализации вышеприведенных условий неэффективного функционирования системы связи можно предложить три базовых варианта воздействия (рис. 5.8).

1) Воздействие на нижестоящем уровне V_i, которое неэффективно на i-ом уровне (то есть не ведет к снижению $Q_i<Q_i^{треб}$), но за счет отображения $V_{i\,нэф}\to X_{i\,эф}\to Y_{i\,эф}\to\ldots\to X_{j\,нэф}\to Y_{j\,нэф}$ на вышестоящий j-ый уровень системы связи формирует его неэффективную среду $X_{j\,нэф}$, приводящую к критическому падению качества функционирования этого уровня ($Q_j<Q_j^{треб}$) или всей системы ($Q<Q^{треб}$) – см. рис. 5.8а.
2) Совокупность воздействий $V=\cup V_i$ на различных уровнях, которые по отдельности неэффективны, но за счет их отображения на вышестоящие уровни создает эффект неэффективных условий среды $X_{j\,нэф}$ на вышестоящем j-ом уровне (рис. 5.8б):

$$\begin{array}{ccccccccccccc} & & & & V_{i\text{-}1\,нэф} & & & & V_{i\,нэф} & & & & \\ & & & & \downarrow & & & & \downarrow & & & & \\ X_{1\,эф} & \to & Y_{1\,эф} & \to & \ldots & \to & X_{i\text{-}1\,эф} & \to & Y_{i\text{-}1\,эф} & \to & X_{i\,эф} & \to & Y_{i\,эф}\ldots\to X_{j\,нэф}\to Y_{j\,нэф} \end{array}$$

Классический подход к оцениванию устойчивости СС СН основан на положении о независимости функционирования протоколов на различных уровнях OSI

Протоколы вышестоящих уровней Π_l должны обеспечивать эффективные параметры функционирования $X_{l\ эф}$ в условиях неэффективных выходных параметров нижестоящих уровней $Y_{l\text{-}1\ нэф}$

$$\varphi_l : Y_{l-1\,нэф} \xrightarrow{\Pi_l} \left[\begin{array}{l} X_{l\,эф} \\ X_{l\,нэф} \end{array} \right.$$

На каждом уровне протоколы Π_l функционально независимы от нижестоящих уровней $\Pi_{l\text{-}1}$ и должны обеспечивать требуемую эффективность функционирования

$$f_l : \{t,\ s_l, X_{l\,эф},\ U_l,\ A_l\} \xrightarrow{\Pi_l} Q_l \,|\, Q_l \geq Q_l^{треб}$$

Следствие: если выходные параметры протоколов нижестоящего уровня $Y_{l\text{-}1\ нэф}$ являются эффективными $Y_{l\text{-}1}=Y_{l\text{-}1\ эф}$, то и условия функционирования протокола вышестоящего уровня являются эффективными

$$Y_{l-1\,эф} \Rightarrow X_{l\,эф}$$

Эффективные условия 1-го уровня служат основой эффективных условий функционирования всех последующих уровней

$$X_{1\,эф} \Rightarrow Y_{1\,эф} \Rightarrow \ldots \Rightarrow Y_{l-1\,эф} \Rightarrow X_{l\,эф} \Rightarrow \ldots \Rightarrow Y_{7\,эф}$$

Принцип оценивания устойчивости СС СН на основе многоуровневой функциональной взаимосвязи ее элементов

Выдвигаемая гипотеза

Эффективные выходные параметры протоколов нижестоящих уровней $Y_{l\text{-}1\ эф}$ могут определять неэффективные условия функционирования протоколов вышестоящего уровня $X_{l\ нэф}$

$$\begin{cases} \varphi_l : Y_{l-1\,нэф} \xrightarrow{\Pi_l} \left[\begin{array}{l} X_{l\,эф}; \\ X_{l\,нэф}; \end{array} \right. \\ \varphi_l : Y_{l-1\,эф} \xrightarrow{\Pi_l} \left[\begin{array}{l} X_{l\,эф}; \\ X_{l\,нэф}. \end{array} \right. \end{cases}$$

Следствие 1: существуют эффективные выходные параметры $Y_{l\text{-}1\ эф}$ и условия функционирования $X_{l\text{-}1\ эф}$ нижестоящих уровней, которые являются причиной неэффективных условий $X_{l\ нэф}$ на вышестоящих уровнях системы связи

$$\exists Y_{l-1\,эф} \Rightarrow X_{l\,нэф}$$

$$\exists X_{l-1\,эф} \Rightarrow Y_{l\,эф} \Rightarrow X_{l\,нэф}$$

Следствие 2: существуют такие эффективные условия функционирования любого из уровней $X_{i\ эф}$, которые могут служить причиной неэффективных условий функционирования $X_{j\ эф}$ $(j>i)$ любого из последующих уровней

$$\exists X_{1\,эф} \Rightarrow \ldots \Rightarrow Y_{l-1\,эф} \Rightarrow X_{l\,нэф}$$

Эмерджентные эффекты, выявленные путем использования принципа оценивания устойчивости СС СН на основе многоуровневой функциональной взаимосвязи ее элементов

Пример существования неэффективных условий функционирования для сетевого уровня

Рис. 5.7. Принцип оценивания устойчивости сситемы связи на основе многоуровневой функциональной взаимосвязи ее элементов

3) Одиночные воздействия V_i или их совокупность $V=\cup V_i$ на различных уровнях, приводящие к возникновению и развитию внутрисистемных конфликтов в системе связи как внутри отдельного уровня (рис. 5.8в), так и между уровнями функционирования (рис. 5.8г).

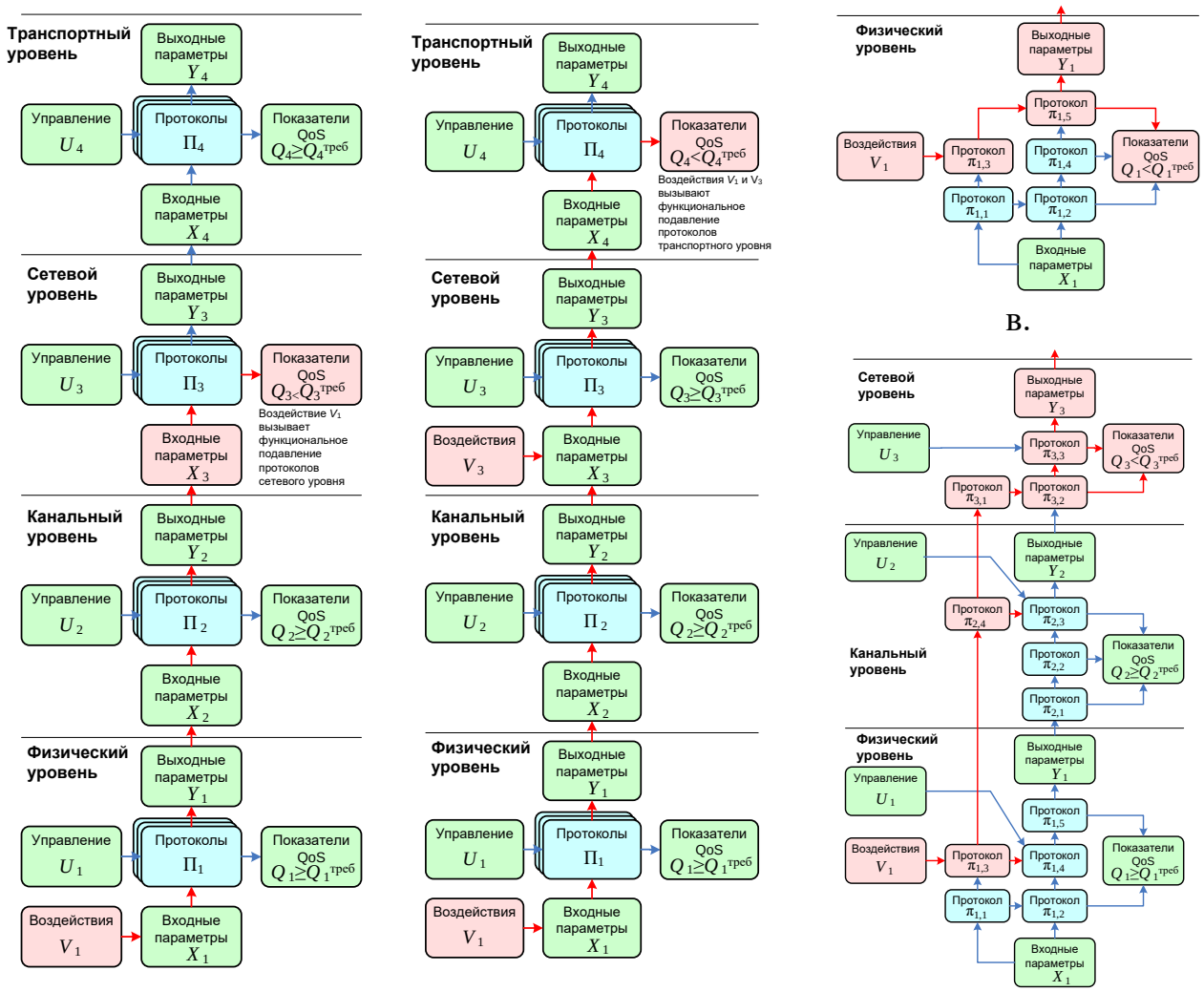

Рис. 5.8. Новые варианты дестабилизирующих воздействий на систему связи:
а) воздействия на нижестоящем уровне, которые за счет отображения на вышестоящий уровень системы связи формирует его неэффективную среду функционирования;
б) совокупность воздействий на различных уровнях, которые по отдельности неэффективны, но за счет их отображения на вышестоящие уровни создает эффект неэффективных условий среды;
в) воздействия, приводящие к возникновению и развитию внутрисистемных конфликтов в системе связи на одном уровне;
г) воздействия, приводящие к возникновению и развитию внутрисистемных конфликтов в системе связи на различных ее уровнях

В случае разработки подобных базовых вариантов воздействий, их реализация будет носить скрытно-бескомпроматный характер, так как идентификация факта такого воздействия потребует от системы управления связью наблю-

дения не только за параметрами Q_l и Y_l на отдельных уровнях, но и наблюдения за поведением отображений ψ_l, γ_l, f_l внутри каждого из уровней, а также за поведением отображений φ_l между уровнями.

5.3.8. Итоговые выводы

Таким образом, любая система связи может быть описана как динамическая многоуровневая иерархическая система, функционирующая в сложной параметрической среде, при этом совокупность протоколов системы связи фактически является частью двух контуров управления – системы управления связью и системы управления воздействиями, которые преследуют антагонистические цели функционирования. Такая функциональная дуальность определяет информационный конфликт вышеуказанных систем управления, который происходит и развивается в приложении ко всем 7-ми уровням модели OSI. Дополнительно к вышеуказанному надо отметить, что тесная функциональная взаимосвязь протоколов между собой как в горизонтальной области – в соответствии с задачами отдельного уровня OSI, так и в вертикальной – в соответствии с задачами межуровневого взаимодействия, может служить основой для постановки новых научных задач. В области информационного противоборства – формирование воздействий нового типа, ориентированных на формирование и развитие внутрисистемных конфликтов в системе связи, а в области управления связью – выработку новых принципов координации отдельных систем управления уровнями OSI, а также распределения ресурсов связи на каждом из уровней с учетом их межуровневого взаимодействия.

Выводы по пятой главе

Представленное в данной главе развитие модели процесса конфликтного взаимодействия системы связи со средствами разведки и дестабилизирующих воздействий (рис. 4.2) основано на учете фактора многоуровневости системы связи и ее представления как иерархической системы в соответствии с уровнями модели OSI (рис. 5.5), элементами каждого из которых являются отдельные протоколы (рис. 5.2). Данная модель не только позволяет описать противоборство двух сторон – системы связи и системы дестабилизирующих воздействий, но и выявить внутренние локальные конфликты за ресурсы между различными протоколами внутри системы связи, обосновать необходимость координации систем управления связью на различных уровнях модели OSI, вскрыть возможности нападающей стороны по реализации новых типов бескомпроматных воздействий на систему связи, основанных на преднамеренном формировании и поддержании в ней локальных конфликтов, нестационарных и переходных процессов, а также неэффективных условий функционирования.

Вместе с тем, декомпозиция системы связи по уровням модели OSI не позволяет в полной мере учесть пространственно-распределенную структуру системы связи, направления и важность передаваемых информационных потоков, а также пространственное размещение средств разведки и нападения. В связи с этим, дальнейшим направлением развития представленной в данной главе модели является формирование топологической модели системы связи.

6. Топологическая модель системы связи в условиях дестабилизирующих воздействий и ведения разведки

6.1. Анализ понятия устойчивости системы связи

6.1.1. Системный подход к определению понятия устойчивость

Теория систем рассматривает различные системы произвольной природы, которые могут быть формализованы в виде совокупности входных, выходных и внутренних параметров, параметров среды, элементов, их состояний и связей между ними, а также множества формальных операторов, описывающих как взаимосвязь указанных параметров и элементов между собой, так и движение (развитие) системы во времени и в пространстве состояний [384].

В теории систем указывается, что системам присущи определенные свойства, через которые описываются те или иные качественные изменения системы при воздействии на нее возмущающих воздействий. К таким свойствам системы относятся следующие.

Надежность – способность системы сохранять свои характеристики при изменении параметров среды [385].

Живучесть – способность системы сохранять значение своих других показателей при разрушении части ее структуры [385].

Помехоустойчивость – способность системы выполнять свои функции в условиях помех [387].

Обобщением этих свойств является понятие устойчивости.

Устойчивость – способность системы возвращаться в исходное состояние или в состояние равновесия после того, как она была из этого состояния выведена под влиянием внешних возмущающих воздействий. При этом под *равновесием* понимается состояние системы, которое оно может сохранять сколь угодно долго в отсутствие внешних возмущающих воздействий [384, 385].

В настоящее время для различных типов формального представления систем, разработаны различные варианты формализации понятия устойчивости. При этом в наибольшей степени разработанными являются критерии устойчивости для динамических систем (устойчивость по Ляпунову, устойчивость по Пуассону, устойчивость по Лагранжу, асимптотическая устойчивость), гидродинамических систем (критерий устойчивости Эйлера, неустойчивости Рэлея-Тейлора, Рихтмайера-Мешкова, Кельвина-Гельмгольца, Рэлея-Плато). Кроме этого, введено понятие вероятностной устойчивости для систем формализованных на основе подходов теории вероятности, а также критерий устойчивости для систем формализованных на основе теоретико-множественного подхода [384].

Наиболее общее формальное определение устойчивости системы дано в работах [384, 386].

Пусть $\Omega : A \to B$ – некоторое отображение Ω множества A в множество B, Θ_A и Θ_B – ограниченные подмножества множеств A и B соответственно, точка (a, b) лежащая в пространстве $A \times B$, при этом $b=\Omega(a)$. Точка (a, b) будет являться устойчивой относительно Θ_A и Θ_B в том и только в том случае, когда для любого $\eta \in \Theta_b$ существует $\mu \in \Theta_a$ такое, что для любого $\pi \in \mu$ будет выполнятся условие $\Omega(\pi) \in \eta$:

$$(\forall \eta \in \Theta_b)(\exists \mu \in \Theta_a) \Rightarrow \left(\forall \pi \middle| \pi \in \mu \to \Omega(\pi) \in \eta\right),$$

где $\Theta_a \subset \Theta_A$ и $\Theta_b \subset \Theta_B$ – окрестности точки (a, b) в множествах A и B соответственно.

Такой подход, основанный на определении устойчивости системы, как свойства траектории ее движения в пространстве состояний постоянно возвращаться в некоторую окрестность точки ее равновесного состояния, для динамических систем сформулирован в виде критерия устойчивости Ляпунова [220], который получил широкое распространение для оценки устойчивости технических систем.

В технических системах, зачастую, возврат в нужное состояние происходит за счет реализации функций управления (см. подраздел 5.3.7). При этом для реализации адекватного управления необходимо знать текущее состояние системы и то состояние в которою систему нужно перевести. В связи с этим свойство устойчивости системы оказывается тесно связано со свойствами управляемости и наблюдаемости (см. подраздел 5.3.5).

Наблюдаемость – это свойство системы, характеризующее возможность определения ее начального или текущего состояния [388].

Управляемость – это свойство системы, характеризующее возможность перевода её из заданного в требуемое состояние путем подачи на ее вход управляющих воздействий [388].

Необходимо отметить, что характеристика способности системы противостоять негативным условиям внешней среды не ограничивается свойством ее устойчивости. Устойчивость является частным случаем свойства адаптивности систем, а адаптивность – частным случаем свойства их самоорганизации [384, 388].

Адаптивность (*адаптируемость*) – способность системы изменять свое поведение с целью сохранения, улучшения или приобретения новых характеристик в условиях воздействий изменяющейся среды [387].

Самоорганизуемость – способность системы самостоятельно вследствие внутренних процессов изменять свое поведение или структуру приспосабливаясь к изменяющимся условиям среды, сохраняя при этом свою целостность [384, 388].

При этом, свойство самоорганизации обобщает широкий класс системных свойств, преимущественно сложных систем, направленных на их развитие в интересах повышения приспосабливаемости к внешней среде: адаптивность, самоприспосабливаемость, самовосстановление, самообучение, самовоспроизведение и т.д. [384, 388].

6.1.2. Понятие устойчивости, учитывающее особенности функционирования системы связи и дестабилизирующие воздействия на нее

Анализ функционирования СС СН и ее составных частей (отдельных подсетей и ТКС), представленный в подразделе 1.1.4 настоящей работы, показывает, что основным свойством СС СН, характеризующим качество ее функционирования в условиях дестабилизирующих воздействий (преднамеренного и непреднамеренного характера) является устойчивость.

Устойчивость системы связи – способность системы выполнять свои функции при выходе из строя части ее элементов в результате воздействия дестабилизирующих факторов [66].

Дестабилизирующие факторы – воздействия на систему связи, источником которых являются физические или технологические процессы внутреннего или внешнего характера, приводящие к выходу из строя элементов системы связи или к нарушению их функционирования.

В соответствии с этим определением различают:

- *внутренние дестабилизирующие факторы*, определяющие свойства надежности элементов СС СН и обусловленные их внутренними свойствами, зависящими от материала, структуры, режимов работы, условий эксплуатации и т.д.;
- *внешние дестабилизирующие факторы*, определяющие свойства живучести и помехоустойчивости элементов СС СН и обусловленные их способностью продолжать функционировать с требуемым качеством в условиях воздействия негативного факторов внешней среды, имеющих физическую, радиоэлектронную, информационную, либо другую природу.

Устойчивость является одним из основных свойств СС СН, при этом терминологические отличия в оценке устойчивости СС СН, в соответствии с текущими руководящими документами, состоят в том, что в качестве внешних дестабилизирующих факторов рассматриваются отдельно обычное и ядерное оружие противника, а также естественные и преднамеренные помехи. При этом устойчивость СС СН рассматривается как интегральное свойство (рис. 1.4), которое в соответствии с работой [76] декомпозируется на:

- *живучесть* – способность СС СН обеспечивать связь с требуемым качеством в условиях воздействия на нее обычного и ядерного оружия;
- *помехоустойчивость* – способность СС СН обеспечивать связь с требуемым качеством в условиях воздействия на нее всех видов помех;
- *надежность* – способность СС СН обеспечивать связь с требуемым качеством, сохраняя во времени требуемые значения эксплуатационных показателей, технического обслуживания, восстановления и ремонта.

Однако, анализ воздействующих на СС СН дестабилизирующих факторов, проведенный в работах Е.Е. Исакова [43, 63], показывает, что понятие устойчивости не может быть формализовано только на основе терминологиче-

ского базиса теорий живучести, помехозащищенности и надежности. Например, в принятой терминологии в понятие устойчивости не включаются прямые и косвенные взаимосвязи между свойствами СС СН по пропускной способности с одной стороны и реально сопутствующие им значения мобильности, боевой готовности, доступности, скрытности, управляемости с другой [43]. Фактически это означает, что для СС СН, функционирующей в особых условиях, перечисленные выше свойства не учитываются при формализации показателей ее устойчивости. Также определенную терминологическую нечеткость вносят работы, в которых происходит взаимоподмена понятий устойчивости, живучести и адаптивности, опять же без четкой формализации этих показателей. Кроме того, ряд авторов применительно к СС различают понятия функциональной и структурной устойчивости [27, 127].

При рассмотрении *структурной устойчивости* учитываются топология сети, межэлементные связи и надежностные характеристики элементов СС СН, вследствие чего задачи, связанные с анализом структурной устойчивости, можно свести к задачам надежности и устойчивости топологических структур в зависимости от конкретизации понятия «дестабилизирующее воздействие».

При рассмотрении *функциональной устойчивости* оценивается способность СС СН достигать цели своего функционирования, при этом особенности ее топологии и межэлементных связей учитываются опосредованно, так как предполагается, что в СС СН уже обеспечивается требуемый уровень связности работоспособных элементов.

Кроме того, существует понятие *информационной устойчивости* – способности СС СН как ОТС в динамике информационного конфликта своевременно, достоверно и скрытно передавать информацию пользователей и осуществлять управление собственными элементами СС СН с учетом дестабилизирующих воздействий на эти элементы со стороны противоборствующей ОТС [5].

Анализ известных работ в области устойчивости систем связи показал, что их подавляющая часть посвящена оценке структурной устойчивости. К наиболее известным таким работам следует отнести исследования: П.Н. Барашкова, А.П. Родимова, К.А. Ткаченко, А.М. Чуднова [1], А.В. Боговика, В.В. Игнатова [2], Е.Е. Исакова [43], Ю.Ю. Громова, В.О. Драчева, К.А. Набатова, О.Г. Ивановой [128], В.К. Попкова [63, 129], И.И. Пасечникова [130], М.М. Егунова, В.П. Шувалова [131], В.В. Грызунова [132], Д.А. Ковалькова [133], Д.А. Перепелкина [134, 135]. Исследование функциональной устойчивости сети с учетом ее динамической реакции на отказы и дестабилизирующие воздействия ведется гораздо меньшим количеством ученых. К русскоязычным специалистам, опубликовывавшим работы по данной тематике, можно отнести: А.Н. Назарова, К.И. Сычева [27], Д.А. Перепелкина [136-147], А.К. Канаева [148-154], С.П. Присяжнюка [156-158], В.В. Поповского [159-162], А.В. Лемешко, О.Ю. Евсеевой, А.А. Романюка [161-164], Р.Л. Михайлова [44, 165-169], а к иностранным ученым: M. Goyal [170-173], S.H. Hosseini [170-172], K. Trivedi, A. Shaikh, G. Choudhury [170], W. Xie [171, 172], K.K. Ramakrishnan [103], S. Amir, N. Biswajit [104], J. Pu, E. Manning, G.C. Shoja [176], S. Huang, K. Kitaya-

ma, F. Cugini, F. Paolucci, A. Giorgetti, L. Valcarenghi, P. Castoldi [177], H. Pun [178], N. Ayari, D. Barbaron, L. Lefevre, P. Primet [179], M.N. Dilber, A. Raza [180], D. Zhao, X. Hu, C. Wu [181], D. Sankar, D. Lancaster [182], C. Labovitz, A. Ahuja [183, 184], Y. Tsegaye, T. Geberehana [185], W Fang, C. Shanzhi, L. Xin, L. Yuhong [186].

6.2. Постановка задачи на моделирование

Целью данной части работы является разработка модели СС СН в условиях дестабилизирующих воздействий на нее, а также формализация показателя устойчивости. Отличительной чертой данной модели, которая составляет ее научную новизну, является учет длительности переходных режимов восстановления связи в СС СН при изменении ее структурных параметров вследствие влияния дестабилизирующих факторов. Именно эта черта отличает данную модель от уже известных вышеуказанных работ в области оценивания устойчивости сети. С учетом того, что в данном разделе рассматривается, прежде всего, сетевой уровень СС СН, модель формируется в формализме теории графов. Данная модель основана на модели, представленной в более ранней работе автора [166], которая, в свою очередь, основана на работах [2, 27, 43, 128, 131, 133, 187].

В основу топологической модели положена информация о пространственно-распределенной структуре СС СН и пространственной конфигурации средств разведки и дестабилизирующих воздействий. Именно эта информация с учетом энергетических и частотно-временных возможностей соответствующих средств позволяет сформировать исходные данные о возможностях ведения разведки и поражения узлов и каналов связи в СС СН.

Для формализации параметров СС СН при формировании модели введем следующие обозначения:

π – значение элемента множества A;

A – множество;

a – элемент множества A;

B – множество;

b – элемент множества B;

b_u – показатель посредничества вершины u в графе G;

b_u – показатель посредничества вершины u в графе G;

$C_{a\,\nu}$ – абсолютная пропускная способность (пакетов в секунду) ν-го элемента j-го пути информационного направления связи (ИНС);

$D(G)$ – диаметр графа G – длина максимального из кратчайших путей d_{ij}, которые можно сформировать между всеми вершинами графа G;

d_{ij} – количество участков сети («хопов») между узлом, обнаружившим отказ пути (узел i), и узлом, ответственным за переключение путей в ИНС (узел j);

E – эффективность сети;

E_z – эффективность сети после удаления из ее состава z-го элемента (узла или линии связи);

$F(\delta_i)$ – функция распределения степеней вершин графа G, определяемая вероятностью того, что вершина u_i в графе G имеет степень δ_i;

$G(u, v)$ – граф, формализующий сеть СС СН в виде множеств вершин $\{u\}$ и соединяющих их ребер $\{v\}$;

$G_{ИНС}$ – подграф, образованный из графа G элементами (вершинами и ребрами), входящими в конкретное ИНС;

H_z – показатель уязвимости сети относительно удаления z-го элемента СС СН (узла или линии связи);

i – счетчик;

j – счетчик;

K – требования к количеству путей в ИНС, в которых должно обеспечиваться требуемое качество обслуживания трафика;

k_i – количество работоспособных путей в i-ом ИНС;

k_{QoS} – количество работоспособных путей на заданном ИНС, обеспечивающих заданное качество обслуживания QoS;

$K_Г$ – коэффициент готовности СС СН;

$K_{Г\,i}$ – коэффициент готовности i-го ИНС;

m – количество ребер в графе;

$M(\bullet)$ – математическое ожидание случайной величины;

m_j – количество линий связи в j-ом пути в составе ИНС;

$m_{рз\,v}$ – количество независимых параметров v-го элемента СС СН, требуемых для для организации дестабилизирующего воздействия;

n – количество вершин в графе;

N – количество ИНС в СС СН;

n_j – количество узлов связи в j-ом пути в составе ИНС;

$P_{ИТВ\,i}$ – вероятность отказа i-го ИНС вследствие ИТВ;

$P_{ИТВ\,v}$ – вероятность отказа v-го элемента ИНС (линии или узла связи) вследствие ИТВ;

$P_{ИТВ\,v}*$ – вероятность успешной реализации ИТВ против v-го элемента СС СН при условии успешной разведки и вскрытия информационных параметров, т.е. при $P_{рз.инф\,v}=1$;

$P_{отк\,i}$ – вероятность отказа i-го ИНС вследствие естественных внутренних дестабилизирующих процессов, описываемых теорией надежности;

$P_{отк\,v}$ – вероятность отказа v-го элемента ИНС (линии или узла связи) вследствие естественных внутренних дестабилизирующих процессов, описываемых теорией надежности;

$P_{отк\,пак\,v}$ – отказ в обслуживании пакета в v-ом элементе j-го пути ИНС;

$P_{раб\,j}$ – вероятность работоспособного состояния j-го пути в составе ИНС;

$P_{раб.эл.\,v}$ – вероятность работоспособного состояния v-го элемента ИНС;

$P_{рз\,v}$ – вероятность разведки противником параметров v-го элемента СС СН;

$P_{рз\,v\,i}$ – вероятность разведки противником i-го параметра v-го элемента СС СН;

$P_{рз.вр\,v}$ – вероятность вскрытия временных параметров v-го элемента СС СН при ведении разведки;

$P_{\text{рз.инф}\,v}$ – вероятность вскрытия информационных параметров v-го элемента СС СН при ведении разведки;

$P_{\text{рз.пр}\,v}$ – вероятность вскрытия местоположения v-го элемента СС СН в пространстве при ведении разведки;

$P_{\text{рз.пр.РРТР}\,v}$ – вероятность вскрытия местоположения v-го элемента СС СН в пространстве средствами РРТР;

$P_{\text{рз.пр.ОЭР}\,v}$ – вероятность вскрытия местоположения v-го элемента СС СН в пространстве средствами ОЭР;

$P_{\text{рз.ст}\,v}$ – вероятность вскрытия структурных параметров v-го элемента СС СН при ведении разведки;

$P_{\text{рз.э}\,v}$ – вероятность успешного приема сигналов и вскрытия энергетических параметров v-го элемента СС СН при ведении разведки;

$P_{\text{РЭП}\,i}$ – вероятность подавления количества линий связи i-го ИНС большего, либо равного величине реберной связности x_v подграфа $G_{\text{ИНС}\,i}$;

$P_{\text{РЭП}\,v}$ – вероятность отказа ν-го элемента ИНС (линии или узла связи) вследствие РЭП;

$P_{\text{РЭП}\,v}$* – вероятность подавления v-го элемента СС СН средствами РЭП при условии его успешной разведки и вскрытия энергетических, временных и структурных параметров т.е. при $P_{\text{рз.э}\,v}=1$, $P_{\text{рз.вр}\,v}=1$ и $P_{\text{рз.ст}\,v}=1$;

$P_{\text{св}}$ – вероятность связности ИНС;

$P_{\text{св}\,i}$ – вероятность связности i-го ИНС в условиях воздействия на его элементы различных дестабилизирующих факторов;

$P_{\text{скр}\,v\,i}$ – вероятность скрытности i-го параметра v-го элемента СС СН;

$P_{\text{скр.вр}\,v}$ – вероятность обеспечения временной скрытности v-го элемента СС СН;

$P_{\text{скр.инф}\,v}$ – вероятность обеспечения информационной скрытности v-го элемента СС СН;

$P_{\text{скр.пр.РРТР}\,v}$ – пространственная скрытность местоположения v-го элемента СС СН по отношению к средствами РРТР;

$P_{\text{скр.пр.ОЭР}\,v}$ – пространственная скрытность местоположения v-го элемента СС СН по отношению к средствами ОЭР;

$P_{\text{скр.ст}\,v}$ – вероятность обеспечения структурной скрытности v-го элемента СС СН;

$P_{\text{скр.э}\,v}$ – вероятность обеспечения энергетической скрытности v-го элемента СС СН;

$P_{\text{У}\,i}$ – устойчивость i-го ИНС в СС СН;

$P_{\text{У ср}}$ – среднесетевая вероятность устойчивости ИНС в СС СН;

$P_{\text{ФП}\,i}$ – вероятность физического поражения узлов связи i-го ИНС большего, либо равного величине вершинной связности x_u подграфа $G_{\text{ИНС}\,i}$;

$P_{\text{ФП}\,v}$ – вероятность отказа ν-го элемента ИНС (линии или узла связи) вследствие его физического поражения;

$P_{\text{ФП}\,v}$* – вероятность физического поражения v-го элемента СС СН при условии его успешной разведки и вскрытия местоположения т.е. при $P_{\text{рз.пр}\,v}=1$;

$P_{ФПЭМИ\ v}$* – вероятность функционального поражения v-го элемента СС СН средствами ФП ЭМИ при условии вскрытия его местоположения при ведении разведки т.е. при $P_{рз.пр\ v}$ =1;

Q_k – качество обслуживания, обеспечиваемое путями (путем) на заданном ИНС;

$Q^{треб}$ – требуемый уровень качества обслуживания;

$T_{В\ i}$ – время восстановления i-го ИНС;

$T_{диагн\ i}$ – время диагностики отказа i-го ИНС;

$T_{зад\ v}$ – время задержки пакета в v-ом элементе j-го пути ИНС;

$T_{О\ i}$ – время между отказами в i-ом ИНС;

$T_{ож\ i}$ – время ожидания восстановления связи (удержания конфигурации) i-ого ИНС;

$t_{отк\ i}$ – время отказа i-го ИНС, заключающееся в утрате свойства связности;

$T_{перекл\ i}$ – время переключения информационных потоков с активных путей на резервные пути в составе i-го ИНС;

T_p – среднее время передачи пакета между отдельными узлами в СС СН;

$T_{рек\ i}$ – длительность реконфигурации путей или активации резервных путей в i-ом ИНС;

$T_{увед\ i}$ – время уведомления узла, ответственного за изменение конфигурации путей в i-ом ИНС;

u – вершина графа G;

v – ребро графа G;

x_u – показатель вершинной связности графа G;

x_v – показатель реберной связности графа G;

Y_u – коэффициент кластеризации вершины u;

z_j – количество элементов j-го пути в составе ИНС;

α_i – коэффициент важности i-го ИНС в сети;

δ_{min} – минимальная степень вершины;

δ_u – степень вершины u;

$\delta_{u\ \Sigma}$ – суммарная степень вершин, инцидентных вершине u;

λ_i – интенсивность трафика, передаваемого в i-ом ИНС;

$\varphi(i, j)$ – общее количество путей между вершинами i и j;

$\varphi(i, u, j)$ – количество путей между вершинами i и j, проходящих через вершину u;

η – значение элемента множества B в окрестности точки (a, b);

Θ_A – ограниченное подмножество множества A;

Θ_a – окрестность точки (a, b) на множестве A;

Θ_B – ограниченное подмножество множества B;

Θ_b – окрестность точки (a, b) на множестве B;

λ_i – интенсивность трафика, передаваемого в i-ом ИНС;

μ – значение элемента множества A в окрестности точки (a, b);

$\varphi(i, j)$ – общее количество путей между вершинами i и j;

$\varphi(i, u, j)$ – количество путей между вершинами i и j, проходящих через вершину u;

Ω – некоторое отображение.

6.3. Обоснование и формализация показателя устойчивости системы связи взаимосвязанного с показателями связности в теории графов

Ввиду того, что показатели устойчивости СС СН определяются параметрами графа, который ее формализует, определим логическую взаимосвязь показателей устойчивости СС СН с показателями связности из теории графов.

Введем основные понятия в соответствии с терминологическим базисом, приведенным в [27, 66, 188].

Маршрут – конечная чередующаяся последовательность вершин и ребер в графе $G(u, v)$, начинающаяся и оканчивающаяся на вершинах, являющимися концевыми. Маршрут называется открытым, если его концевые вершины различны, в противном случае он называется замкнутым.

Цепь – маршрут, в котором все его ребра (но не вершины) различны.

Путь – открытая цепь, то есть цепь, концевые вершины которой различны.

Степень вершины – число ребер, инцидентных этой вершине.

Информационное направление связи (ИНС) – совокупность линий и узлов связи, обеспечивающая связь между двумя оконечными пунктами сети.

Подграф ИНС ($G_{ИНС}$) – подграф, образованный из графа G элементами (вершинами и ребрами), входящими в данное ИНС.

Показатели связности СС СН могут быть определены через показатели связности графа $G(u, v)$, формализующего СС СН, в виде множеств вершин $\{u\}$ и соединяющих их ребер $\{v\}$ (рис. 6.1). При этом, как правило, в процессе формализации СС вершинами графа представляются такие узлы СС, к которым направлены не менее трех линий связи [66]. Показатели связности i-го ИНС определяются через показатели связности его подграфа $G_{ИНС\ i}$.

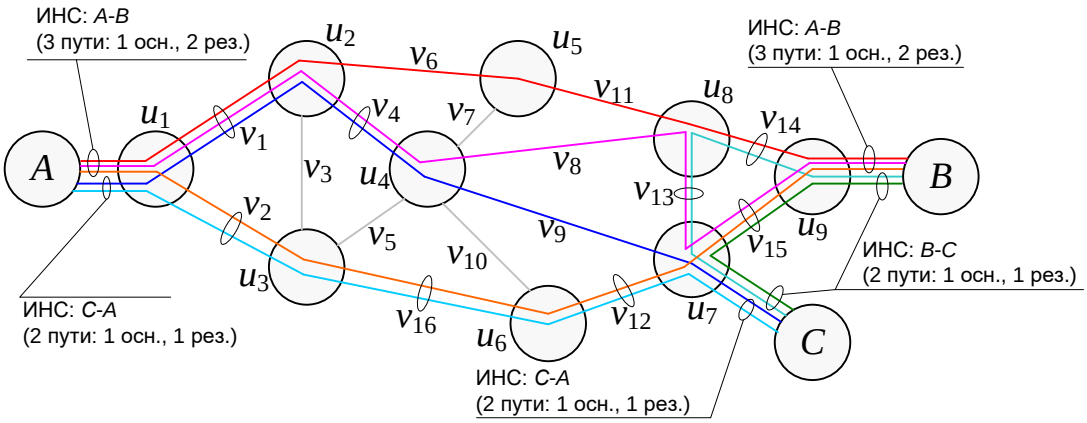

Рис. 6.1. Граф, формализующий СС СН

Для графа G различают показатели вершинной x_u и реберной x_v связности. Вершинная связность x_u определяет минимальное число вершин, удаление которых приводит к несвязному графу, а реберная связность x_v – минимальное число ребер, удаление которых приводит к тому же результату [188]. Минимальная степень вершины δ_{min} в графе G определяется минимальным количе-

ством ребер, инцидентных вершине. Показатели x_v, x_u и δ_{min} связаны между собой следующим неравенством:

$$x_u \leq x_v \leq \delta_{min} \leq 2m/n, \quad (6.1)$$

где: m – количество ребер в графе; n – количество вершин в графе.

Проведя анализ выражения (6.1), можно сделать вывод о том, что связность графа G нарушается при удалении x_u вершин или x_v ребер. Предельный случай для неравенства (6.1) наступает в случае, если граф сети полносвязный. В этом случае любая пара вершин графа связана между собой ребром и имеет место равенство

$$x_u = x_v = \delta_{min} = 2m/n. \quad (6.2)$$

Таким образом, значение связности СС СН максимально для полносвязного графа. Для остальных случаев ее значение не может превысить значения минимальной степени вершины δ_{min}. То есть для повышения связности СС СН в условиях дестабилизирующих воздействий необходимо равномерное распределение плотности степеней вершин формализованного графа СС СН.

Для СС СН значение вершинной связности x_u определяет количество узлов связи (вершин графа), поражение которых приведет к несвязному графу, то есть к утрате свойства устойчивости. Значение реберной связности x_v определяет количество линий связи (ребер графа), приведение которых в неработоспособное состояние приведет к тому же результату.

Анализ функционирования СС СН в условиях вооруженных конфликтов [10] позволяет сделать вывод о том, что основными источниками дестабилизирующих воздействий на линии связи являются преднамеренные помехи, а на узлы связи – средства физического поражения, ФП ЭМИ и ИТВ. Причем вклад преднамеренных помех в складывающуюся электромагнитную обстановку в военное время несоизмеримо больше, нежели естественных помех, а вероятность поражения узла связи средствами поражения много выше вероятности отказа узла вследствие естественных процессов надежности. Поэтому для СС СН значение реберной связности x_v характеризует эффективность применения средств РЭП, а значение вершинной связности x_u – эффективность применения средств поражения (физического и ФП ЭМИ). Таким образом, значения вершинной (x_u) и реберной (x_v) связности формализованного графа СС СН могут служить как критериями устойчивости СС СН, так и критериями эффективности дестабилизирующих воздействий и определять то количество элементов СС СН, отказ которых соответствует утрате свойства устойчивости.

Дополнительно к показателям реберной и вершинной связности можно использовать показатели из теории сложных сетей, представленные в работе [187] и также описывающие устойчивость формализованного графа СС.

1) Диаметр графа $D(G)$ – длина максимального из кратчайших путей d_{ij}, которые можно сформировать между всеми вершинами графа G:

$$D(G) = \max(d_{ij} \mid d_{ij}<\infty),\ i=1...n,\ j=1...n,\ i\neq j. \quad (6.3)$$

В современных протоколах маршрутизации используется ограничение на число ретрансляций сообщения (пакета). Соответственно, в графе, представляющим такую СС СН, будут считаться связными только те пары узлов (вершин графа), между которыми существует путь, имеющий длину не более заданного.

Таким образом, данный показатель характеризует требование к протоколу маршрутизации по возможному количеству ретрансляций информационных пакетов.

2) Функция распределения степеней вершин $F(\delta_i)$ графа G, определяемая вероятностью того, что вершина u_i в графе G имеет степень δ_i. Функция $F(\delta_i)$ может характеризоваться распределением Пуассона, экспоненциальным или степенным распределением и используется при анализе вероятностных характеристик связности графа, формализующего СС СН.

3) Средний путь d_{cp} между вершинами графа G:

$$d_{\text{ср}} = \frac{2}{n(n+1)} \sum_{i \neq j} d_{ij}, \tag{6.4}$$

где: n – количество вершин графа; d_{ij} – кратчайший путь между i-ой и j-ой вершинами графа.

Чем меньше величина среднего пути $d_{\text{ср}}$, тем меньше элементов СС СН (узлов и линий связи) входит в состав путей ИНС и, соответственно, ниже вероятность их отказа и выше вероятность связности СС СН.

4) Показатель уязвимости сети H_z относительно удаления z-го элемента СС СН (узла или линии связи):

$$H_z = \left| E - E_z \right| / E, \tag{6.5}$$

где: E – эффективность исходной сети; E_z – эффективность сети после удаления z-го элемента (узла или линии связи).

В качестве меры эффективности могут быть использованы усредненные показатели качества обслуживания в СС СН. Для пакетных СС СН такими показателями могут являться: пропускная способность СС СН, нормированная к количеству ИНС; средняя длительность передачи сообщения (пакета) от абонента-источника к абоненту-получателю в СС СН; вероятность отказа в обслуживании.

5) Посредничество b_u вершины u:

$$b_u = \sum_{i \neq j} \frac{\varphi(i, u, j)}{\varphi(i, j)}, \tag{6.6}$$

где: $\varphi(i, j)$ – общее количество путей между вершинами i и j; $\varphi(i, u, j)$ – количество путей между вершинами i и j, проходящих через вершину u.

Величина посредничества вершины b_u определяет степень важности соответствующего ей узла связи при маршрутизации информационных потоков, то есть чем выше b_u, тем большее количество транзитных маршрутов, проходящих через узел связи u, будут нуждаться в перенаправлении в случае его отказа.

6) Коэффициент кластеризации вершины Y_u:

$$Y_u = \frac{2\delta_{u\Sigma}}{\delta_u(\delta_u - 1)}, \tag{6.7}$$

где: δ_u – степень вершины u; $\delta_{u\Sigma}$ – суммарная степень вершин, инцидентных вершине u.

Большое значение коэффициента кластеризации является признаком принадлежности вершины к группе узлов с высокой плотностью взаимосвязей

между собой, а распределение коэффициента кластеризации – соответствует тенденции к образованию таких групп.

Показатели уязвимости H_z, посредничества b_u и кластеризации Y_u могут быть использованы при определении коэффициентов важности элементов СС СН в ходе решения как задач повышения устойчивости СС СН, так и задач повышения эффективности преднамеренного воздействия на нее. Например, учет коэффициента кластеризации Y_u позволит скорректировать направление воздействия средств РЭП с целью подавления граничных элементов кластеров в интересах их изоляции.

В соответствии со стандартом [66], показателем устойчивости СС СН является значение вероятности связности ИНС $P_{св}$, под которой понимается вероятность того, что на заданном направлении связи существует хотя бы один путь, по которому возможна передача информации с требуемым качеством обслуживания QoS:

$$P_{св}=P(k_{QoS} \geq 1 \mid \{Q_k\} \in \{Q^{треб}\}), \qquad (6.8)$$

где: k_{QoS} – количество работоспособных путей на заданном ИНС, обеспечивающих заданное качество обслуживания QoS; Q_k – качество обслуживания, обеспечиваемое путями (путем) на заданном ИНС; $Q^{треб}$ – требуемый уровень качества обслуживания.

Вместе с тем, данное определение связности не учитывает важность отдельных ИНС, количество и распределение в них путей, а также особенности влияния на них дестабилизирующих воздействии. В связи с этим, в работе А.Н. Назарова и К.И. Сычева [27], в качестве показателя устойчивости сети предложено использовать *среднесетевую вероятность устойчивости ИНС* ($P_{У\,ср}$):

$$P_{У\,ср} = \frac{1}{N}\sum_{i=1}^{N} P_{У\,i}\,, \qquad (6.9)$$

где: N – количество ИНС в СС СН; $P_{У\,i}$ – устойчивость i-го ИНС, $i=\overline{1,N}$.

При этом устойчивость каждого i-го ИНС $P_{У\,i}$, входящего в сумму (6.9), будет определяться выражением [27]:

$$P_{У\,i} = K_{Г\,i}\, P_{св\,i}\,, \qquad (6.10)$$

где: $K_{Г\,i}$ – коэффициент готовности i-го ИНС; $P_{св\,i}$ – вероятность связности i-го ИНС в условиях влияния на него дестабилизирующих воздействий.

В выражении (6.10) коэффициент готовности $K_{Г\,i}$ определяет временные параметры процесса отказ – восстановление ИНС при влиянии на ИНС дестабилизирующих факторов, а вероятность связности $P_{св\,i}$ – структурно-вероятностные параметры ИНС.

Необходимо отметить, что при использовании показателя устойчивости в виде (6.9) вводится допущение о равнозначности различных ИНС в составе СС СН. Однако ИНС имеют различную важность и для учета их различного вклада в общий показатель устойчивости (выражение (6.9)) целесообразно ввести соответствующие весовые коэффициенты важности α_i для каждого i-го ИНС в СС СН [76]:

$$P_{\text{У ср}} = \sum_{i=1}^{N} \alpha_i P_{\text{У}i}\,, \tag{6.11}$$

где α_i удовлетворяют условию нормировки

$$\sum_{i=1}^{N} \alpha_i = 1\,.$$

В работе [76] предполагается, что весовые коэффициенты α_i в выражении (6.11) задаются исходя из конкретных условий и целей функционирования СС СН. Однако в этой работе не указываются конкретные подходы к вычислению коэффициентов важности.

В работе [27] коэффициенты важности i-го ИНС предложено определять исходя из циркулирующих по ним долей трафика:

$$\alpha_i(\lambda_i) = \frac{\lambda_i}{\sum_{i=1}^{N} \lambda_i}\,, \tag{6.12}$$

где λ_i – интенсивность трафика, передаваемого в i-том ИНС.

В качестве весовых коэффициентов α_i также могут быть использованы коэффициенты уязвимости H_z (6.5), посредничества b_u (6.6) и кластеризации Y_u (6.7). Например, в случае учета степени посредничества узлов b_u в коэффициенте важности i-го ИНС, α_i примет вид:

$$\alpha_i(b_u) = \frac{\sum_{j=1}^{k_i} \sum_{\nu=1}^{n_j} b_{u\,j\nu}}{\sum_{i=1}^{N} \sum_{j=1}^{k_i} \sum_{\nu=1}^{n_j} b_{u\,ij\nu}}\,, \tag{6.13}$$

где: k_i – количество путей в составе i-го ИНС; n_j – количество вершин в составе j-го пути i-го ИНС; $b_{u\,j\nu}$ – коэффициент посредничества ν-го элемента j-го пути в рассматриваемом ИНС; $b_{u\,ij\nu}$ – коэффициент посредничества ν-го элемента j-го пути в i-ом ИНС.

По аналогии, могут быть получены выражения для коэффициента важности i-го ИНС α_i в зависимости от коэффициентов уязвимости H_i и кластеризации Y_u:

$$\alpha_i(H) = \frac{\sum_{j=1}^{k_i} \sum_{\nu=1}^{z_j} H_{j\nu}}{\sum_{i=1}^{N} \sum_{j=1}^{k_i} \sum_{\nu=1}^{z_j} H_{ij\nu}}\,, \tag{6.14}$$

где: z_j – количество элементов (m_j линий и n_j узлов связи) в составе ИНС; $H_{j\nu}$ – коэффициент уязвимости ν-го элемента (вершины или ребра) j-го пути рассматриваемого ИНС; $H_{ij\nu}$ – коэффициент уязвимости ν-го элемента (вершины или ребра) j-го пути i-го ИНС;

$$\alpha_i(Y_u) = \frac{\sum_{j=1}^{k_i} \sum_{\nu=1}^{n_j} Y_{u\,j\nu}}{\sum_{i=1}^{N} \sum_{j=1}^{k_i} \sum_{\nu=1}^{n_j} Y_{u\,ij\nu}}\,, \tag{6.15}$$

где: n_j – количество узлов связи в составе ИНС; $Y_{u\,jv}$ – коэффициент кластеризации v-ой вершины j-го пути рассматриваемого ИНС; $Y_{u\,ijv}$ – коэффициент кластеризации v-ой вершины j-го пути i-го ИНС.

Вместе с тем, даже несмотря на возможность использования весовых коэффициентов, показатель устойчивости (6.10) учитывает структурные и динамические параметры устойчивости СС СН в слишком обобщенном виде, а также не учитывает особенности воздействия на элементы ИНС различных типов дестабилизирующих воздействий. Для учета вышеуказанных факторов были разработаны отдельные подходы к формализации, представленные ниже.

6.4. Формализация структурных параметров устойчивости системы связи с учетом дестабилизирующих воздействий различного типа на ее отдельные элементы

Рассмотрим более подробно факторы, определяющие вероятность связности отдельного i-го ИНС $P_{\text{св}\,i}$ в выражении (6.10) при определении показателя устойчивости СС СН.

Для учета специфики каждого типа дестабилизирующего воздействия вероятность связности $P_{\text{св}\,i}$ каждого отдельного i-го ИНС из выражения (6.10) предлагается определять в следующем виде:

$$P_{\text{св}\,i} = \left(1 - P_{\text{ФП}\,i}\right)\left(1 - P_{\text{ФПЭМИ}\,i}\right)\left(1 - P_{\text{РЭП}\,i}\right)\left(1 - P_{\text{ИТВ}\,i}\right)\left(1 - P_{\text{отк}\,i}\right), \qquad (6.16)$$

где: $P_{\text{ФП}\,i}$ – вероятность физического поражения (ФП) огневыми средствами такого количества узлов связи в ИНС, которое больше или равно величине вершинной связности x_u подграфа $G_{\text{ИНС}\,i}$ и переводит этот подграф в несвязное состояние; $P_{\text{ФПЭМИ}\,i}$ – вероятность функционального поражения ЭМИ такого количества узлов связи в ИНС, которое больше или равно величине вершинной связности x_u подграфа $G_{\text{ИНС}\,i}$ и переводит этот подграф в несвязное состояние; $P_{\text{РЭП}\,i}$ – вероятность радиоэлектронного подавления такого количества линий связи ИНС, которое больше или равно величине реберной связности x_v подграфа $G_{\text{ИНС}\,i}$ и переводит этот подграф в несвязное состояние; $P_{\text{ИТВ}\,i}$ – вероятность отказа такого количества элементов ИНС (линий и узлов связи) вследствие влияния ИТВ, которое больше или равно величине вершинной связности x_u или реберной связности x_v подграфа $G_{\text{ИНС}\,i}$ и переводит этот подграф в несвязное состояние; $P_{\text{отк}\,i}$ – вероятность такого количества отказов элементов ИНС (линий или узлов связи) вследствие воздействия внутренних дестабилизирующих факторов и естественных процессов надежности, которое больше или равно величине вершинной связности x_u или реберной связности x_v подграфа $G_{\text{ИНС}\,i}$ и переводит этот подграф в несвязное состояние.

Условие о влиянии каждого типа дестабилизирующего воздействия таким образом, чтобы оно приводило к критическому снижению вершинной (x_u) или реберной (x_v) связности подграфа $G_{\text{ИНС}\,i}$ в выражении (6.16), т.е. переводило бы этот подграф в несвязное состояние, по сути значит, что в таком подграфе пути передачи между источником и адресатом в ИНС отсутствуют.

Вместе с тем определение выражения (6.16) для всего ИНС может представлять определенную сложность, однако, если известны вероятности воздей-

ствия соответствующих дестабилизирующих факторов на каждый элемент, можно применить следующую свертку показателей.

Связность i-го ИНС определяется работоспособным состоянием всех k_i-ых путей, каждый из которых содержит z_j элементов (узлов и каналов связи) (при этом $j=\overline{1,k_i}$), в связи с чем выражение для $P_{\text{св}\,i}$ с учетом параметров отдельных элементов примет вид:

$$P_{\text{св}\,i}=1-\prod_{j=1}^{k_i}\left(1-P_{\text{раб}\,j}\right)=1-\prod_{j=1}^{k_i}\left(1-\prod_{\nu=1}^{z_j}P_{\text{раб. эл.}\,\nu}\right), \qquad (6.17)$$

где: k_i – количество путей в i-ом ИНС; $P_{\text{раб}\,j}$ – вероятность работоспособного состояния j-го пути в ИНС; j – номер пути в ИНС; $P_{\text{раб.эл.}\,\nu}$ – вероятность работоспособного состояния ν-го элемента ИНС (канала или узла связи); ν – номер элемента в ИНС; $z_j = n_j + m_j$ – число элементов (m_j линий и n_j узлов связи) в j-ом пути ИНС.

Отметим, что для свертки (6.17) введено допущение о том, что каждый j-ый путь в ИНС является работоспособным, если в нем работоспособны все z_j его элементов (узлов и каналов связи). Связность же i-го ИНС определяется работоспособным состоянием всех k_i-ых путей, каждый из которых содержит z_j элементов ($j=\overline{1,k_i}$).

В выражении (6.17) предполагается, что каждый ν-ый элемент i-го ИНС (узел или канал связи) подвергается воздействию дестабилизирующих факторов всех типов:

$$P_{\text{раб.эл.}\,\nu}=\left(1-P_{\text{ФП}\,\nu}\right)\left(1-P_{\text{ФПЭМИ}\,\nu}\right)\left(1-P_{\text{РЭП}\,\nu}\right)\left(1-P_{\text{ИТВ}\,\nu}\right)\left(1-P_{\text{отк}\,\nu}\right), \qquad (6.18)$$

где: $P_{\text{ФП}\,\nu}$ – вероятность отказа ν-го элемента ИНС (узла связи) вследствие его физического поражения огневыми средствами; $P_{\text{ФП ЭМИ}\,\nu}$ – вероятность отказа ν-го элемента ИНС (узла связи) вследствие его функционального поражения ЭМИ; $P_{\text{РЭП}\,\nu}$ – вероятность отказа ν-го элемента ИНС (канала связи) вследствие его радиоэлектронного подавления; $P_{\text{ИТВ}\,\nu}$ – вероятность отказа ν-го элемента ИНС (канала или узла связи связи) вследствие влияния ИТВ; $P_{\text{отк}\,\nu}$ – вероятность отказа ν-го элемента ИНС (канала или узла связи связи) вследствие воздействия внутренних дестабилизирующих факторов и естественных процессов надежности.

Если какой-либо из дестабилизирующих факторов отсутствует, то соответствующая вероятность равна нулю.

Из выражения (6.17) можно определить математическое ожидание количества работоспособных путей в ИНС $M(k)$:

$$M\left(k\right)=\sum_{j=1}^{k_i}j\left(1-\prod_{\nu=1}^{z_j}P_{\text{раб. эл.}\,\nu}\right). \qquad (6.19)$$

Если допустить, что все j-ые пути в составе ИНС характеризуются равным значением вероятности работоспособного состояния пути $P_{\text{раб}\,j}$, то можно рассчитать количество путей k_i, которое обеспечит требуемую вероятность связности отдельного i-го ИНС $P_{\text{св}\,i}$:

$$k_i=\left\lfloor \log_{\left(1-P_{\text{раб}\,j}\right)}\left(1-P_{\text{св}\,i}\right)\right\rfloor. \qquad (6.20)$$

где $\lfloor \bullet \rfloor$ – оператор округления до наименьшего целого числа.

Зачастую в практике построения современных СС СН используется резервирование путей в ИНС, когда один путь является основным, а остальные – резервными. В этом случае вероятность связного состояния ИНС, состоящего из одного основного и (k_i–1) резервных путей (соответственно из $z_{осн}$ и z_j элементов, где $j=\overline{1, k_i-1}$), будет определяться как:

$$P_{св\,i} = 1 - \left(1 - \prod_{v=1}^{z_{осн}} P_{раб.\,эл.\,v}\right) \prod_{j=1}^{k_i-1} \left(1 - \prod_{v=1}^{z_j} P_{раб.\,эл.\,v}\right). \qquad (6.21)$$

Так как для любого j-го пути $P_{раб.эл.\,v} \leq 1$, то для любого ИНС добавление резервных путей будет увеличивать вероятность его связности $P_{св\,i}$.

Вместе с тем, выражение (6.21) не учитывает возможные пересечения путей на элементах подграфа ИНС.

Зависимость вероятности связности i-го ИНС $P_{св\,i}$ от количества путей k_i в ИНС с учетом их пересечений по общим элементам сети показана в работе Д.А. Ковалькова [133]. В случае, если первыми k_i путями обеспечивается вероятность связности $P_{св\,k_i}$, то добавление очередного пути (k_i+1) приведет к увеличению вероятности связности ИНС до $P_{св\,k_i+1}$. Вероятность $P_{св\,k_i+1}$ будет определяться вероятностью двух событий – исправен хотя бы один из первых k_i путей или исправен (k_i+1)-ый путь, в соответствии с рекуррентной формулой [133]:

$$P_{св\,i} = P_{св\,k_i} + P_{св\,k_i+1} - P_{св\,k_i+1} \cdot P_{св\,k_i},$$

при этом в произведении вероятностей связности ИНС $P_{св\,k_i+1} \cdot P_{св\,k_i}$ при наличии общих элементов, связность, обеспечиваемая элементами, входящими в первые k_i путей и общими с новым (k_i +l)-ым путем, заменяется единицей.

6.5. Формализация структурных параметров устойчивости системы связи с учетом ведения разведки против ее отдельных элементов

Специфика показателей $P_{ФП\,v}$, $P_{ФПЭМИ\,v}$, $P_{РЭП\,v}$ и $P_{ИТВ\,v}$ в выражении (6.18) состоит в том, что для осуществления дестабилизирующего воздействия соответствующего типа необходимо провести предварительную разведку объекта воздействия, с целью вскрытия параметров необходимых для целеуказания средствам поражения. Для средств физического поражения и средств ФП ЭМИ такими параметрами является местоположение объектов СС СН, для средств РЭП – сигнальные параметры подавляемых линий связи, для ИТВ – состояние адресных и структурно-сетевых параметров подсетей и узлов в информационном пространстве. Эти параметры вскрываются соответствующими видами разведки. При этом показатели $P_{ФП\,v}$, $P_{ФП\,ЭМИ\,v}$, $P_{РЭП\,v}$ и $P_{ИТВ\,v}$ будут являться условными вероятностями при условии, что параметры элемента СС СН, требуемые для осуществления на него соответствующего типа воздействия, уже были вскрыты с вероятностью 1.

Пусть вероятность успешной разведки противником параметров v-го элемента СС СН равна $P_{рз\,v}$. Если для организации дестабилизирующего воздей-

ствия системой разведки требуется вскрытие не менее $m_{\text{рз v}}$ независимых i-ых параметров v-го элемента СС СН, то [190]

$$P_{\text{рз v}} = \prod_{i=1}^{m_{\text{рз v}}} P_{\text{рз v}\,i}\,. \qquad (6.22)$$

При этом вероятность вскрытия вышеуказанных i-ых параметров v-го элемента СС СН определяется соответствующими показателями его скрытности [190]:

$$P_{\text{скр v}\,i} = 1 - P_{\text{рз v}\,i}, \qquad (6.23)$$

где $P_{\text{скр v}\,i}$ – вероятность скрытности i-го параметра v-го элемента СС СН, то есть показатель, определяющий способность элемента не допустить вскрытие своего i-го параметра функционирования разведкой противника.

В работе [191] скрытность связного РЭС, как элемента СС СН, рассматривается в пяти аспектах:

1) *энергетическая скрытность* – способность противостоять обнаружению сигналов РЭС средствами РРТР, которая может оцениваться различными показателями: вероятностью обнаружения сигналов РЭС при заданной вероятности ложной тревоги; отношением сигнал-шум на входе приемника РРТР, обеспечивающем заданные вероятности обнаружения РЭС и уровень вероятности ложной тревоги; дальность обнаружения сигналов РЭС при заданном отношении сигнал-шум;
2) *структурная скрытность* – способность противостоять вскрытию структуры сигнала (определяется используемым кодированием и модуляцией) средствами РРТР, которая может оцениваться условной вероятностью правильного определения структуры сигнала при условии, что сигнал правильно обнаружен;
3) *информационная скрытность* – способность противостоять вскрытию смысла передаваемых сообщений средствами РР или компьютерной разведки, при условии правильного вскрытия структуры сигнала, которая может оцениваться вероятностью вскрытия семантического содержания передаваемых сообщений. К информационной скрытности также можно отнести способность противостоять вскрытию служебной информации протоколов и адресно-сетевой информации СС СН средствами сетевой и потоковой компьютерной разведки;
4) *временная скрытность* – способность противостоять вскрытию средствами РРТР временных параметров работы РЭС, которая может оцениваться вероятностью сбора информации о временных параметрах работы РЭС на заданной длительности наблюдения;
5) *пространственная скрытность* – способность противостоять вскрытию местоположения РЭС и пространственной ориентации направлений ее работы, которая может оцениваться различными показателями: вероятностью точного определения местоположения РЭС; вероятностью точного определения направлений связи РЭС; радиусом зоны, в которой с заданной вероятностью находится РЭС.

Несмотря на широкую применимость вышеуказанных показателей скрытности для оценки помехозащищенности РЭС в работах [190, 191], предлагается модифицировать их в направлении их использования для оценивания эффективности тех видов разведки (представленных в разделе 3), которые ориентированы на вскрытие элементов СС СН в интересах организации на них соответствующего типа дестабилизирующих воздействий.

Вероятность физического поражения ν-го элемента СС СН (узла связи) огневыми средствами с учетом того, что для этого необходима разведка с целью вскрытия местоположения элемента будет равна условной вероятности:

$$P_{\text{ФП}\,\nu} = \left(P^{*}_{\text{ФП}\,\nu} \middle| P_{\text{рз.пр}\,\nu} = 1\right) P_{\text{рз.пр}\,\nu}, \qquad (6.24)$$

где: $P_{\text{ФП}\,\nu}$ – значение условной вероятности физического поражения ν-го элемента СС СН (узла связи) огневыми средствами; $P^{*}_{\text{ФП}\,\nu} \middle| P_{\text{рз.пр}\,\nu} = 1$ – вероятность поражения ν-го элемента СС СН (узла связи) при условии его успешной разведки и вскрытия местоположения т.е. при $P_{\text{рз.пр}\,\nu}$ =1; $P_{\text{рз.пр}\,\nu}$ – вероятность разведки местоположения ν-го элемента СС СН (узла связи) в пространстве.

С учетом того, что разведка местоположения ν-го элемента СС СН (узла связи) может вестись как средствами РРТР, так и средствами ОЭР, которые действуют одновременно и независимо, то для $P_{\text{рз.пр}\,\nu}$ можно записать:

$$P_{\text{рз.пр}\,\nu} = P_{\text{рз.пр.РРТР}\,\nu} + P_{\text{рз.пр.ОЭР}\,\nu} - P_{\text{рз.пр.РРТР}\,\nu}\, P_{\text{рз.пр.ОЭР}\,\nu}, \qquad (6.25)$$

где: $P_{\text{рз.пр.РРТР}\,\nu}$ – вероятность вскрытия местоположения в пространстве ν-го элемента СС СН (узла связи) средствами РРТР; $P_{\text{рз. пр.ОЭР}\,\nu}$ – вероятность вскрытия местоположения в пространстве ν-го элемента СС СН (узла связи) средствами ОЭР.

Так как оба эти вида разведки ориентированы на нарушение свойства пространственной скрытности элемента СС СН, то выражение (6.25) можно записать в виде:

$$P_{\text{рз.пр}\,\nu} = \left(1 - P_{\text{скр.пр.РРТР}\,\nu}\right) + \left(1 - P_{\text{скр.пр.ОЭР}\,\nu}\right) - \left(1 - P_{\text{скр.пр.РРТР}\,\nu}\right)\left(1 - P_{\text{скр.пр.ОЭР}\,\nu}\right), \qquad (6.26)$$

где: $P_{\text{скр.пр.РРТР}\,\nu}$ – пространственная скрытность местоположения ν-го элемента СС СН (узла связи) по отношению к средствами РРТР; $P_{\text{скр.пр.ОЭР}\,\nu}$ – пространственная скрытность местоположения ν-го элемента СС СН (узла связи) по отношению к средствами ОЭР.

Аналогично рассуждая, получим выражения для $P_{\text{ФПЭМИ}\,\nu}$, $P_{\text{РЭП}\,\nu}$ и $P_{\text{ИТВ}\,\nu}$ с учетом показателей вероятности разведки параметров отдельных элементов СС СН.

Вероятность функционального поражения ν-го элемента СС СН (узла связи) средствами ФП ЭМИ, как и для случая физического поражения, также будет определяться вероятностью успешной разведки его местоположения:

$$P_{\text{ФПЭМИ}\,\nu} = \left(P^{*}_{\text{ФПЭМИ}\,\nu} \middle| P_{\text{рз.пр}\,\nu} = 1\right) P_{\text{рз.пр}\,\nu}, \qquad (6.27)$$

где: $P_{\text{ФПЭМИ}\,\nu}$ – значение условной вероятности функционального поражения ЭМИ ν-го элемента СС СН (узла связи); $P^{*}_{\text{ФПЭМИ}\,\nu} \middle| P_{\text{рз.пр}\,\nu} = 1$ – вероятность функционального поражения ЭМИ ν-го элемента СС СН (узла связи) при условии его

успешной разведки и вскрытия местоположения т.е. $P_{\text{рз.пр}\,\nu}=1$; $P_{\text{рз.пр}\,\nu}$ – имеет тот же смысл, что и в выражении (6.24).

Аналогично физическому поражению, для параметра $P_{\text{рз.пр}\,\nu}$ при функциональном поражении ЭМИ ν-го элемента СС СН будут справедливы формулы (6.25) и (6.26).

Вероятность радиоэлектронного подавления ν-го элемента СС СН (линии связи) средствами РЭП с учетом того, что для этого необходима разведка энергетических, временных и структурных параметров этого элемента СС СН, будет равна произведению соответствующих условных вероятностей:

$$P_{\text{РЭП}\,\nu}=\left(P^{*}_{\text{РЭП}\,\nu}\left|P_{\text{рз.ст}\,\nu}=1,P_{\text{рз.вр}\,\nu}=1\right.\right)\left(P_{\text{рз.ст}\,\nu}\left|P_{\text{рз.э}\,\nu}=1\right.\right)\left(P_{\text{рз.вр}\,\nu}\left|P_{\text{рз.э}\,\nu}=1\right.\right)P_{\text{рз.э}\,\nu}, \quad (6.28)$$

где: $P_{\text{РЭП}\,\nu}$ – значение условной вероятности радиоэлектронного подавления ν-го элемента СС СН (канала связи); $P_{\text{рз.э}\,\nu}$ – значение вероятности успешного приема сигналов и вскрытия энергетических параметров ν-го элемента СС СН (канала связи); $P_{\text{рз.вр}\,\nu}\left|P_{\text{рз.э}\,\nu}=1\right.$ – значение условной вероятности разведки и вскрытия временных параметров ν-го элемента СС СН (канала связи) при условии вскрытия энергетических параметров $P_{\text{рз.э}\,\nu}=1$; $P_{\text{рз.ст}\,\nu}\left|P_{\text{рз.э}\,\nu}=1\right.$ – значение условной вероятности разведки и вскрытия структурных параметров ν-го элемента СС СН (канала связи) при условии вскрытия энергетических параметров $P_{\text{рз.э}\,\nu}=1$; $P^{*}_{\text{РЭП}\,\nu}\left|P_{\text{рз.ст}\,\nu}=1,P_{\text{рз.вр}\,\nu}=1\right.$ – вероятность радиоэлектронного подавления ν-го элемента СС СН (канала связи) при условии вскрытия структурных и временных параметров $P_{\text{рз.ст}\,\nu}=1$, $P_{\text{рз.вр}\,\nu}=1$.

Отметим, что энергетические, временные и структурные параметры элемента СС СН, требуемые для решения задач его радиоэлектронного подавления, вскрываются исключительно средствами РРТР. При этом переход от вероятности разведки к параметрам скрытности ν-го элемента СС СН (канала связи) осуществляется следующем образом:

$$P_{\text{рз.э}\,\nu}=1-P_{\text{скр.э}\,\nu},\ P_{\text{рз.вр}\,\nu}=1-P_{\text{скр.вр}\,\nu},\ P_{\text{рз.ст}\,\nu}=1-P_{\text{скр.ст}\,\nu},$$

где: $P_{\text{скр.э}\,\nu}$ – вероятность обеспечения энергетической скрытности ν-го элемента СС СН (канала связи) от средств РРТР; $P_{\text{рз.вр}\,\nu}$ – вероятность обеспечения временной скрытности ν-го элемента СС СН (канала связи) от средств РРТР; $P_{\text{рз.ст}\,\nu}$ – вероятность обеспечения структурной скрытности ν-го элемента СС СН (канала связи) от средств РРТР.

Вероятность реализации ИТВ на ν-ый элемент СС СН (узел или линию связи) с учетом того, что для этого необходима разведка информационных, энергетических, временных и структурных параметров это элемента, будет равна произведению условных вероятностей:

$$P_{\text{ИТВ}\,\nu}=\left(P^{*}_{\text{ИТВ}\,\nu}\left|P_{\text{рз.инф}\,\nu}=1\right.\right)\left(P_{\text{рз.инф}\,\nu}\left|P_{\text{рз.ст}\,\nu}=1,P_{\text{рз.вр}\,\nu}=1\right.\right)\times$$
$$\times\left(P_{\text{рз.ст}\,\nu}\left|P_{\text{рз.э}\,\nu}=1\right.\right)\left(P_{\text{рз.вр}\,\nu}\left|P_{\text{рз.э}\,\nu}=1\right.\right)P_{\text{рз.э}\,\nu}, \quad (6.29)$$

где: $P_{\text{ИТВ}\,\nu}$ – значение условной вероятности успешной разведки и реализации ИТВ против ν-го элемента СС СН (узла или канала связи); $P^{*}_{\text{ИТВ}\,\nu}\left|P_{\text{рз.инф}\,\nu}=1\right.$ – вероятность успешной реализации ИТВ против ν-го элемента СС СН (узла или канала связи) при условии успешной разведки и вскрытия информационных

параметров т.е. $P_{\text{рз.инф}\,\nu}=1$; $P_{\text{рз.инф}\,\nu}\left|P_{\text{рз.ст}\,\nu}=1, P_{\text{рз.вр}\,\nu}=1\right.$ – значение условной вероятности успешного вскрытия информационных параметров ν-го элемента СС СН (узла или канала связи), содержавших служебную информацию для целеуказания при реализации ИТВ, при условии что были вскрыты структурные и временные параметры $P_{\text{рз.ст}\,\nu}=1$, $P_{\text{рз.вр}\,\nu}=1$; $P_{\text{рз.вр}\,\nu}\left|P_{\text{рз.э}\,\nu}=1, P_{\text{рз.ст}\,\nu}\right|P_{\text{рз.э}\,\nu}=1$, $P_{\text{рз.э}\,\nu}$ – имеют тоже значение, что и в выражении (6.28).

Отметим, что энергетические, временные и структурные параметры элемента СС СН в радиодиапазоне вскрываются исключительно средствами РРТР, а информационные параметры – средствами РР или компьютерной разведки. При этом переход к параметрам информационной скрытности ν-го элемента СС СН (узла или канала связи) осуществляется следующем образом:

$$P_{\text{рз.инф}\,\nu}=1-P_{\text{скр.инф}\,\nu}.$$

6.6. Формализация структурных параметров устойчивости системы связи с учетом требований к качеству обслуживания трафика

При решении задач оценивания устойчивости СС СН, с учетом требований к качеству обслуживания (QoS) передаваемого трафика, можно использовать следующий подход.

Рассматривая СС СН с коммутацией пакетов, за показатели QoS j-го пути конкретного ИНС можно принять показатели QoS обслуживания пакетов в его отдельных элементах пути (узлах и каналах связи) z_j, которые формализуются в виде моделей систем массового обслуживания (СМО). Таким образом, выражения для соответствующих показателей QoS j-го пути конкретного ИНС примут вид:

1) время передачи пакета по j-му пути:

$$T_{\text{зад}\,j}=\sum_{\nu=1}^{z_j}T_{\text{зад}\,\nu};$$

2) абсолютная пропускная способность j-го пути:

$$C_{a\,j}=\min_{\nu\in\left[1,z_j\right]}\left\{C_{a\,\nu}\right\};$$

3) вероятность отказа в обслуживании пакета при передаче его по j-му пути:

$$P_{\text{отк пак}\,j}=1-\prod_{\nu=1}^{z_j}\left(1-P_{\text{отк пак}\,\nu}\right);$$

где $T_{\text{зад}\,\nu}$ – время задержки пакета в ν-ом элементе j-го пути; $C_{a\,\nu}$ – абсолютная пропускная способность (пакетов в секунду) ν-го элемента j-го пути; $P_{\text{отк пак}\,\nu}$ – отказ в обслуживании пакета в ν-ом элементе j-го пути.

С учетом данных выражений, соответствие j-го пути ИНС заданному уровню QoS определяется выполнением интегрального критерия $Q_j \geq Q_j^{\text{треб}}$, равносильного системе:

$$Q_j \geq Q_j^{\text{треб}} \Leftrightarrow \begin{cases} T_{\text{зад}\,j} \leq T_{\text{зад}\,j}^{\text{треб}}; \\ C_{a\,j} \geq C_{a\,j}^{\text{треб}}; \\ P_{\text{отк пак}\,j} \leq P_{\text{отк пак}\,j}^{\text{треб}}. \end{cases} \tag{6.30}$$

С учетом интегрального критерия (6.30), выражение (6.21) для оценки вероятности связности i-го ИНС, будет определяться произведением вероятностей выполнения на k_i -ых путях этого ИНС требований по QoS:

$$P_{\text{св}\,i} = 1 - \prod_{j=1}^{k_i} P\left(T_{\text{зад}\,j} \leq T_{\text{зад}\,j}^{\text{треб}}; C_{a\,j} \geq C_{a\,j}^{\text{треб}}; P_{\text{отк пак}\,j} \leq P_{\text{отк пак}\,j}^{\text{треб}}\right). \tag{6.31}$$

При этом математическое ожидание количества путей в ИНС, в которых обеспечивается заданный уровень QoS, будет равно:

$$M\left(k_{QoS}\right) = \sum_{j=1}^{k_i} jP\left(T_{\text{зад}\,j} \leq T_{\text{зад}\,j}^{\text{треб}}; C_{a\,j} \geq C_{a\,j}^{\text{треб}}; P_{\text{отк пак}\,j} \leq P_{\text{отк пак}\,j}^{\text{треб}}\right). \tag{6.32}$$

где: k_{QoS} – количество путей, в составе ИНС, в которых обеспечивается заданный уровень QoS; $M(\cdot)$ – обозначение математического ожидания.

В соответствии со стандартом [66] для сохранения связности ИНС достаточно, чтобы в его составе функционировал как минимум один путь, в котором обеспечивается заданный уровень QoS. В этом случае показатель связности ИНС можно представить, как вероятность сохранения в ИНС одного или более путей с требуемым QoS:

$$P_{\text{св}\,i} = P\left(M\left(k_{QoS}\right) \geq 1\right). \tag{6.33}$$

Вместе с тем, в СС СН, как правило, приняты различные схемы резервирования, направленные на повышения вероятности связности ИНС в условиях различных дестабилизирующих воздействий. В случае если в СС СН принята схема резервирования 1+k, в которой основной путь резервируется не менее k резервными путями выражение (6.33) можно переписать в виде: выражение

$$P_{\text{св}\,i} = P\left(M\left(k_{QoS}\right) \geq 1 + k\right). \tag{6.34}$$

6.7. Формализация временных параметров устойчивости системы связи с учетом длительности процессов восстановления связи

Временным показателем устойчивости i-го ИНС является коэффициент готовности $K_{\text{Г}\,i}$, который определяется наработкой на отказ $T_{\text{О}\,i}$ и временем восстановления $T_{\text{В}\,i}$:

$$K_{\text{Г}\,i} = \frac{T_{\text{О}\,i}}{T_{\text{О}\,i} + T_{\text{В}\,i}}. \tag{6.35}$$

В случае если известны временные параметры дестабилизирующих воздействий и длительности между отказами можно аппроксимировать в виде функции интенсивности отказов каждого i-го ИНС $\lambda_{\text{отк}\,i}(t)$, то можно определить

функцию вероятности длительности сохранения работоспособности i-го ИНС, которая соответствует вероятности его связного состояния $P_{\text{св}\,i}$:

$$P_{\text{св}\,i}(t) = P(t_{\text{отк}\,i} \geq t), \tag{6.36}$$

где $t_{\text{отк}\,i}$ – длительность до момента отказа i-го ИНС, заключающегося в утрате свойства связности.

В результате преобразований с использованием научно-методического аппарата теории надежности выражение (6.36) примет вид:

$$P_{\text{св}\,i}(t) = \exp\left(-\int_0^t \lambda_{\text{отк}\,i}(\tau)d\tau\right). \tag{6.37}$$

Наработка на отказ $T_{\text{О}\,i}$ является математическим ожиданием функции вероятности времени сохранения работоспособного состояния ИНС и, с учетом (6.37), определяется выражением:

$$T_{\text{О}\,i} = \int_0^\infty P_{\text{св}\,i}(t)\,dt = \int_0^\infty \left(\exp\left(-\int_0^\infty \lambda_{\text{отк}\,i}(t)dt\right)\right)dt\,. \tag{6.38}$$

При допущении о конфликтно-устойчивом процессе функционирования ИНС в условиях совокупности дестабилизирующих воздействий, можно считать, что поток отказов является простейшим. Функция распределения интенсивности отказов для i-го ИНС в этом случае будет являться постоянной величиной $\lambda_{\text{отк}\,i}(t) = \lambda_{\text{отк}\,i}$. При данных допущениях выражения для $P_{\text{св}\,i}$ и $T_{\text{О}\,i}$ примут вид:

$$P_{\text{св}\,i}(t) = \exp\left(-\lambda_{\text{отк}\,i}\,t\right),\ T_{\text{О}\,i} = 1/\lambda_{\text{отк}\,i}. \tag{6.39}$$

Время восстановления ИНС $T_{\text{В}\,i}$ в выражении (6.35), согласно работы [131], состоит из времени диагностики отказа ИНС $T_{\text{диагн}\,i}$, времени ожидания восстановления связи (удержания конфигурации ИНС) $T_{\text{ож}\,i}$, времени уведомления узла, ответственного за изменение конфигурации путей ИНС $T_{\text{увед}\,i}$, длительности резервирования и реконфигурации путей в ИНС $T_{\text{рек}\,i}$ и времени переключения информационных потоков с активных путей на резервные пути в составе ИНС $T_{\text{перекл}\,i}$:

$$K_{\text{Г}\,i} = \frac{T_{\text{О}\,i}}{T_{\text{О}\,i} + T_{\text{В}\,i}} = \frac{T_{\text{О}\,i}}{T_{\text{О}\,i} + \left(T_{\text{диагн}\,i} + T_{\text{ож}\,i} + T_{\text{увед}\,i} + T_{\text{рек}\,i} + T_{\text{перекл}\,i}\right)}\,. \tag{6.40}$$

При этом, время уведомления $T_{\text{увед}\,i}$ в ИНС зависит от времени ретрансляции между отдельными узлами сообщения об отказе $T_{\text{р}}$ и от количества ретрансляций этого сообщения в сети (так называемых, хопов) d_{ij}, во время передачи между узлом, обнаружившим отказ пути (узел i), и узлом, ответственным за переключение путей в ИНС (узел j).

$$T_{\text{увед}\,i} = T_{\text{р}}\,d_{ij}\,. \tag{6.41}$$

6.8. Итоговая схема оценивания устойчивости на основе топологической модели системы связи

Рассмотренные выше структурно-вероятностные и временные параметры, определяющие показатель единый показатель устойчивости СС СН (определяются выражениями (6.9) или (6.11)), могут быть взаимоувязаны в единую формализованную систему, представленную на рис. 6.2.

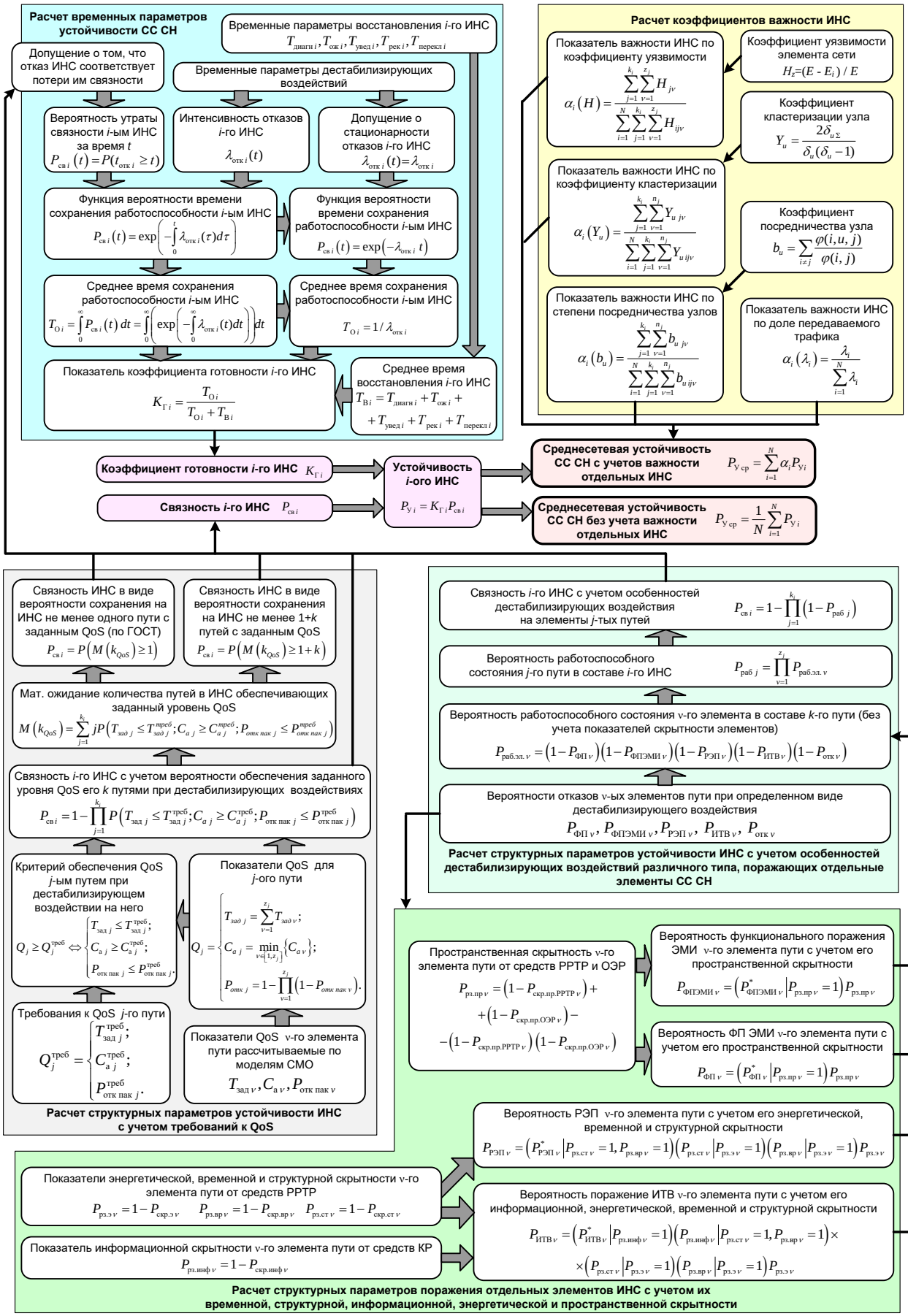

Рис. 6.2. Схема оценки показателя устойчивости СС СН в топологической модели

Представленная на рис. 6.2 схема оценки устойчивости СС СН, позволяет увязать между собой понятийный аппарат руководящих документов и аналитические параметры устойчивости, предлагаемые различными авторами, а также позволяет учесть, как временные параметры процесса функционирования СС СН в условиях воздействия различных дестабилизирующих воздействий, так и структурно-вероятностные параметры этого процесса с учетом их взаимозависимости.

Выводы по шестой главе

Проведенный анализ показал, что свойство устойчивости является системным свойством СС СН, которое, с одной стороны объединяет в себя частные показатели способности системы сохранять свою структуру и функциональность при различных типах возмущающих воздействий – живучести, помехоустойчивости, надежности, а, с другой стороны, является частным по отношению к свойствам адаптивности и самоорганизации, описывающим способность системы приспосабливаться к негативным условиям внешней среды.

Интегральный показатель устойчивости СС СН, декомпозированный на отдельные показатели в соответствии с предложенной схемой (рис. 6.2), показывает, что заданный уровень устойчивости СС СН обеспечивается не только высокими значениями структурно-сетевых параметров в условиях дестабилизирующих воздействий (определяется показателем структурной связности элементов), но и высоким значением коэффициента готовности СС СН (определяется показателем времени восстановления связи в СС СН). Верно и обратное – заданный уровень снижения устойчивости СС СН за счет влияния преднамеренных дестабилизирующих воздействий, может быть достигнут не только за счет масштабного разрушения структуры СС СН, но и за счет высокой интенсивности дестабилизирующих воздействия при минимальном воздействии на структуру СС СН. Таким образом, представленная в данной главе топологическая модель системы связи может быть использована для расчета конечного показателя устойчивости СС СН с учетом как параметров системы связи, так и параметров дестабилизирующих воздействий и рекомендуется к использованию специалистам, ведущим работы в области повышения качества связи или разработчикам новых видов ИТВ и способов РЭП для оценки эффективности предлагаемых решений.

7. Игровая модель системы связи в условиях дестабилизирующих воздействий и ведения разведки

7.1. Постановка задачи на моделирование

Предложенная выше топологическая модель системы связи описывает структурные характеристики системы в условиях воздействия дестабилизирующих факторов. Однако, данная топологическая модель не ориентирована на описание процесса многоэтапного информационного конфликта, в котором стороны меняют свои стратегии на каждом этапе функционирования, как это показано в концептуальной модели, представленной в главе 4. Для интегрального описания топологических параметров сети и их смены в процессе многоэтапного информационного конфликта предлагается сформировать игровую модель системы связи, в которой выбор и смена стратегий противоборствующих сторон рассматривается в формализме теории игр.

Для формализации игровой модели введем следующие обозначения:

$|I|$ – число элементов множества I;

$|J|$ – число элементов множества J;

$|S|$ – число элементов множества S;

A – матрица приоритетности ИНС;

$a_{\lambda,\lambda}$ – коэффициент важности λ-го ИНС;

$H(S_j, V_i)$ – фазовая траектория, которая соответствует динамике совместного изменения состояний S_j и V_i в процессе развития многоэтапного конфликта метасистемы «система связи – система дестабилизирующих воздействий»;

$H^{\text{сдв}}(S_j, V_i)$ – состояние метасистемы $H(S_j, V_i)$, наблюдаемое системой дестабилизирующих воздействий;

$H^{\text{сс}}(S_j, V_i)$ – состояние метасистемы $H(S_j, V_i)$, наблюдаемое системой связи;

I – множество стратегий нападения на систему связи со стороны системы дестабилизирующих воздействий;

i – стратегия нападения на систему связи со стороны системы дестабилизирующего воздействия;

J – множество стратегий защиты системы связи;

j – стратегия защиты системы связи;

K – количество вариантов дестабилизирующего воздействия;

k – номер дестабилизирующего воздействия;

L – количество иерархий в системе управления;

l – номер иерархии системы управления;

m – счетчик;

M – общее количество элементов (узлов и линий связи) в системе связи;

N – количество этапов в многоэтапной информационном конфликте;

n – счетчик;

N_Λ – количество ИНС, организуемых в системе связи;

$P_i(V_i)$ – вероятность применения системой дестабилизирующих воздействий i-го варианта нападения, который соответствует использованию V_i структуре использования средств разведки и нападения;

$P_j(S_j)$ – вероятность применения системой связи j-го варианта защиты, который соответствует использованию S_j-структуре организации связи;

$P_{У\ i}$ – вероятность устойчивости i-го ИНС;

$P_{У\ ср}$ – итоговый показатель устойчивости системы связи – среднесетевая вероятность устойчивости ИНС;

$P_{У\ ср}(S_j, V_i)$ – показатель устойчивости системы связи в условиях, когда против системы связи реализован вариант нападения V_i, а система связи использует структуру организации связи S_j;

Q – матрица показателей качества функционирования ИНС в системе связи;

q – показатель качества системы связи;

$q_{\lambda,j,i}$ – показатель качества λ-го ИНС, если на нем используется j-ый вариант распределения линий и узлов связи, подвергающийся i-му варианту дестабилизирующего воздействия;

$S=S_{ус}\cup S_{лс}$ – структура защищаемой системы связи, состоящая из структуры размещения узлов связи $S_{ус}$ и линий связи между узлами $S_{лс}$;

S_j – структура системы связи, реализуемая в рамках j-ой стратегии защиты;

$S_j(t_n)$ – структура системы связи, соответствующая j-ой стратегии защиты, на n-ом этапе конфликта;

$S_j^{опт}(t_n)$ – структура системы связи, соответствующая j-ой стратегии защиты, которая является оптимальной на n-ом этапе конфликта;

$s_{n,m}$ – элемент множества $S=S_{ус}\cup S_{лс}$, задающий принадлежность конкретного узла или линии связи к ИНС от n-го узла связи к m-му узлу;

$S_{лс}$ – подмножество S, задающее структуру размещения линий связи;

$S_{ус}$ – подмножество S, задающее структуру размещения узлов связи;

$V=\{V_i\}=\{v_{s,k}\}_i$ – множество вариантов воздействия, которые может реализовать субъект нападения;

$V_i(t_n)$ – вариант воздействия, который соответствует i-ой стратегии нападения, на n-ом этапе конфликта;

$V_i=\{v_{s,k}\}$ – воздействие на систему связи, реализуемое в рамках i-ой стратегии нападения;

$v_{s,k}$ – элемент множества V, задающий воздействие k-го типа на s-ый элемент (узел или линию связи) системы связи;

γ – оператор, который описывает процесс эволюции метасистемы $H(S_j, V_i)$ в фазовом пространстве $V\times S$;

η – отображение, задающие наблюдение (мониторинг) параметров метасистемы со стороны системы связи;

λ – номер ИНС;

$\Lambda=\{\lambda_{n,m}\}$ – структура ИНС, организуемых в системе связи;

$\lambda_{n,m}$ – элемент множества Λ, задающий наличие ИНС от n-го узла связи к m-му узлу;

μ – отображение, задающие наблюдение (разведку) параметров метасистемы со стороны системы дестабилизирующих воздействий.

Целью моделирования является формализация структурных параметров противоборствующих сторон (системы связи и системы дестабилизирующих воздействий) с учетом динамики развития информационного конфликта и возможности смены стратегий сторон для достижения наилучшего выигрыша.

В основу игровой модели системы связи положена модель, представленная в работе [2] (в подразделе 2.3), которая была модифицирована с целью ее совместимости с концептуальной моделью, представленной в главе 4, и с топологической моделью, представленной в главе 6.

7.2. Формализация структур системы связи и системы дестабилизирующих воздействий

Для адекватного описания процессов конфликтного взаимодействия системы связи и системы дестабилизирующих воздействий на длительности информационного конфликта применим дискретный подход к формализации времени, подразумевающий разбиение всей длительности конфликта на отдельные этапы, внутри которых конфликтующие стороны придерживаются неизменных стратегий разведки, нападения и защиты. Это значит, что на длительности конфликта задается конечное множество как вариантов структуры системы связи, так и вариантов структуры системы дестабилизирующих воздействий, а также конечное множество их стратегий.

Определим множество допустимых вариантов организации связи в СС СН как множество булевых матриц $\Lambda=\{\lambda_{n,m}\}$ размером $N_\Lambda \times N_\Lambda$, где N_Λ – максимально возможное количество ИНС «точка – точка» между узлами в сети СС СН. Очевидно, что в случае совокупности независимых ИНС получим конечное счетное множество матриц $\{\lambda_{n,m}\}$ с количеством элементов $2N_\Lambda$. Будем считать, что $\lambda_{n,m}=1$, если организуется ИНС от n-го узла связи к m-му узлу и $\lambda_{n,m}=0$ – в противном случае.

Для каждого конкретного варианта организации связи Λ может быть задано J множеств булевых матриц распределения ресурсов СС СН $S_j=S_{\text{ус}} \cup S_{\text{лс}}$ ($j=1\ldots J$), заключающееся в конкретизации вариантов распределения линий $S_{\text{лс}}=\{s_{n,m}\}_{\text{лс}}$ и узлов связи $S_{\text{ус}}=\{s_{n,m}\}_{\text{ус}}$ для каждой из ИНС:

$$\{S_j\}_\lambda = \begin{vmatrix} s_{1,1} & s_{1,2} & \ldots & s_{1,M} \\ s_{2,1} & s_{2,2} & \ldots & s_{2,M} \\ \ldots & \ldots & \ldots & \ldots \\ s_{M,1} & s_{M,2} & \ldots & s_{M,M} \end{vmatrix}, \lambda=1\ldots N_\Lambda,$$

где M – общее количество элементов (узлов и линий связи) в системе связи.

В матрицах S_j каждый элемент $s_{n,m}=1$, если линия или узел связи используется в ИНС от n-го узла связи к m-му узлу, и $s_{n,m}=0$ – в противном случае.

Отличие матриц $\{\lambda_{n,m}\}$ и S_j состоит в следующем. Матрица $\{\lambda_{n,m}\}$ задает ИНС в формате «исходящий узел – конечный узел». При этом каждому конкретному ИНС между определенной парой узлов, который соответствует одно-

му из элементов из матрицы $\{\lambda_{n,m}\}$, ставится в соответствие матрица S_j, определяющая, какие элементы сети (узлы и линии связи) образуют этот ИНС.

В дальнейшем будем полагать, что множество Λ задано, и цель оптимизации состоит в выборе матрицы $S_j = S_{\text{ус}} \cup S_{\text{лс}}$ j-го варианта распределения множеств $S_{\text{ус}} = \{s_{n,m}\}_{\text{лс}}$ и $S_{\text{лс}} = \{s_{n,m}\}_{\text{ус}}$ таким образом, чтобы обеспечить наибольшую эффективность СС СН по показателю q в условиях реализации i-ой стратегии нападения.

Пусть система дестабилизирующих воздействий, состоящая из подсистем разведки и нападения, имеет возможность воздействия на любой s-ый элемент системы связи (линию или узел связи). Назовем i-ой стратегией нападения булеву матрицу V_i размером $|S| \times K$ (где $|S|$ – число элементов множества S) с элементами $v_{s,k}$, которые принимают значение $v_{s,k} = 1$, если на s-ый элемент (узел или линию связи) системы связи осуществляется воздействие k-го типа (считаем, что всего осуществляется K типов воздействия), и $v_{s,k} = 0$ – в противном случае:

$$V_i = \begin{vmatrix} v_{1,1} & v_{1,2} & \dots & v_{1,|S|} \\ v_{2,1} & v_{2,2} & \dots & v_{2,|S|} \\ \dots & \dots & \dots & \dots \\ v_{K,1} & v_{K,2} & \dots & v_{K,|S|} \end{vmatrix}.$$

Значение k условно может соответствовать типу воздействия: k=1 – воздействие средств РРТР; k=2 – воздействие средств оптико-электронной разведки; k=3 – воздействие средств компьютерной разведки; k=4 – воздействие средств физического поражения; k=5 – воздействие средств ФП ЭМИ; k=6 – воздействие средств РЭП; k=7 – воздействие средств ИТВ (всего K=7).

При задании интегральных вариантов воздействий на некоторый s-ый элемент (линию или узел связи) СС СН, в s-ом столбце матрицы V_i элементы $v_{s,k}$ принимают значение единица, если k-ый тип воздействия осуществляется на s-ый элемент, и ноль, если k-ый тип воздействия не осуществляется.

Множество стратегий нападения V в качестве элементов будет содержать подмножества всех возможных вариантов воздействия V_i, то есть $V=\{V_i\}$.

7.3. Формализация показателя качества системы связи

Введем матрицу показателей качества функционирования ИНС в системе связи – Q. Очевидно, что каждой комбинации стратегий j, i (которые, в свою очередь, соответствуют комбинации V_i, S_j) соответствует множество показателей качества $\{q_\lambda\}$, где λ – номер ИНС. Таким образом может быть составлена трехмерная матрица показателей качества Q, элементами которой $q_{\lambda,j,i}$ будут показатели качества λ-го ИНС, если на нем используется j-ый вариант распределения линий и узлов связи (соответствует структуре S_j), подвергающийся i-му варианту дестабилизирующего воздействия (соответствует структуре V_i).

Зададим матрицу приоритетности ИНС диагональной матрицей A:

$$A = \begin{vmatrix} \alpha_{1,1} & 0 & \dots & 0 \\ 0 & \alpha_{2,2} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \alpha_{\lambda,\lambda} \end{vmatrix}, \text{ где } \sum_{\lambda=1}^{|\Lambda|} \alpha_{\lambda,\lambda} = 1.$$

Элементы $a_{\lambda,\lambda}$ являются коэффициентами, учитывающими важность λ-го ИНС. Варианты расчета коэффициентов $a_{\lambda,\lambda}$ рассмотрены ранее – см. выражения (6.12-6.15).

Тогда свертка

$$Q\left(S_j, V_i\right) = Q \times A \times S_j \times V_i,$$

будет соответствовать интегральному показателю эффективности системы связи Q, выраженному через стратегии защиты j и нападения i.

Введенная таким образом модель взаимодействия СС СН и системы дестабилизирующих воздействий является достаточно общей и позволяет описывать процессы выбора оптимальных стратегий в достаточно широком классе целей функционирования. Конкретные цели функционирования будут определяться физическим смыслом, вкладываемым в показатель эффективности q.

Учитывая материалы главы 6, за интегральный показатель эффективности СС СН в условиях дестабилизирующих воздействий примем показатель устойчивости – среднесетевую вероятность устойчивости ИНС (выражение (6.11)):

$$P_{\text{у ср}} = \sum_{i=1}^{N} \alpha_i P_{\text{у}i}, \qquad (7.1)$$

где: a_i – значимость i-го ИНС; $P_{\text{у}i} = K_{\text{Г}i}\, P_{\text{св}i}$ – вероятность устойчивости i-го ИНС.

При этом, как показано в главе 6 (рис. 6.2), показатель $P_{\text{у ср}}$ является интегральным и в него могут сворачиваться как частные показатели устойчивости СС СН к применению различных средств поражения (средств физического поражения, средств ФП ЭМИ, РЭП и ИТВ), так и частные показатели разведзащищенности от различных типов разведки (средства РРТР, ОЭС, КР). Таким образом, показатель (7.1) является интегральной характеристикой, по которой можно проводить сравнительный анализ и выбор структур систем связи S_j.

7.4. Формализация процесса взаимодействия системы связи и системы дестабилизирующих воздействий в виде игры

При выборе структуры системы связи S_j в условиях противоборства особенностью является то, что устойчивость отдельных ИНС $P_{\text{у}i}$ и сети в целом $P_{\text{у ср}}$ будут зависеть от стратегий j, i, используемых обеими противоборствующими сторонами соответственно для защиты и нападения. То есть показатель эффективности выбора структуры сети S_j может представляться в виде функции $P_{\text{у ср}}(S_j, V_i)$, определенной на множестве $S \times V$, где $S=\{S_j\}$ – множество решений по построению структуры системы связи S_j в соответствии с j-ой стратегией защиты, а $V=\{V_i\}$ – множество реализаций i-ых стратегий нападения системы дестабилизирующих воздействий.

Критерием выбора эффективной структуры системы связи S_j будет максимизация показателя устойчивости сети $P_{\text{У ср}}$:

$$\max_S P_{\text{У ср}}\left(S_j, V_i\right).$$

При этом целью нападающей стороны является минимизация показателя устойчивости сети $P_{\text{У св}}$:

$$\min_V P_{\text{У ср}}\left(S_j, V_i\right).$$

В условиях таких противоположных целей противоборствующих сторон, процесс их конфликтного взаимодействия может быть формализован на основе минимаксного подхода:

$$\max_S \min_V P_{\text{У ср}}\left(S_j, V_i\right) = \min_V \max_S P_{\text{У ср}}\left(S_j, V_i\right). \qquad (7.2)$$

Ввиду конечности множеств S и V, а также стратегий j и i, возможно составить матрицу показателей устойчивости сети для всех возможных комбинаций стратегий нападения i и стратегии защиты j, которым соответствуют структуры V_i и S_j:

$$\left\{P_{\text{У ср}}\right\} = \begin{vmatrix} P_{\text{У ср}}\left(S_1, V_1\right) & P_{\text{У ср}}\left(S_1, V_2\right) & \dots & P_{\text{У ср}}\left(S_1, V_{|I|}\right) \\ P_{\text{У ср}}\left(S_2, V_1\right) & P_{\text{У ср}}\left(S_2, V_2\right) & \dots & P_{\text{У ср}}\left(S_2, V_{|I|}\right) \\ \dots & \dots & \dots & \dots \\ P_{\text{У ср}}\left(S_{|J|}, V_1\right) & P_{\text{У ср}}\left(S_{|J|}, V_2\right) & \dots & P_{\text{У ср}}\left(S_{|J|}, V_{|I|}\right) \end{vmatrix}, \qquad (7.3)$$

где: $|I|$ – количество элементов в множестве стратегий нападения I, $i \in I$; $|J|$ – количество элементов в множестве стратегий защиты J, $j \in J$.

Решение задачи выбора эффективной структуры системы связи S_j сведется к отысканию седловой точки матрицы (7.3), что равносильно определению номеров j, i для рациональных вариантов структуры системы связи S_j при заданном варианте воздействия V_i.

Наибольшие трудности при выборе структуры системы связи S_j по критерию (7.2) вызывает так называемое «проклятие размерности», то есть лавинообразное нарастание размерности матрицы (7.3) при увеличении числа стратегий нападения i и защиты j. Это делает задачу выбора структуры S_j трудноразрешимой даже при небольшом количестве элементов сети.

Разрешение этой трудности может заключаться к переходе к конечному, относительно небольшому числу вариантов стратегий нападения i и защиты j, а также соответствующим вариантам структуры системы связи S_j и вариантам воздействий V_i.

Еще одной трудностью является то, что на практике часто матрица (7.3) может не иметь седловой точки, что указывает на отсутствие решения в игре с так называемыми «чистыми стратегиями». В этом случае решение может быть получено в игре со «смешанными стратегиями», при которой для каждого из вариантов стратегий нападения i и защиты j назначаются вероятности их применения $P_i(S_j)$ и $P_j(V_j)$, при нормировке

$$\sum_{j=1}^{J} P_j\left(S_j\right) = 1 \text{ и } \sum_{i=1}^{I} P_i\left(V_i\right) = 1.$$

Как доказывается в теории игр [2], в этом случае решение для S_j будет получено вследствие того, что для конечномерных матричных игр решение в смешанных стратегиях всегда существует.

Таким образом, приступая к исследованию любой игры $S \times R$, необходимо сначала проверить, имеет ли матрица (7.3) седловые точки и, соответственно, решения в чистых стратегиях. Если этого нет, то необходимо искать решение в смешанных стратегиях.

Допустим, что найдена смешанная стратегия для системы связи, имеющая вид дискретной функции распределения $F(P_j(S_j))$, $j=1\ldots J$. Тогда при применении нападающей стороной какой-либо чистой i-ой ($i \in I$) стратегии показатель устойчивости системы связи составит

$$P_{\text{у ср}} = P_{\text{у ср}}(S_1, V_i) P_1(S_1) + \ldots + P_{\text{у ср}}(S_j, V_i) P_j(S_j) + \ldots$$
$$\ldots + P_{\text{у ср}}(S_J, V_i) P_J(S_J) \text{ при } \forall i \in I. \qquad (7.4)$$

Аналогично, сделаем предположение о смешанной стратегии системы дестабилизирующих воздействий с дискретной функцией распределения $F(P_i(V_i))$, $i=1\ldots I$, при применении системой связи чистой j-ой ($j \in J$) стратегии защиты, показатель устойчивости системы связи будет равен

$$P_{\text{у ср}} = P_{\text{у ср}}(S_j, V_1) P_1(V_1) + \ldots + P_{\text{у ср}}(S_j, V_i) P_i(V_i) + \ldots$$
$$\ldots + P_{\text{у ср}}(S_j, V_I) P_I(V_I) \text{ при } \forall j \in J. \qquad (7.5)$$

Поскольку соотношения (7.4) и (7.5) справедливы для любых стратегий нападения $i \in I$ и защиты $j \in J$, то эти соотношения можно рассматривать как систему неоднородных линейных уравнений с неизвестными – вероятностями реализации стратегий нападения $P_i(V_i)$ и защиты $P_j(S_j)$, а также итоговым значением устойчивости системы связи $P_{\text{у ср}}$:

$$\begin{cases} P_{\text{у ср}} = P_{\text{у ср}}(S_j, V_1) P_1(V_1) + \ldots + P_{\text{у ср}}(S_j, V_i) P_i(V_i) + \ldots \\ \quad \ldots + P_{\text{у ср}}(S_j, V_I) P_I(V_I), \; j = 1 \ldots J; \\ P_{\text{у ср}} = P_{\text{у ср}}(S_1, V_i) P_1(S_1) + \ldots + P_{\text{у ср}}(S_j, V_i) P_j(S_j) + \ldots \\ \quad + P_{\text{у ср}}(S_J, V_i) P_J(S_J), i = 1 \ldots I; \\ P_1(V_1) + \ldots + P_i(V_i) + \ldots + P_I(V_I) = 1; \\ P_1(S_1) + \ldots + P_i(S_i) + \ldots + P_I(S_I) = 1. \end{cases} \qquad (7.6)$$

В выражении (7.6) значения показателя устойчивости системы связи $P_{\text{у ср}}(S_j, V_i)$ для каждого конкретной комбинации варианта структуры сети S_j и варианта нападения V_i могут быть определены в соответствии с топологической моделью системы связи (рис. 6.2).

Решение системы уравнений (7.6) позволит определить гарантируемый в среднем показатель устойчивости системы связи $P_{\text{у ср}}$, а также наиболее вероятные стратегии нападения $P_i(V_i)$ и защиты $P_j(S_j)$, позволяющие достичь этого значения.

Если по каким-либо причинам прямой вариант решения системы (7.6) окажется неприменимым, то можно перейти к эквивалентной задаче линейного программирования:

$$
\begin{cases}
P_{\text{У ср}}\left(S_j,V_1\right)P_1\left(V_1\right)+\ldots+P_{\text{У ср}}\left(S_j,V_i\right)P_i\left(V_i\right)+\ldots \\
\quad \ldots+P_{\text{У ср}}\left(S_j,V_I\right)P_I\left(V_I\right)-P_{\text{У ср}}=0,\ j=1\ldots J; \\
P_{\text{У ср}}\left(S_1,V_i\right)P_1\left(S_1\right)+\ldots+P_{\text{У ср}}\left(S_j,V_i\right)P_j\left(S_j\right)+\ldots \\
\quad \ldots+P_{\text{У ср}}\left(S_J,V_i\right)P_J\left(S_J\right)-P_{\text{У ср}}=0, i=1\ldots I; \\
P_1\left(V_1\right)+\ldots+P_i\left(V_i\right)+\ldots+P_I\left(V_I\right)=1; \\
P_1\left(S_1\right)+\ldots+P_i\left(S_i\right)+\ldots+P_I\left(S_I\right)=1.
\end{cases}
\tag{7.7}
$$

Таким образом, оценка устойчивости системы связи $P_{\text{У ср}}$ в условиях воздействия системы дестабилизирующих воздействий и определения рациональных структур ее построения S_j может быть представлена в виде упрощенной схемы, представленной на рис. 7.1. С помощью описанного выше подхода может быть решена задача поиска оптимальной структуры системы связи S_j на этапах ее планирования, когда априори неизвестно какую стратегию нападения $P_i(V_i)$ выберет противник.

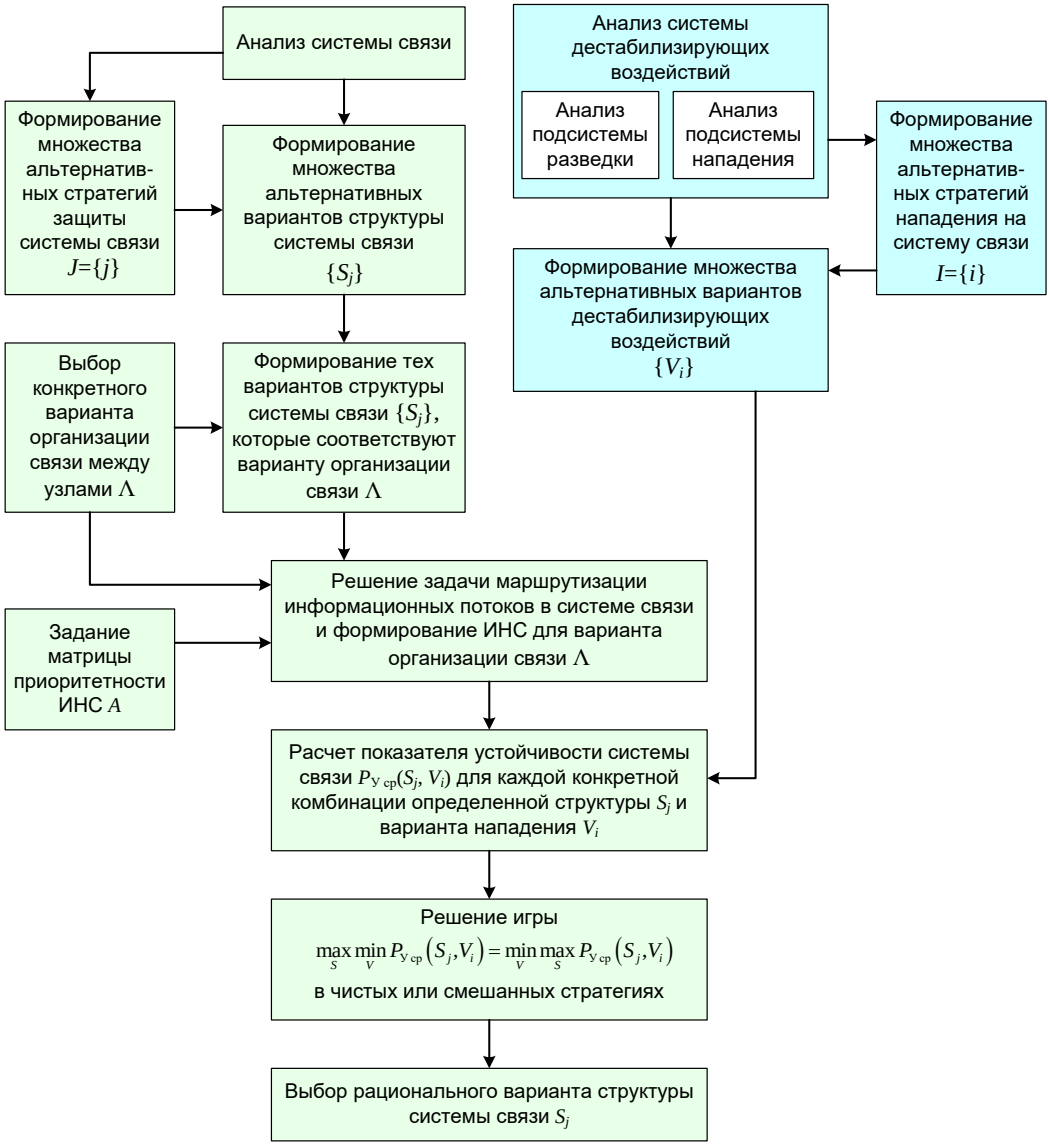

Рис. 7.1. Схема оценки устойчивости системы связи $P_{\text{У ср}}$ и определения рациональной структуры ее построения S_j

7.5. Формализация многоэтапного игрового информационного конфликта системы связи

На этапах оперативного управления системой связи необходимо осуществлять управление ее структурой S_j по результатам наблюдения за конкретными действиями противника по применению им конкретных вариантов дестабилизирующих воздействий V_i. Процесс движения системы связи в пространстве состояний S_j под воздействием V_i будем рассматривать как многоэтапный информационный конфликт.

Сущность информационного конфликта заключается в стремлении каждой стороны к целенаправленному изменению своего состояния и состояния противоборствующей стороны. В этом случае динамику конфликта можно представить, как эволюцию некоторой «метасистемы» более высокого уровня, включающей в себя в качестве составных элементов как систему связи, так и систему дестабилизирующих воздействий.

Для формального описания многоэтапного информационного конфликта примем допущение о дискретном процессе смены состояний S_j и V_i, подобно тому как это рассмотрено в подразделе 4.6. Дискретное представление этапов конфликта позволит более адекватно отразить реальные процессы принятия решений о смене стратегий i, j, а также об изменении состояний сторон V_i, S_j с учетом очередности выполнения различных задач на каждом из этапов. При этом формальной математической схемой модели многоэтапного информационного конфликта будет некоторая временная последовательность смены состояний S_j и V_i.

Рассмотрим фазовое пространство $V \times S$, в котором метасистема «система связи – система дестабилизирующих воздействий» описывает фазовую траекторию $H(S_j, V_i)$, которая, в свою очередь, соответствует динамике совместного изменения состояний S_j и V_i в процессе развития многоэтапного конфликта.

Введем оператор γ, который описывает процесс эволюции метасистемы $H(S_j, V_i)$ в фазовом пространстве $V \times S$, как последовательность смены состояний S_j, V_i в дискретные моменты времени t_n, $n=1\ldots N$:

$$H_0(t_0);$$
$$\gamma_1 : H_0(t_0) \rightarrow H_1(t_1);$$
$$\gamma_2 : H_1(t_1) \rightarrow H_2(t_2);$$
$$\ldots$$
$$\gamma_n : H_{n-1}(t_{n-1}) \rightarrow H_n(t_n);$$
$$\ldots$$
$$\gamma_N : H_{N-1}(t_{N-1}) \rightarrow H_N(t_N),$$

где: n – счетчик этапов многоэтапного информационного конфликта; N – количество этапов информационного конфликта.

Содержание оператора $\gamma_1 \ldots \gamma_N$, в общем случае, может зависеть от номера этапа конфликта n. Однако, если цели конфликтующих сторон не меняются, а в реальной метасистеме «система связи – система дестабилизирующих воздей-

ствий» это именно так, то можно считать, что $\gamma_1 = \gamma_2 = \ldots = \gamma_N$. Таким образом, оператор γ сводится к функции $\gamma(H, t)$.

Целенаправленность эволюции метасистемы заключается в том, что ее траектория $H(S_j, V_i)$ зависит от стратегий нападения i и защиты j, принятых противоборствующими сторонами на каждом этапе конфликта. Таким образом, можно записать:

$$\gamma_n : <H_{n-1}(S_{j-1}, V_{i-1}), t_{n-1}> \rightarrow < H_n(S_j, V_i), t_n >.$$

Исходя из содержания процессов конфликтного взаимодействия сторон в метасистеме «система связи – система дестабилизирующих воздействий», можно принять следующую последовательность изменения состояний. Пусть на n-ом этапе конфликта в соответствии с наблюдаемым состоянием системы связи S_{j-1}, сложившимся на предыдущем этапе t_{n-1}, система дестабилизирующих воздействий принимает i-ую стратегию воздействия и переводит себя в состояние, соответствующее варианту воздействия V_i. Это, в свою очередь, влечет изменение состояния метасистемы $H_{n-1}(S_{j-1}, V_{i-1}) \rightarrow H_n(S_{j-1}, V_i)$. В результате, структура системы связи S_{j-1} перестает удовлетворять требованиям устойчивости по показателю $P_{У\ ср}$. Для обеспечения этих требований система связи формирует j-ую стратегию защиты и переводит себя в состояние S_j. В результате на n-ом этапе конфликта в момент окончания этапа t_n состояние метасистемы изменяется на $H_n(S_{j-1}, V_i) \rightarrow H_n(S_j, V_i)$. Таким образом, процесс изменения состояния метасистемы «система связи – система дестабилизирующих воздействий» на каждом n-ом этапе конфликта можно представить двумя последовательными подэтапами:

$$\begin{aligned} &\gamma_{n,1} : H_{n-1}\left(S_{j-1}, V_{i-1}\right) \rightarrow H_n\left(S_{j-1}, V_i\right); \\ &\gamma_{n,2} : H_n\left(S_{j-1}, V_i\right) \rightarrow H_n\left(S_j, V_i\right). \end{aligned} \tag{7.8}$$

Согласно (7.8), оператор γ_n, определяющий эволюцию состояния метасистемы на n-ом этапе, может быть представлен совокупностью последовательно действующих операторов $\gamma_{n,1}$ и $\gamma_{n,2}$, где $\gamma_{n,1}$ – оператор, отображающий изменения стратегии нападения со стороны системы дестабилизирующих воздействий, $\gamma_{n,2}$ – оператор, отображающий изменения стратегии защиты системы связи.

7.6. Формализация процесса принятия решений в многоэтапном игровом информационном конфликте

Для завершения построения общей формальной схемы многоэтапного конфликта необходимо ввести описание процесса принятия решений на изменение стратегий нападения и защиты.

В общем случае, организация процесса принятия решений о выборе стратегий нападения и защиты может быть определена как многоуровневая иерархическая структура, характерная для каждой из сторон, которая состоит из взаимосвязанных подсистем, элементы которых имеют право принимать решения. В соответствии с принципом принятия решений в иерархической системе, будем считать, что вышестоящий элемент ставит задачу нижестоящему и влияет на него путем изменения задач, введения ограничений или перечислением допустимых альтернатив действий. Нижестоящий элемент свободен в своих дей-

ствиях при выполнении поставленных задач в рамках указанных ограничений или альтернатив. Нижестоящий элемент влияет на решение вышестоящего элемента путем информирования его о принятых решениях и их возможных последствиях. Вышестоящий элемент в соответствии с этой информацией может скорректировать свое решение либо полностью изменить его.

Важной особенностью процессов принятия решений в системе связи и системе дестабилизирующих воздействий является неполная информированность органов управления об обстановке, то есть о значении вектора состояния $H(S_j, V_i)$.

Учитывая формально определенный выше смысл $H(S_j, V_i)$, к основным видам неопределенности можно отнести следующие:

- неопределенность в целях функционирования противоположной стороны;
- неопределенность в представлении внутреннего состояния системы связи S_j, возникающая из-за сложности учета в математической модели всех взаимосвязей между элементами системы, возможной неоптимальности выбора стратегий защиты, ошибок в определении состояния элементов системы и ошибочного прогнозирования изменения их состояния к следующему этапу конфликта;
- неопределенность в представлении состояния системы дестабилизирующих воздействий V_i, возникающая из-за отсутствия точных знаний об ее структуре и параметрах используемых средств, а также о потенциальных стратегиях нападения на последующих этапах конфликта;
- неопределенность в представлении результатов воздействий системы дестабилизирующих воздействий на систему связи и наоборот.

Учет всех указанных типов неопределенности в формальном виде может быть осуществлен через введение некоторых отображений μ и η, отображающих реальное состояние метасистемы $H(S_j, V_i)$ в некоторые ее информационные образы $H^{сс}(S_j, V_i)$ и $H^{сдв}(S_j, V_i)$, которые соответствуют наблюдению состояния $H(S_j, V_i)$ системой связи и системой дестабилизирующих воздействий:

$$\mu : H(S_j, V_i) \rightarrow H^{сдв}(S_j, V_i);$$

$$\eta : H(S_j, V_i) \rightarrow H^{сс}(S_j, V_i),$$

где: μ – отображение, задающее наблюдение (разведку) параметров метасистемы со стороны системы дестабилизирующих воздействий; η – отображение, задающее наблюдение (мониторинг) параметров метасистемы со стороны системы связи.

Состояния $H^{сс}(S_j, V_i)$ и $H^{сдв}(S_j, V_i)$ соответствуют определению противоборствующими сторонами некоторых «кажущихся» образов состояния метасистемы $H(S_j, V_i)$. Фактически, это соответствует выбору наиболее правдоподобных гипотез $H^{сс}(S_j, V_i)$ и $H^{сдв}(S_j, V_i)$ о реальным состоянии системы $H(S_j, V_i)$ по результатам наблюдения η и μ.

В реальных системах, очевидно, всегда существует такое минимальное количество информации, при котором нельзя сделать каких-либо выводов по поводу гипотез $H^{сс}(S_j, V_i)$ и $H^{сдв}(S_j, V_i)$. В терминах данной модели это означает, что существует некоторое предельное количество информации, являющееся ар-

гументом отображений η и μ, которое позволяет выдвинуть гипотезы $H^{сс}(S_j, V_i)$ и $H^{сдв}(S_j, V_i)$ с требуемым уровнем достоверности. В противном случае, отображения η и μ не позволяют сформировать правдоподобные гипотезы $\mu{:}H(S_j, V_i) \to H^{сдв}(S_j, V_i)$ и $\eta{:}H(S_j, V_i) \to H^{сс}(S_j, V_i)$.

Вышерассмотренные свойства процессов конфликтного взаимодействия сторон в метасистеме «система связи – система дестабилизирующих воздействий» и принятые предположения о наблюдаемости состояния $H(S_j, V_i)$ позволяют построить формальную схему поэтапного принятия решений в противоборствующих системах. Декомпозиция процесса принятия решений на l-ом уровне иерархии системы управления (применительно к системе связи) на n-ом этапе может быть представлена последовательностью следующих операций:

- декомпозиция общей цели функционирования системы γ на ряд частных подцелей и далее – на задачи для отдельных элементов и подсистем;
- фиксация смены варианта воздействия со стороны системы дестабилизирующих воздействий с $V_{i\text{-}1}$ на V_i в соответствии с новой i-ой стратегией нападения: $H(S_{j\text{-}1}, V_{i\text{-}1}) \to H(S_{j\text{-}1}, V_i)$;
- формирование гипотезы о состоянии метасистемы на основе результатов наблюдения/мониторинга: η: $H(S_{j\text{-}1}, V_i) \to H^{сс}(S_{j\text{-}1}, V_i)$;
- формирование множества альтернативных j-ых стратегий защиты системы связи и соответствующих им структур $\{S_j\}, j \in J$;
- выбор из множества альтернатив такой оптимальной стратегии j-ой стратегии защиты системы связи и соответствующей ей структуры S_j, которая в условиях наблюдаемого состояния метасистемы $H^{сс}(S_{j\text{-}1}, V_i)$ обеспечивала бы выполнение критерия эффективности $P_{У\ ср} \to \max$;
- реализация j-ой стратегии защиты системы связи путем перехода к S_j структуре: $H(S_{j\text{-}1}, V_i) \to H(S_j, V_i)$.

Такая же последовательность операций характерна и для противоположной стороны – системы дестабилизирующих воздействий. С учетом того, что критерием выбора j-ой стратегии системы связи является максимизация показателя ее устойчивости $P_{У\ ср} \to \max$, а критерием выбора i-ой стратегии системой дестабилизирующих воздействий ее минимизация: $P_{У\ ср} \to \min$, то выражение (7.8) может быть представлено в следующем виде

$$\begin{aligned} &\gamma_{n,1} : H_{n-1}\left(S_{j-1}, V_{i-1}\right) \to H_n\left(S_{j-1}, V_i\right) \Big| P_{У\ ср} \to \min; \\ &\gamma_{n,2} : H_n\left(S_{j-1}, V_i\right) \to H_n\left(S_j, V_i\right) \Big| P_{У\ ср} \to \max. \end{aligned} \tag{7.9}$$

В выражении (7.9) критерий $P_{У\ ср} \to \min$ соответствует подэтапу, на котором «ходит» система дестабилизирующих воздействий, а критерий $P_{У\ ср} \to \max$ – подэтапу, на котором «ходит» система связи.

Введение наблюдений η: $H(S_j, V_i) \to H^{сс}(S_j, V_i)$ в сочетании с принципом последовательного (поэтапного) принятия решений (7.9) превращает процесс оптимизации структуры системы связи S_j (7.2) в многошаговый минимаксный процесс поиска наилучших j-ых стратегий, условных ко всем предыдущим состояниям $H(t_0),\ldots, H(t_{n\text{-}1})$ и наблюдениям $H^{сс}(t_0),\ldots, H^{сс}(t_{n\text{-}1})$ на каждом из n этапов конфликта:

$$S_j^{\text{опт}}(t_n) = \arg\left\{ \max_{\substack{S_j(t_n) \\ S_j(t_{n-1}),\ldots,S_j(t_0),V_i(t_{n-1}),\ldots,V_i(t_0)}} \min_{\substack{V_i(t_n) \\ S_j(t_{n-1}),\ldots,S_j(t_0),V_i(t_{n-1}),\ldots,V_i(t_0)}} \ldots \max_{\substack{S_j(t_1) \\ S_j(t_0),V_i(t_1)}} \min_{\substack{V_i(t_1) \\ S_j(t_0)}} P_{\text{У ср}} \right\}. \quad (7.10)$$

Однако в такой постановке задача оптимизации становится практически нереализуемой из-за необходимости учета и хранения огромного количества информации о состояниях метасистемы «система связи – система дестабилизирующих воздействий» $H(S_j, V_i)$ на всех этапах конфликта $H(t_0),\ldots, H(t_{n-1})$. Тем более, что высокая динамичность современных боевых действий, возможность резких изменений обстановки ставят под сомнение необходимость реального учета всех предыдущих состояний $H(t_0),\ldots, H(t_{n-1})$.

Относительно просто реализуемые технически и вполне пригодные для практики процедуры управления в данных условиях можно получить путем использования теории марковских процессов, в которых учитываются только текущее $H(t_n)$ и предшествующее $H(t_{n-1})$ состояния метасистемы. В этом случае задачу выбора оптимальной структуры системы связи $S_j^{\text{опт}}(t_n)$ можно рассматривать как задачу поиска наилучшей j-ой стратегии, удовлетворяющей критерию $P_{\text{У ср}} \to \max$:

$$S_j^{\text{опт}}(t_n) = \arg\left\{ \max_{\substack{S_j(t_n) \\ S_{j-1}(t_{n-1}),V_i(t_n)}} \min_{\substack{V_i(t_n) \\ S_{j-1}(t_{n-1})}} P_{\text{У ср}} \right\}. \quad (7.11)$$

В соответствии с выражением (7.11), поиск оптимальной структуры системы связи $S_j^{\text{опт}}(t_n)$ на n-ом этапе конфликта сводится к двум подэтапам:

1) оценка устойчивости системы связи $P_{\text{У ср}}$ в предположении, что на данном этапе конфликта нападающая сторона из множества альтернатив выбрала и реализовала такую i-ую стратегию воздействия (вариант нападения V_i), которая соответствует критерию $P_{\text{У ср}} \to \min$ при условии нахождения системы связи в состоянии $S_{j-1}(t_{n-1})$;
2) выбор и реализация системой связи из множества альтернатив той j-ой стратегии защиты (структуры системы связи S_j), которая соответствует критерию $P_{\text{У ср}} \to \max$ при условии нахождения системы связи в состоянии $S_{j-1}(t_{n-1})$ и уже реализованного на данном этапе воздействия $V_i(t_n)$.

Интересным направлением дальнейшего развития подхода (7.11) может являться упреждающее формирование оптимальной структуры системы связи $S_j^{\text{опт}}(t_{n+1})$, основанное на прогнозе того, что система дестабилизирующих воздействий выберет оптимальное воздействие $V_i(t_{n+1})$ по критерию $P_{\text{У ср}} \to \min$ на следующем n+1 этапе конфликта:

$$S_j^{\text{опт}}(t_n) = \arg\left\{ \max_{\substack{S_j(t_{n+1}) \\ S_{j-1}(t_n),V_i(t_{n+1})}} \min_{\substack{V_i(t_{n+1}) \\ S_{j-1}(t_n)}} \max_{\substack{S_{j-1}(t_n) \\ S_{j-2}(t_{n-1}),V_{i-1}(t_n)}} P_{\text{У ср}} \right\}. \quad (7.12)$$

В этом случае поиск превентивно-упреждающей оптимальной структуры системы связи $S_j^{\text{опт}}(t_{n+1})$ на n-ом этапе конфликта сводится к трем подэтапам:

1) выбор и реализация системой связи из множества альтернатив (j-1)-ой стратегии защиты, которая соответствует структуре системы связи

$S_{j-1}(t_n)$ и критерию $P_{У\ ср} \to \max$ при условии, что ранее система связи находилась в состоянии $S_{j-2}(t_{n-1})$, и на данном этапе уже было реализовано воздействие $V_{i-1}(t_n)$;

2) формирование прогнозируемого варианта нападения $V_i(t_{n+1})$ в предположении, что на следующем этапе конфликта t_{n+1} нападающая сторона из множества альтернатив выберет и реализует такую i-ую стратегию воздействия, которая соответствует критерию $P_{У\ ср} \to \min$ при условии текущего нахождения системы связи в состоянии $S_{j-1}(t_n)$;
3) выбор и реализация системой связи из множества альтернатив j-ой стратегии защиты, которая соответствует структуре системы связи $S_j(t_{n+1})$ и критерию $P_{У\ ср} \to \max$ при условии нахождения системы связи в состоянии $S_{j-1}(t_n)$ и прогнозируемого воздействия $V_i(t_{n+1})$.

Представленные подходы позволяют существенно упростить задачу поиска оптимальной структуры системы связи $S_j^{опт}(t_n)$, разбив ее на ряд последовательно решаемых частных задач максимизации и минимизации.

Выводы по седьмой главе

На основе показателя устойчивости системы связи, разработанного в предыдущей главе, предложена модель, которая в формализме теории игр позволяет учесть различные комбинации структур системы связи и вариантов дестабилизирующего воздействия. Показано, что на основе игры с прямыми или смешанными стратегиями возможно обосновать наиболее вероятные варианты дестабилизирующих воздействий, а также рациональную структуру системы связи в информационном конфликте. Развивая игровую модель в направлении моделирования многоэтапного информационного конфликта, предложена формализация принятия решений противоборствующими сторонами при выборе стратегий на каждом из этапов конфликта. Предложена формализация правила выбора стратегии защиты и соответствующей ей структуры системы связи в виде минимаксного критерия. Данный критерий позволяет осуществить поиск рациональной структуры системы связи как при оперативном (с учетом сложившейся ситуации на этом же этапе информационного конфликта), так и при превентивном принятии решении (на следующем этапе информационного конфликта, с учетом прогнозируемой стратегии действий противника).

Заключение

На протяжении 80-90-х гг. прошлого века информационные технологии, за счет своего революционного развития, проникали во все сферы жизнедеятельности человека. Это в конечном итоге привело к тому, что они сформировали новое технологическое ядро систем государственного и военного управления – системы связи специального назначения. Одновременно с этим, в условиях развития теории и практики вооруженной борьбы, возникают новые, специфичные именно для этих систем связи угрозы, например, такие как информационно-технические воздействия или средства компьютерной разведки. Кардинальным образом меняются формы и способы противодействия системам связи в процессе военных действий. Следствием этого является насущная потребность в уточнении и развитии существующих моделей систем связи специального назначения в условиях дестабилизирующих воздействий и ведения разведки.

Данная работа направлена на формирование новых описательных моделей системы связи специального назначения, систем дестабилизирующего воздействия и разведки, которые бы учитывали их современное состояние и тенденции развития на ближайшую перспективу. Кроме того, в работе представлены результаты разработки формальных моделей системы связи, функционирующей в условиях дестабилизирующих воздействий и ведения разведки. Отличительной особенностью разработанных формальных моделей является формализация процесса взаимодействия системы связи, системы дестабилизирующего воздействия и системы разведки в виде информационного конфликта. Именно этот подход и отличает данную работу от других работ по тематике устойчивости, живучести или помехозащищенности систем специальной связи.

Автор выражает надежду на то, что результат его работы заинтересует широкий круг специалистов, а материал, представленный в монографии, вызовет благосклонное внимание соискателей ученых степеней, военных и технических специалистов, которые выбрали сложные и увлекательные проблемы повышения устойчивости, живучести и помехозащищенности систем связи, в качестве области своих научных интересов.

Список сокращений

2B1Q – 2 Binary 1 Quaternary – линейное кодирование, в котором каждые два бита (2B) передаются за один такт (1) сигналом, имеющим четыре состояния (Q – Quadra).
A1 – амплитудная манипуляция.
A3 – амплитудная модуляция.
A3E – двухканальная амплитудная модуляция.
ADI – Alternate Digit Inversion Code – линейное кодирование с поразрядно-чередующейся инверсией.
AG – Access Gateway – шлюз доступа.
AMI – Alternate Mark Inversion – биполярное линейное кодирование с чередующейся инверсией на «1».
ANI – Access Network Interface – интерфейс доступа к сети.
APSK – Amplitude Phase Shift Keying – амплитудно-фазовая манипуляция.
ARP – Address Resolution Protocol – протокол разрешения адресов.
ASON – Automatic Switched Optical Network – автоматически коммутируемая оптическая сеть.
ASTN – Automatic Switched Transport Network – автоматически коммутируемая транспортная сеть.
ATM – Asynchronous Transfer Mode – технология асинхронной передачи данных.
B8ZS – Bipolar with 8-Zeros Substitution – биполярное линейное кодирование с заменой 8-ми нулей.
BGP – Border Gateway Protocol – протокол маршрутизации межсетевого шлюза.
BIOS – Basic Input-Output System – базовая система ввода-вывода.
BPI – Bit Interleaved Party – способ контроля четности для мониторинга ошибок в модулях STM-n в технологии SDH.
CAC – Call Admission Control – контроль за установлением соединений.
CDMA – Code Division Multiple Access – множественный доступ с кодовым разделением.
CMI – Coded Mark Inversion Code – линейное кодирование с инверсией кодовых комбинаций.
COFDM – Coded Orthogonal Frequency Division Multiplexing – ортогональное частотное разделение каналов с кодированием.
CoS – Class of Service – класс обслуживания.
CQ – Class based Queuing – класс приоритетной дисциплины обслуживания очередей.
CRC – Circle Redundancy Check – контрольная сумма.

CSI – Conflict System Interconnection Reference Model – эталонная модель взаимодействия конфликтующих систем.

CSMA/CA Carrier Sense Multiple Access With Collision Avoidance – множественный доступ с контролем несущей и предотвращением коллизий.

CSMA/CD – Carrier Sense Multiply Access / Collision Detection – метод множественного доступа с контролем несущей и обнаружением коллизий.

CWDM – Wavelength-Division Multiplexing – мультиплексирование с разделением по длине волны.

CES – Circuit Emulation Service – служба эмуляции соединений.

DAMA – Demand Assigned Multiple Access – многостанционный доступ с предоставлением каналов по требованию.

DCGS – Distributed Common Ground System – Автоматизированная система сбора, обработки и распределения разведывательной информации.

DDOS – Distributed Denial of Service – распределённая атака «отказ в обслуживании».

DHCP – Dynamic Host Configuration Protocol – протокол автоматического назначения адресов.

DiffServ – Differentiated Service – дифференцированное обслуживание.

DNS – Domain Name System – система доменных имен.

DOS – Denial of Service – атака «отказ в обслуживании».

DVB – Digital Video Broadcasting – стандарт цифрового видеовещания.

DVB-RSC – Digital Video Broadcasting with Return Satellite Chanel – стандарт спутниковой цифровой передачи данных с обратным каналом через спутник.

DVB-S – Digital Video Broadcasting – Satellite – стандарт спутниковой цифровой передачи данных.

DVMRP – Distance Vector Multicast Routing Protocol – протокол дистанционно-векторной многоадресной маршрутизации.

DWDM – Dense Wavelength Division Multiplexing – плотное мультиплексирование с разделением по длине волны.

E1 – стандарт цифровой передачи данных PDH, соответствующий скорости передачи 2048 кбит/с.

E2 – стандарт цифровой передачи данных PDH, соответствующий скорости передачи 8448 кбит/с.

E3 – стандарт цифровой передачи данных PDH, соответствующий скорости передачи 34368 кбит/с.

E4 – стандарт цифровой передачи данных PDH, соответствующий скорости передачи 139264кбит/с.

EBGP – External Border Gateway Protocol – внешний протокол маршрутизации межсетевого шлюза.

EGP – Exterior Getaway Protocols – протокол «наружного» шлюза.

EIGRP – Enhanced Interior Gateway Routing Protocol – дистанционно-векторный протокол динамической маршрутизации.
EoT – Ethernet-over-Transport – технология работы сети Ethernet поверх транспортных протоколов.
F1 – амплитудная манипуляция.
F1B – одноканальная частотная манипуляция.
F3 – частотная модуляция.
FDMA – Frequency Division Multiple Access – множественный доступ с разделением по частоте.
FEC – Forward Error Correction – прямая коррекция ошибок.
FR – Frame Relay – технология пакетной сети.
FSK – Frequency Shift Keying – частотная манипуляция.
G1B – одноканальная фазовая манипуляция.
G3E – фазовая модуляция.
GIG – Global Information Grid – глобальная информационная сеть.
GII – Global Information Infrastructure – концепция глобальной информационной инфраструктуры.
GMSK – Gaussian Minimum Shift Keying – гауссовская минимальная манипуляция.
H3E – одноканальная модуляция с полной несущей (разрешена для использования только на частоте 2182 кГц).
HDB3 – High-Density Bipolar 3-Zeros – биполярное линейное кодирование высокой плотности с заменой 3-ех нулей.
HDWDM – High-Dense WDM – сверхплотное мультиплексирование с разделением по длине волны.
HSRP – Hot Standby Router Protocol – протокол виртуализации маршрутизатора.
IBGP – Internal Border Gateway Protocol – внутренний протокол маршрутизации межсетевого шлюза.
ICMP – Internet Control Message Protocol – протокол межсетевых управляющих сообщений в IP сетях.
IGMP – Internet Group Management Protocol – протокол управления групповой передачей данных, основанных на протоколе IP.
IGRP – Interior Gateway Routing Protocol – внутренний протокол маршрутизации.
IMS – IP Multimedia Subsystem – протокол передачи мультимедийного содержимого в IP сетях.
IntServ – Integrated Service – интегрированное обслуживание.
IP – Internet Protocol – интернет протокол адресации.
Ipv4 – Internet Protocol version 4 – интернет протокол, в котором под адрес отводиться 4 байта.
Ipv6 – Internet Protocol version 6 – интернет протокол, в котором под адрес отводиться 6 байтов.
IPSec – IP Security – набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP.

ISDN – Integrated Services Digital Network – цифровая сеть с интеграцией услуг.

IS-IS – Intermediate System to Intermediate System – протокол динамической маршрутизации, основанный на технологии оценки состояния каналов.

ISO – International Organization for Standardization –международная организация по стандартизации.

J3E – одноканальная амплитудная модуляция с подавленной несущей.

J7D – амплитудная модуляция цифрового первичного сигнала основной несущей с одной боковой полосой и подавленной несущей.

L2TP – Layer 2 Tunneling Protocol – протокол туннелирования второго уровня для поддержки виртуальных частных сетей.

LDCP – Low-Density Parity-Check Code – код с малой плотностью проверок на чётность.

M2M – Machine-to-Machine – технология межмашинного взаимодействия.

MANET – Mobile Ad hos Network – беспроводная децентрализованная самоорганизующаяся сеть.

MARS – Multicast Address Resolution Server – сервер разрешения широковещательных адресов.

MCPC – Multiple Channels per Carrier – несколько каналов на одну несущую.

MCU – Multipoint Control Unit – блок многоточечного управления.

MF-TDM – Multi-Frequency TDM – частотно-временное мультиплексирование каналов.

MF-TDMA – Multi-Frequency TDMA – многочастотный доступ с разделением по времени.

MG – Media Gateway – медиашлюз или транспортный шлюз.

MGC – Media Gateway Controller – контроллер медиашлюза.

MMF – Multi Mode Fiber – многомодовый оптоволоконный кабель.

MNS – Network Management System – система управления сетью.

MPCP – Multi-Point Control Protocol – протокол управления множеством узлов, который обеспечивает порядок передачи данных и устраняет коллизии.

MPLS – Internet Protocol and Multiprotocol label switching – интернет протокол быстрой коммутации по меткам.

MPLS-TE – MPLS Traffic Engineering – протокол MPLS с поддержкой функций управления трафиком.

MSTP – Multiple Spanning Tree Protocol – составной протокол покрывающего дерева.

NACF – Network Attachment and Control Functions – функции управления доступом пользователей к ресурсам сети.

NGN – Next Generation Networks – сеть следующего поколения.

NRZ – Non Return to Zero – линейное однополярное кодирование без возвращения к нулю.
NRZI – Non Return to Zero with ones Inverted – линейное кодирование с инверсией при единице.
NP – Non priority – неприоритетный трафик.
OFDM – Orthogonal frequency-division multiplexing — мультиплексирование с ортогональным частотным разделением каналов.
OQPSK – Offset QPSK – квадратурно-фазовая манипуляция со сдвигом частоты.
OSE/RM – Open System Environment / Reference Model – эталонная модель среды открытых систем.
OSI – Open System Interconnect – эталонная модель взаимодействия открытых систем.
OSPF – Open Shortest Path First – протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала.
OTDM – Optical Time Division Multiplexing – оптическое временное мультиплексирование каналов.
OTH – Optical Transport Hierarchy – оптическая транспортная иерархия.
OTN – Optical Transport Network – оптическая транспортная сеть.
OTU – Optical Transport Unit – оптический транспортный блок.
P – Priority – приоритетный трафик.
PCM – Pulse Code Modulation – импульсно-кодовая модуляция.
PDH – Plesiochronic Digital Hierarchy – плезиохронная цифровая иерархия.
PES – PSTN/ISDN Emulation Subsystem – подсистема эмуляции телефонных и ISDN сетей.
PIM – Protocol Independent Multicast – протокол независимого сетевого многоадресного вещания.
PIM-DM – Protocol Independent Multicast – Dense Mode – протокол независимого сетевого многоадресного вещания для высокоплотных групп получателей.
PIM-SM – Protocol Independent Multicast – Sparse Mode – протокол независимого сетевого многоадресного вещания для рассредоточенных групп.
PIM-SSM – Protocol Independent Multicast – Source Specific Mode – протокол независимого сетевого многоадресного вещания.
PNNI – Private Network-to-Network Interface – иерархический динамический протокол маршрутизации с установлением соединений основанный на анализе состояния каналов.
PON – Passive Optical Network – технология пассивной оптической сети.
PSK – Phase Shift Keying – фазовая манипуляция.

PVSTP – Per-VLAN Spanning Tree Protocol – расширенная версия протокола STP для функционирования в виртуальных локальных сетях.
QAM – Quadrature Amplitude Modulation – квадратурная амплитудная модуляция.
QoS – Quality of Service – качество обслуживания.
QPSK – Quadrature Phase Shift Keying – квадратурная фазовая манипуляция.
R3E – одноканальная амплитудная модуляция с ослабленной несущей.
RACF – Resource and Admission Control Functions – функции управления сетевыми ресурсами.
RACF – Resource and Admission Control Functions – функции управления сетевыми ресурсами.
RAG – Residential Access Gateway – резидентный шлюз доступа.
RED – Random Early Detection – механизм раннего обнаружения перегрузок.
RIP – Routing Information Protocol – внутренний протокол маршрутизации.
RSTP – Rapid Spanning Tree Protocol – быстрый протокол покрывающего дерева
RSVP – Resource ReSerVation Protocol – протокол резервирования ресурсов.
RT – Real Time – трафик «реального времени».
SBC – Session Border Controller – пограничный шлюз, являющийся контроллером соединений.
SBC – Session Border Controller – пограничный контроллер соединений.
SCPC – Single Channel per Carrier – один канал на несущую
SDH – Synchronous Digital Hierarchy – синхронная цифровая иерархия.
SG – Signalling Gateway – сигнальный шлюз.
SIP – Session Initiation Protocol – протокол установления сеанса для обмена мультимедийными данными.
SLA – Service Level Agreement – соглашение об уровне обслуживания.
SMF – Single Mode Fiber – одномодовый оптиволоконный кабель.
SSC – Streaming Service Component – элемент управления потоковыми сообщениями.
STANAG – STANdardization AGreement – семейство протоколов, стандартизированных НАТО для передачи данных (STANAG-4285, STANAG-4444, STANAG-4538, STANAG-5066 и т.д.).
STM – Synchronous Transport Module – синхронный транспортный модуль.
STP – Screening Twisted Pair – экранированная витая пара.
STP – Spanning Tree Protocol – протокол остовного дерева.

TCM – Trellis Coded Modulation – решетчатая кодированная модуляция.
TDM – Time Division Multiplexing – временное мультиплексирование.
TDMA – Time Division Multiple Access – множественный доступ с разделением по времени.
TDMoIP – Time Division Multiplexing over IP – протокол эмуляции традиционных каналов с временным мультиплексированием (E1, T1, E3 или T3) в IP сетях.
TDMoP – Time Division Multiplexing over Packet networks – протокол эмуляции традиционных каналов с временным мультиплексированием (E1, T1, E3 или T3) в сетях с коммутацией пакетов.
TE – Traffic Engineering – управление трафиком.
TG – Trunking Gateway – транкинговый шлюз.
TMN – Telecommunications Management Network – концепция управления сетью.
UTP – Unshielded Twisted Pair – неэкранированная витая пара.
VLAN – Virtual Local Area Network – виртуальная локальная компьютерная сеть.
VPLS – Virtual Private LAN Service – сервис виртуальной частной сети.
VPN – Virtual Private Network – виртуальная частная сеть.
VRRP – Virtual Router Redundancy Protocol – протокол виртуализации маршрутизатора.
VSAT – Very Small Aperture Terminal – технология сети спутниковой связи на основе использования малых земных станций.
WDM – Wave Division Multiplexing – технология волнового мультиплексирования.
WDM – Wavelength-Division Multiplexing – мультиплексирование каналов с разделением по длине волны.
АСУ – автоматизированная система управления.
АСУС – автоматизированная система управления связью.
АТС – автоматическая телефонная станция.
АФАР – активная фазированная антенная решетка.
АФУ – антенно-фидерное устройство.
БД – база данных.
БИС – большая интегральная схема.
БПЛА – беспилотный летательный аппарат.
БРПД – баллистическая ракета подводной лодки.
БЧХ – помехоустойчивый код Боуза-Чоудхури-Хоквенгема.
ВВС – Военно-воздушные силы.
ВВТ – вооружение и военная техника.
ВМГ – взрывомагнитный генератор.
ВМС – Военно-морские силы.
ВОЛС – волоконно-оптическая линия связи.
ВС – Вооруженные силы.
ВТО – высокоточное оружие.

ВЦ – вычислительный центр.
ГЗЛА – гиперзвуковой летательный аппарат.
ДВ – длинные волны.
ДКМВ – декаметровые волны.
ДМВ – децеметровые волны.
ДРГ – диверсионно-разведывательная группа.
ЕСЭ – Единая сеть электросвязи (РФ).
ЗПП – забрасываемый передатчик помех.
ИБ – информационная безопасность.
ИКС – инфокоммуникационная система.
ИКС СН – инфокоммуникационная система специального назначения.
ИНС – информационное направление связи.
ИПб – информационное противоборство.
ИПВ – информационно-психологическое воздействие.
ИРИ – источник радиоизлучения.
ИС – интегральная схема.
ИТВ – информационно-техническое воздействие.
КА – космический аппарат.
КВ – короткие волны.
КПД – коэффициент полезного действия.
КР – компьютерная разведка.
ЛПР – лицо, принимающее решения.
ЛЭП – линия электропередачи.
МБР – межконтинентальная баллистическая ракета.
МВША – малогабаритная высокоскоростная широкодиапазонная аппаратура.
МВ – метровые волны.
ММВ – миллиметровые волны.
МО – Министерство обороны.
МОП – металл-оксид-полупроводник (технология создания полупроводниковых устройств).
МСЭ-Т – сектор стандартизации электросвязи Международного союза электросвязи.
НАТО – Организация североатлантического договора.
НМА – научно-методический аппарат.
ОМП – оружие массового поражения.
ОСШ – отношения мощности сигнала к мощности шума.
ОТС – организационно-техническая система.
ОЭР – оптико-электронная разведка.
ОЦК – основной цифровой канал.
ПО – программное обеспечение.
ППРЧ – псевдослучайная перестройка рабочей частоты.
ПРО – противоракетная оборона.
ПС ЭМВ – преднамеренное силовое электромагнитное воздействие.
ПУ – пункт управления.

ПЭМИН – побочные электромагнитные излучения и наводки.
РЛР – радиолокационная разведка.
РР – радиоразведка.
РРЛ – радиорелейная линия.
РРТР – радио- и радиотехническая разведка.
РС – помехоустойчивый код Рида-Соломона.
РТР – радиотехническая разведка.
РФ – Российская Федерация.
РЭБ – радиоэлектронная борьба.
РЭП – радиоэлектронное подавление.
РЭПр – радиоэлектронное поражение.
РЭС – радиоэлектронное средство.
СБИС – сверхбольшая интегральная схема.
СВ – средние волны (электромагнитный диапазон).
СВ – сухопутные войска.
СВЧ – сверхвысокие частоты.
СДВ – сверхдлинные волны.
СМВ – сантиметровые волны.
СМО – система массового обслуживания.
СНИО – самонаводящиеся на излучение оружие.
СНЧ – сверхнизкие частоты.
СРНС – спутниковая радионавигационная система.
СС – система связи.
СС ОП – система связи общего пользования.
СС СН – система связи специального назначения.
ССС – спутниковая система связи.
СУБД – система управления базой данных.
США – Соединенные Штаты Америки.
ТВД – театр военных действий.
ТКС – телекоммуникационная система.
ТРРЛ – тропосферная радиорелейная линия.
ТТХ – тактико-технические характеристики.
ТфОП – телефонная сеть общего пользования.
УАБ – управляемая авиабомба.
УКВ – ультракороткие волны.
УС – узел связи.
ФАР – фазированная антенная решетка.
ФП – физическое поражение.
ФП ЭМИ – функциональное поражение электромагнитным излучением.
ШПС – широкополосный сигнал.
ЭДС – электродвижущая сила.
ЭМИ – электромагнитное излучение.
ЭМП – электромагнитное поле.

Список используемых обозначений

Обозначения, используемые в 4-ой главе

d – оперативная информация;

d_1 – оперативная информация о состоянии объекта защиты S_1, получаемая системами мониторинга ОТС S_1;

d_2 – оперативная информация о состоянии объекта защиты S_1, получаемая системами разведки ОТС S_2;

$e_{ад}$ – единица показателя адекватности управления в ОТС;

$e_{непр}$ – единица показателя непрерывности управления в ОТС;

$e_{оп}$ – единица показателя оперативности управления в ОТС;

$e_{скр}$ – единица показателя скрытности управления в ОТС;

$e_{ус}$ – единица показателя устойчивости управления в ОТС;

F_1 – функция выигрыша ОТС S_1;

F_2 – функция выигрыша ОТС S_2;

I – множество стратегий нападения;

i – стратегия нападения ОТС S_2 на ОТС S_1, включающая в себя стратегии ведения разведки $i_р$ и использования средств нападения $i_н$;

$i_н$ – стратегия использования средств нападения ОТС S_2;

$i_{н\ ИТВ}$ – стратегия нападения ОТС S_2 средствами и способами ИТВ;

$i_{н\ ИТВ}^{защ}$ – стратегия защиты средств ИТВ в составе ОТС S_2 от контратакующих воздействий со стороны ОТС S_1;

$i_{н\ РЭП}$ – стратегия нападения ОТС S_2 средствами РЭП;

$i_{н\ РЭП}^{защ}$ – стратегия защиты средств РЭП в составе ОТС S_2 от контратакующих воздействий со стороны ОТС S_1;

$i_{н\ ФП}$ – стратегия нападения ОТС S_2 средствами физического (огневого) поражения;

$i_{н\ ФП\ ЭМИ}$ – стратегия нападения ОТС S_2 средствами ФП ЭМИ;

$i_{н\ ФП\ ЭМИ}^{защ}$ – стратегия защиты средств ФП ЭМИ в составе ОТС S_2 от контратакующих воздействий со стороны ОТС S_1;

$i_{н\ ФП}^{защ}$ – стратегия защиты средств физического (огневого) поражения ОТС S_2 от контратакующих воздействий со стороны ОТС S_1;

$i_н^{защ}$ – стратегия защиты средств нападения ОТС S_2 от контратакующих воздействий со стороны ОТС S_1;

$i_р$ – стратегия ведения разведки со стороны ОТС S_2;

$i_{р\ КР}$ – стратегия ведения компьютерной разведки со стороны ОТС S_2;

$i_{р\ КР}^{защ}$ – стратегия защиты средств компьютерной разведки ОТС S_2 от от контратакующих воздействий со стороны ОТС S_1;

$i_{р\ ОЭР}$ – стратегия ведения ОЭР со стороны ОТС S_2;

$i_{р\ ОЭР}^{защ}$ – стратегия защиты средств ОЭР в составе ОТС S_2 от контратакующих воздействий со стороны ОТС S_1;

$i_{р\ РРТР}$ – стратегия ведения РРТР со стороны ОТС S_2;

$i_{р\ РРТР}^{защ}$ – стратегия защиты средств РРТР в составе ОТС S_2 от контратакующих воздействий противоборствующей стороны;

$i_{р}^{защ}$ – стратегия защиты средств разведки от контратакующих воздействий со стороны ОТС S_1;

J – множества стратегий защиты;

j – стратегия защиты ОТС S_1;

$j_{сс}$ – стратегия защиты элементов СС СН в составе ОТС S_1;

$j_{ИТВ}$ – стратегия контратак средствами ИТВ в составе ОТС S_1 на нападающую ОТС S_2;

$j_{ИТВ}^{защ}$ – стратегия защиты СС СН в составе ОТС S_1 от средств ИТВ нападающей ОТС S_2;

$j_{КР}$ – стратегия контратак средствами компьютерной разведки ОТС S_1 на нападающую ОТС S_2;

$j_{КР}^{защ}$ – стратегия защиты СС СН в составе ОТС S_1 от средств компьютерной разведки нападающей ОТС S_2;

$j_{лс}$ – стратегия управления конфигурацией и режимами работы линий связи СС СН;

$j_{н}$ – стратегия контратак ОТС S_1 на средства нападения ОТС S_2;

$j_{н}^{защ}$ – стратегия защиты СС СН в составе ОТС S_1 от средств нападения ОТС S_2;

$j_{ОЭР}$ – стратегия контратак ОТС S_1 на средства ОЭР нападающей ОТС S_2;

$j_{ОЭР}^{защ}$ – стратегия защиты СС СН в составе ОТС S_1 от средств ОЭР нападающей ОТС S_2;

$j_{р}$ – стратегия контратак ОТС S_1 на средства разведки ОТС S_2;

$j_{р}^{защ}$ – стратегия защиты СС СН в составе ОТС S_1 от средств ведения разведки ОТС S_2;

$j_{РРТР}$ – стратегия контратак средств РРТР нападающей стороны;

$j_{РРТР}^{защ}$ – стратегия защиты СС СН в составе ОТС S_1 от средств РРТР нападающей ОТС S_2;

$j_{РЭП}$ – стратегия контратак ОТС S_1 на средства РЭП нападающей ОТС S_2;

$j_{РЭП}^{защ}$ – стратегия защиты СС СН от средств РЭП нападающей ОТС S_2;

$j_{ус}$ – стратегия управления конфигурацией и режимами работы узлов связи СС СН в составе ОТС S_1;

$j_{ФП}$ – стратегия контратак ОТС S_1 на средства физического (огневого) поражения нападающей ОТС S_2;

$j_{ФП\,ЭМИ}$ – стратегия контратак ОТС S_1 на средства ФП ЭМИ нападающей ОТС S_2;

$j_{ФП\,ЭМИ}^{защ}$ – стратегия защиты СС СН в составе ОТС S_1 от средств ФП ЭМИ нападающей ОТС S_2;

$j_{ФП}^{защ}$ – стратегия защиты СС СН в составе ОТС S_1 от средств физического (огневого) поражения нападающей ОТС S_2;

k – счетчик этапов информационного конфликта;

N – количество этапов информационного конфликта;

$P_{акт}$ – вероятность обеспечения актуальности информации;

$P_{без}$ – вероятность обеспечения в СС СН требуемого уровня безопасности связи;

$P_{дост}$ – вероятность достоверности информации;

$P_{дост}^{треб}$ – требуемый уровень достоверности информации;

$P_{полн}$ – вероятность полноты информации;

$P_{св}$ – вероятность обеспечения в СС СН требуемого уровня своевременности связи;

Q – совокупность показателей, которые характеризуют качество формирования ($Q_{форм}$), передачи ($Q_{прд}$), хранения ($Q_{хр}$), обработки ($Q_{обр}$) и представления ($Q_{пр}$) информации в ОТС;

$Q_{обр}$ – показатель, который характеризует качество обработки информации в ОТС;

$Q_{пр}$ – показатель, который характеризует качество представления (визуализации) информации в ОТС для лиц, принимающих решения;

$Q_{прд}$ – показатель, который характеризует качество передачи информации в ОТС;

$Q_{форм}$ – показатель, который характеризует качество формирования информации в ОТС;

$Q_{хр}$ – показатель, который характеризует качество хранения информации в ОТС;

$R_{сс}$ – ресурс СС СН;

$R_{ИТВ}$ – ресурс средств ИТВ;

$R_{КР}$ – ресурс средств компьютерной разведки;

$R_{лс}$ – ресурс совокупности линий связи в составе СС СН;

$R_{н}$ – ресурс средств нападения;

$R_{ОЭР}$ – ресурс средств ОЭР;

$R_{р}$ – ресурс средств разведки;

$R_{РРТР}$ – ресурс средств РРТР;

$R_{РЭП}$ – ресурс средств РЭП;

$R_{ус}$ – ресурс совокупности узлов связи в составе СС СН;

$R_{ФП}$ – ресурс средств физического (огневого) поражения;

$R_{ФПЭМИ}$ – ресурс средств ФП ЭМИ;

S_1 – ОТС, соответствующая объекту защиты, в состав которой входит СС СН;

S_2 – ОТС, соответствующая субъекту нападения, содержащая в своем составе подсистему разведки и подсистему нападения;

t_k – момент времени окончания k-го этапа информационного конфликта;

$T_{изм}$ – среднее время изменения реальной обстановки, появления новых или изменения существующих объектов или явлений в процессе функционирования ОТС;

$T_{ик}$ – длительность информационного конфликта;

$T_{обн}$ – среднее или фиксированное время обновления информации в системе управления;

$T_{обр}$ – среднее время обработки информации в управляющей системе.

$T_{пр}$ – среднее время представления информации органу или лицу, принимающему решение;

$T_{прд}$ – время передачи информации;

$T_{прд}$ – среднее время передачи информации по СС СН;

$T_{прд}^{треб}$ – требуемое время передачи информации, в течение которого информация сохраняет свою актуальность (оперативную ценность);

$T_{форм}$ – среднее время формирования информации о новых событиях и явлениях реальной обстановки;

$T_{хр}$ – среднее время хранения информации;

U – вектор качества управления в ОТС S_1;

$U_{ад}$ – адекватность управления;

$U_{непр}$ – непрерывность управления;

$U_{оп}$ – оперативность управления;

$U_{скр}$ – скрытность управления;

$U_{ус}$ – устойчивость управления;

V – объем информации;

$V_{к}$ – объем командной (распорядительной) информации;

$V_{пос}$ – объем постоянной информации;

$V_{тек}$ – объем текущей информации;

x – абсолютное значение некоторого показателя ОТС;

$x_{ид}$ – некоторое идеальное значение показателя x в условиях отсутствия дестабилизирующих воздействий на элементы ОТС;

$x^{норм}$ – нормированное значение показателя x;

γ – информационный ущерб;

Δt_k – длительность k-го этапа информационного конфликта;

$\Delta\xi_1$ – изменение уровня выигрыша ОТС S_1 в ходе k-го этапа информационного конфликта;

$\lambda_{изм} = 1/T_{изм}$ – средняя интенсивность (темп) изменения реальной обстановки, появления новых или изменения существующих объектов или явлений в процессе функционирования ОТС;

ξ_1 – показатель выигрыша ОТС S_1;

$\xi_{1\ ож}$ – некоторый усредненный удельный (в единицу времени) ожидаемый выигрыш ОТС S_1 от применения управляемых средств связи, в отсутствии дестабилизирующих воздействий на элементы СС СН;

ξ_1^0 – выигрыш ОТС S_1, в отсутствие дестабилизирующих воздействий нападающей ОТС;

$\xi_1^{инт}$ – средний интегральный выигрыш ОТС S_1 за время конфликта $T_{ик}$;

ξ_2 – показатель выигрыша ОТС S_2;

$\xi_2^{инт}$ – средний интегральный выигрыш ОТС S_2 за время конфликта $T_{ик}$;

$\tau_1^{защ}$ – длительность этапа защиты ОТС S_1 от ОТС S_2;

$\tau_1^{реак}$ – время реакции управляющей системы ОТС S_1;

$\tau_2^{нап}$ – длительность этапа нападения ОТС S_2 на ОТС S_1;

$\tau_2^{реак}$ – время реакции управляющей системы ОТС S_2;

ψ – семантическая (энтропийная) ценность информации.

Обозначения, используемые в 5-ой главе

$|\cdot|$ – количество элементов в множестве $(\cdot)$;

$\mathbb{E}(\cdot)$ – область значений $(\cdot)$;

a – алгоритм, как часть элемент математического обеспечения системы связи;

$A=\bigcup_{l} A_l$ – множество элементов алгоритмов, составляющих математическое обеспечение системы связи;

$A_l=\bigcup_{\Pi_l} A_{l,\pi}$ – множество алгоритмов, являющихся частью математического обеспечения, реализующих функционирование протоколов Π_l на l-ом уровне системы связи;

$A_{l,\pi}=\{a \mid a\in D(\pi_l)\}$ – множество алгоритмов, являющихся частью математического обеспечения, реализующих функционирование π-го протокола на l-ом уровне функционирования системы связи;

$D(\cdot)$ – область определения $(\cdot)$;

$E=\{e_i\}$ – множество средств связи, установленных на узлах сети связи;

f – отображение, определяющее выходные показатели качества обслуживания Q системы связи;

f_l – отображение, определяющее выходные показатели качества обслуживания Q_l, которые обеспечивают множество протоколов Π_l на l-ом уровне функционирования;

$f_{l,\pi}$ – отображение, определяющее выходные показатели качества обслуживания $Q_{l,\pi}$, которые обеспечивает протокол π_l на своем l-ом уровне функционирования;

$K=\{k_{ij}\}$ – множество каналов связи, соединяющих узлы связи (средства связи). Предполагается, что канал k_{ij} соединяет узлы z_i и z_j в случае, если средства связи e_i и e_j, размещенные на этих узлах, используют совместный протокол связи $\pi_{l.k}$;

k_u – индикатор устойчивости системы связи;

$l=1\ldots7$ – номер уровня функционирования системы связи в соответствии с моделью OSI;

$M=\bigcup_{l} M_l$ – канал разведки параметров $\{Y_l\}$ и показателей QoS Q на всех уровнях системы связи со стороны системы дестабилизирующих воздействий;

$M_l=\bigcup_{\Pi_l} M_{l,\pi}$ – канал разведки параметров Y_l и показателей QoS Q_l на l-ом уровне системы связи со стороны системы дестабилизирующих воздействий;

$M_{l,\pi}=\{\mu \mid \mu\in \mathbb{E}(\pi_l),\ \mu\in Q_{l,\pi}\times Y_{l,\pi}\}$ – канал разведки выходных параметров $Y_{l,\pi}$ и показателей QoS $Q_{l,\pi}$, которые обеспечиваются протоколом π_l на своем l-ом уровне системы связи со стороны системы дестабилизирующих воздействий;

$N=\bigcup_{l} N_l$ – канал наблюдения параметров Y и показателей QoS Q на всех уровнях системы связи со стороны системы управления связью;

$N_l=\bigcup_{\Pi_l} N_{l,\pi}$ – канал наблюдения параметров Y_l и показателей QoS Q_l на l-ом уровне системы связи со стороны системы управления связью;

$N_{l,\pi}=\{\eta \mid \eta\in \mathbb{E}(\pi_l),\ \eta\in Q_{l,\pi}\times Y_{l,\pi}\}$ – канал наблюдения выходных параметров $Y_{l,\pi}$ и показателей QoS $Q_{l,\pi}$, которые обеспечиваются протоколом π_l на своем l-ом уровне системы связи со стороны системы управления связью;

q – отдельный показатель качества QoS функционирования системы связи;

$Q = \bigcup_{l} Q_l$ – множество показателей QoS системы связи на всех ее уровнях;

$Q_l = \bigcup_{\Pi_l} Q_{l,\pi}$ – множество показателей QoS системы связи на l-ом уровне;

$Q_{l,M} = \bigcup_{\Pi_l} Q_{l,\pi,M}$ – множество показателей QoS системы связи на l-ом уровне, наблюдаемых системой дестабилизирующих воздействий по каналу разведки M_l;

$Q_{l,N} = \bigcup_{\Pi_l} Q_{l,\pi,N}$ – множество показателей QoS системы связи на l-ом уровне, наблюдаемых системой управления связи по каналу наблюдения N_l;

$Q_{l,\pi} = \{q \mid q \in \mathbb{E}(\pi_l)\}$ – множество показателей QoS системы связи на l-ом уровне, которые обеспечивает π_l-ый протокол связи;

$Q_{l,\pi,M} = \{q \mid q \in Q_{l,\pi},\ q \in M_{l,\pi}\}$ – множество показателей QoS системы связи на l-ом уровне, которые обеспечивает π_l-ый протокол связи, наблюдаемых системой дестабилизирующих воздействий по каналу разведки $M_{l,\pi}$;

$Q_{l,\pi,N} = \{q \mid q \in Q_{l,\pi},\ q \in N_{l,\pi}\}$ – множество показателей QoS системы связи на l-ом уровне, которые обеспечивает π_l-ый протокол связи, наблюдаемых системой управления связи по каналу наблюдения $N_{l,\pi}$;

$Q_{l,\pi,v} = \{q_{l,\pi} \mid q_{l,\pi} < q_{l,\pi}^{\text{треб}}\}$ – множество показателей QoS системы связи на l-ом уровне, которые обеспечивает π_l-ый протокол связи и которые снижаются в результате преднамеренных дестабилизирующих воздействий $V_{l,\pi}$;

$Q_M = \bigcup_{l} Q_{l,M}$ – множество показателей QoS системы связи на всех ее уровнях, наблюдаемых системой дестабилизирующих воздействий по каналу разведки M;

$Q_N = \bigcup_{l} Q_{l,N}$ – множество показателей QoS системы связи на всех ее уровнях, наблюдаемых системой управления связи по каналу наблюдения N;

r – отдельный тип ресурса системы связи;

$R = \bigcup_{l} R_l$ – ресурс системы связи на всех уровнях ее функционирования;

$R_l = \bigcup_{\Pi_l} R_{l,\pi}$ – ресурс системы связи на l-ом уровне ее функционирования, используемый для функционирования протоколов Π_l и организации связи;

$R_{l,V} = \{r \mid r \in D(V_l),\ r \in R_l\}$ – ресурс на l-ом уровне функционирования системы связи, используемый системой дестабилизирующих воздействий для V_l-го воздействия на протоколы связи Π_l;

$R_{l,\pi} = \{r \mid r \in D(\pi_l)\}$ – ресурс системы связи на l-ом уровне ее функционирования, используемый для функционирования π-го протокола;

$S = \{t_0, t, \{S_l\}, X, U, A, \Theta, Z, E, K, \Lambda\}$ – множество состояний системы связи;

$S_{\text{conf}} = \{t, R, \Omega, A, \Theta, Z, K, \Lambda\}$ – конфигурация системы связи, определяющая ее текущую структуру и множество функциональных связей;

$S_{\text{conf}}^{\text{набл}} = \{t, R, \Omega, A, \Theta, Z, K, \Lambda\} \in M$ – конфигурация системы связи, наблюдаемая по каналу разведки со стороны системы дестабилизирующих воздействий;

$S_l = \{S_{l,\pi}\} \cup \Theta_l$ – множество состояний l-ого уровня функционирования системы связи, определяемое состояниями протоколов и связями между ними;

$S_{l,\pi} = \{s_\pi\}$ – множество состояний π_l-го протокола связи на l-ом уровне функционирования системы связи;

s_π – состояние π-го протокола связи;

t – время функционирования системы связи;

T – множество моментов времени функционирования системы связи (непрерывных или дискретных);

t_0 – начальный момент функционирования системы связи;

T_U – множество моментов времени выдачи управляющих воздействий на элементы системы связи со стороны системы управления связью;

T_V – время, в течении которого осуществляются дестабилизирующие воздействия на элементы системы связи со стороны противника;

T_η – множество моментов времени наблюдения элементов системы связи со стороны системы управления связью;

$t_{набл}$ – интервал времени наблюдения;

$t_{тек}$ – текущий момент функционирования системы связи;

u – управляющее воздействие на элемент системы связи со стороны системы управления связью;

$U = \bigcup_l U_l$ – функционал, задающий множество управляющих воздействий (управление) на протоколы П всех уровней со стороны системы управления связью с целью обеспечения требуемых показателей QoS Q;

$U_l = \bigcup_{П_l} U_{l,\pi}$ – функционал, задающий множество управляющих воздействий (управление) на протоколы $П_l$ l-ого уровня со стороны системы управления связью на этом уровне с целью обеспечения требуемых показателей QoS Q_l;

$u_{l,\pi}$ – управляющее воздействие на протокол π_l системы связи со стороны системы управления связью на l-ом уровне функционирования;

$U_{l,\pi} = u_{l,\pi} \times T$ – функционал, задающий множество управляющих воздействий (управление) на протокол π_l, со стороны системы управления связью на l-ом уровне с целью обеспечения протоколом требуемых показателей QoS $Q_{l,\pi}$;

v – отдельное воздействие со стороны системы дестабилизирующих воздействий;

$V = \bigcup_l V_l$ – множество воздействий, осуществляемых на все уровни системы связи со стороны системы дестабилизирующих воздействий;

$V_l = \bigcup_{П_l} V_{l,\pi}$ – множество воздействий, осуществляемых на l-ый уровень системы связи со стороны системы дестабилизирующих воздействий;

$V_{l,\pi} = \{v \mid v \in D(\pi_l),\ v \in R_{l,\pi} \times \Omega_{l,\pi} \times A_{l,\pi} \times \Theta_{l,\pi}\}$ – множество воздействий со стороны системы дестабилизирующих воздействий на протокол π_l, функционирующий на l-ом уровне системы связи;

$X = \bigcup_l X_l = \chi \times R \times V$ – множество параметров среды, определяющих параметрическое пространство для системы связи на всех ее уровнях, с учетом ее ресурсов R, параметров естественной среды χ и всего множества дестабилизирующих воздействий V;

$X_l = \bigcup_{П_l} X_{l,\pi} = \chi_l \times R_l \times V_l$ – множество параметров среды, определяющих параметрическое пространство для протоколов системы связи $П_l$ на l-ом уровне функционирования, с учетом ресурсов l-го уровня R_l, параметров естественной среды χ_l и множества V_l дестабилизирующих воздействий на этом уровне;

$X_{l,\pi} = \chi_{l,\pi} \times R_{l,\pi} \times V_{l,\pi}$ – множество параметров среды, определяющих параметрическое пространство для протокола π_l системы связи на l-ом уровне функционирования, с учетом выделяемых протоколу на l-ом уровне ресурсов $R_{l,\pi}$, параметров естественной среды $\chi_{l,\pi}$ и множества $V_{l,\pi}$ преднамеренных дестабилизирующих воздействий на этот протокол;

y – выходной параметр протокола системы связи;

$Y = \bigcup_{l} Y_l$ – множество выходных параметров системы связи;

Y_7 – конечные выходные параметры системы связи;

$Y_l = \bigcup_{\Pi_l} Y_{l,\pi}$ – множество выходных параметров l-го уровня системы связи;

$Y_{l,M} = \bigcup_{\Pi_l} Y_{l,\pi,M}$ – множество выходных параметров l-го уровня системы связи, наблюдаемых системой дестабилизирующих воздействий по каналу разведки M_l;

$Y_{l,N} = \bigcup_{\Pi_l} Y_{l,\pi,N}$ – множество выходных параметров l-го уровня системы связи, наблюдаемых системой управления связи по каналу наблюдения N_l;

$Y_{l,\pi} = \{y \mid y \in \mathbb{E}(\pi_l)\}$ – множество выходных параметров π_l-го протокола на l-ом уровне системы связи;

$Y_{l,\pi,M} = \{y \mid y \in Y_{l,\pi},\ y \in M_{l,\pi}\}$ – множество выходных параметров π_l-го протокола на l-ом уровне, наблюдаемых системой дестабилизирующих воздействий по каналу разведки $M_{l,\pi}$;

$Y_{l,\pi,N} = \{y \mid y \in Y_{l,\pi},\ y \in N_{l,\pi}\}$ – множество выходных параметров π_l-го протокола на l-ом уровне, наблюдаемых системой управления связью по каналу наблюдения $N_{l,\pi}$;

$Y_M = \bigcup_{l} Y_{l,M}$ – множество выходных параметров всех уровней системы связи, наблюдаемых системой дестабилизирующих воздействий по каналу разведки M;

$Y_N = \bigcup_{l} Y_{l,N}$ – множество выходных параметров всех уровней системы связи, наблюдаемых системой управления связи по каналу наблюдения N;

$Z = \{z_i\}$ – множество узлов системы связи;

γ – отображение, определяющее выходные параметры Y системы связи;

γ_l – отображение, определяющее выходные параметры Y_l множества протоколов Π_l на l-ом уровне;

$\gamma_{l,\pi}$ – отображение, определяющее выходные параметры Y_π протокола π_l на l-ом уровне;

η – параметр, наблюдаемый со стороны системы управления связью;

$\Theta = \{(\pi_{l1,i}, \pi_{l2,j})\},\ i, j = 1 \ldots |\Pi_l|,\ l_1, l_2, = 1 \ldots 7$ – множество функциональных связей между протоколами $\pi \in \Pi$ в системе связи на различных ее уровнях;

$\Theta_l = \{(\pi_{l,i}, \pi_{l,j})\},\ i, j = 1 \ldots |\Pi_l|$ – множество функциональных связей между протоколами $\pi_l \in \Pi_l$ на l-ом уровне системы связи;

$\Theta_{l,\pi} = \{(a_{l,,\pi,i}, a_{l,,\pi,j})\},\ i, j = 1 \ldots |A_{l,\pi}|$ – множество функциональных связей между алгоритмами $A_{l,\pi}$ в протоколе π_l на l-ом уровне системы связи;

Λ – информационная структура системы связи, определяющая маршруты циркуляции информационных потоков;

μ – параметр, наблюдаемый по каналу разведки со стороны системы управления воздействиями противника;

π – протокол связи;

$\Pi = \bigcup_l \Pi_l$ – множество протоколов, используемых в системе связи на всех уровнях ее функционирования;

π_l – протокол на l-ом уровне функционирования системы связи;

$\Pi_l = \bigcup_i \{\pi_{l,i}\}$ – множество протоколов, используемых в системе связи, на l-ом уровне ее функционирования;

$\pi_{l,i}$ – i-ый протокол на l-ом уровне функционирования системы связи;

$\varphi = \bigcup_l \varphi_l$ – множество отображений, определяющих межиерархические связи между уровнями системы связи;

φ_l – отображение, определяющее параметрическое множество среды функционирования X_{l+1} протоколов более высокого уровня Π_{l+1};

$\varphi_{l,\pi}$ – отображение, определяющее параметрическое множество среды функционирования протоколов более высокого уровня X_{l+1}, зависимое от протокола π_l на l-ом уровне;

$\chi = \bigcup_l \chi_l$ – множество параметров естественной среды функционирования системы связи;

$\chi_l = \bigcup_{\Pi_l} \chi_{l,\pi}$ – множество параметров естественной среды функционирования системы связи, определяющие параметрическое пространство для протоколов Π_l на l-ом уровне;

$\chi_{l,\pi}$ – множество параметров естественной среды функционирования системы связи (без преднамеренных дестабилизирующих воздействий), определяющие параметрическое пространство для протокола π_l на l-ом уровне;

ψ – отображение, задающее смену состояний $s \in S$ системы связи;

ψ_l – отображение, задающее смену состояний $s_l \in S_l$ l-го уровня системы связи;

$\psi_{l,\pi}$ – отображение, задающее смену состояний $s_{l,\pi} \in S_{l,\pi}$ протокола π_l на l-ом уровне функционирования;

ω – параметр алгоритма a;

$\Omega = \bigcup_l \Omega_l$ – множество параметров алгоритмов на всех уровнях системы связи;

$\Omega_l = \bigcup_{\Pi_l} \Omega_{l,\pi}$ – множество параметров алгоритмов протоколов Π_l на l-ом уровне системы связи;

$\Omega_{l,\pi} = \bigcup_\pi \Omega_{l,\pi,a}$ – множество параметров алгоритмов π-го протокола связи на l-ом уровне системы связи;

$\Omega_{l,\pi,a} = \{\omega \mid \omega \in D(a),\ a \in D(\pi_l)\}$ – множество параметров a-го алгоритма π-го протокола на l-ом уровне системы связи;

$\Pi_{l,v} = \bigcup_i \{\pi_{l,i} \mid V_l \in X_{l,\pi}\}$ – множество протоколов, используемых на l-ом уровне системы связи и подвергающихся преднамеренному дестабилизирующему воздействию V_l.

Обозначения, используемые в 6-ой главе

π – значение элемента множества A;

A – множество;

a – элемент множества A;

B – множество;

b – элемент множества B;

b_u – показатель посредничества вершины u в графе G;

b_u – показатель посредничества вершины u в графе G;

$C_{\text{а}\,\nu}$ – абсолютная пропускная способность (пакетов в секунду) ν-го элемента j-го пути информационного направления связи (ИНС);

$D(G)$ – диаметр графа G – длина максимального из кратчайших путей d_{ij}, котороые можно сформировать между всеми вершинами графа G;

d_{ij} – количество участков сети (хопов) между узлом, обнаружившим отказ пути (узел i), и узлом, ответственным за переключение путей в ИНС (узел j);

E – эффективность сети;

E_z – эффективность сети после удаления из ее состава z-го элемента (узла или линии связи);

$F(\delta_i)$ – функция распределения степеней вершин графа G, определяемая вероятностью того, что вершина u_i в графе G имеет степень δ_i;

$G(u, v)$ – граф, формализующий сеть СС СН в виде множеств вершин $\{u\}$ и соединяющих их ребер $\{v\}$;

$G_{\text{ИНС}}$ – подграф, образованный из графа G элементами (вершинами и ребрами), входящими в конкретное ИНС;

H_z – показатель уязвимости сети относительно удаления z-го элемента СС СН (узла или линии связи);

i – счетчик;

j – счетчик;

K – требования к количеству путей в ИНС, в которых должно обеспечиваться требуемое качество обслуживания трафика;

k_i – количество работоспособных путей в i-ом ИНС;

k_{QoS} – количество работоспособных путей на заданном ИНС, обеспечивающих заданное качество обслуживания QoS;

$K_{\text{Г}}$ – коэффициент готовности СС СН;

$K_{\text{Г}\,i}$ – коэффициент готовности i-го ИНС;

m – количество ребер в графе;

$M(\bullet)$ – математическое ожидание случайной величины;

m_j – количество линий связи в j-ом пути в составе ИНС;

$m_{\text{рз}\,\nu}$ – количество независимых параметров ν-го элемента СС СН, требуемых для для организации дестабилизирующего воздействия;

n – количество вершин в графе;

N – количество ИНС в СС СН;

n_j – количество узлов связи в j-ом пути в составе ИНС;

$P_{\text{ИТВ}\,i}$ – вероятность отказа i-го ИНС вследствие ИТВ;

$P_{\text{ИТВ}\,\nu}$ – вероятность отказа ν-го элемента ИНС (линии или узла связи) вследствие ИТВ;

$P_{ИТВ\ v}$* – вероятность успешной реализации ИТВ против v-го элемента СС СН при условии успешной разведки и вскрытия информационных параметров, т.е. при $P_{рз.инф\ v}$ =1;

$P_{отк\ i}$ – вероятность отказа i-го ИНС вследствие естественных внутренних дестабилизирующих процессов, описываемых теорией надежности;

$P_{отк\ v}$ – вероятность отказа v-го элемента ИНС (линии или узла связи) вследствие естественных внутренних дестабилизирующих процессов, описываемых теорией надежности;

$P_{отк\ пак\ v}$ – отказ в обслуживании пакета в v-ом элементе j-го пути ИНС;

$P_{раб\ j}$ – вероятность работоспособного состояния j-го пути в составе ИНС;

$P_{раб.эл.\ v}$ – вероятность работоспособного состояния v-го элемента ИНС;

$P_{рз\ v}$ – вероятность разведки противником параметров v-го элемента СС СН;

$P_{рз\ v\ i}$ – вероятность разведки противником i-го параметра v-го элемента СС СН;

$P_{рз.вр\ v}$ – вероятность вскрытия временных параметров v-го элемента СС СН при ведении разведки;

$P_{рз.инф\ v}$ – вероятность вскрытия информационных параметров v-го элемента СС СН при ведении разведки;

$P_{рз.пр\ v}$ – вероятность вскрытия местоположения v-го элемента СС СН в пространстве при ведении разведки;

$P_{рз.пр.РРТР\ v}$ – вероятность вскрытия местоположения v-го элемента СС СН в пространстве средствами РРТР;

$P_{рз.пр.ОЭР\ v}$ – вероятность вскрытия местоположения v-го элемента СС СН в пространстве средствами ОЭР;

$P_{рз.ст\ v}$ – вероятность вскрытия структурных параметров v-го элемента СС СН при ведении разведки;

$P_{рз.э\ v}$ – вероятность успешного приема сигналов и вскрытия энергетических параметров v-го элемента СС СН при ведении разведки;

$P_{РЭП\ i}$ – вероятность подавления количества линий связи i-го ИНС большего, либо равного величине реберной связности x_v подграфа $G_{ИНС\ i}$;

$P_{РЭП\ v}$ – вероятность отказа v-го элемента ИНС (линии или узла связи) вследствие РЭП;

$P_{РЭП\ v}$* – вероятность подавления v-го элемента СС СН средствами РЭП при условии его успешной разведки и вскрытия энергетических, временных и структурных параметров т.е. при $P_{рз.э\ v}$ =1, $P_{рз.вр\ v}$ =1 и $P_{рз.ст\ v}$ =1;

$P_{св}$ – вероятность связности ИНС;

$P_{св\ i}$ – вероятность связности i-го ИНС в условиях воздействия на его элементы различных дестабилизирующих факторов;

$P_{скр\ v\ i}$ – вероятность скрытности i-го параметра v-го элемента СС СН;

$P_{скр.вр\ v}$ – вероятность обеспечения временной скрытности v-го элемента СС СН;

$P_{скр.инф\ v}$ – вероятность обеспечения информационной скрытности v-го элемента СС СН;

$P_{скр.пр.РРТР\ v}$ – пространственная скрытность местоположения v-го элемента СС СН по отношению к средствами РРТР;

$P_{скр.пр.ОЭР\ v}$ – пространственная скрытность местоположения v-го элемента СС СН по отношению к средствами ОЭР;

$P_{скр.ст\ v}$ – вероятность обеспечения структурной скрытности v-го элемента СС СН;

$P_{скр.э\ v}$ – вероятность обеспечения энергетической скрытности v-го элемента СС СН;

$P_{У\ i}$ – устойчивость i-го ИНС в СС СН;

$P_{У\ ср}$ – среднесетевая вероятность устойчивости ИНС в СС СН;

$P_{ФП\ i}$ – вероятность физического поражения узлов связи i-го ИНС большего, либо равного величине вершинной связности x_u подграфа $G_{ИНС\ i}$;

$P_{ФП\ v}$ – вероятность отказа v-го элемента ИНС (линии или узла связи) вследствие его физического поражения;

$P_{ФП\ v}$* – вероятность физического поражения v-го элемента СС СН при условии его успешной разведки и вскрытия местоположения т.е. при $P_{рз.пр\ v}$ =1;

$P_{ФПЭМИ\ v}$* – вероятность функционального поражения v-го элемента СС СН средствами ФП ЭМИ при условии вскрытия его местоположения при ведении разведки т.е. при $P_{рз.пр\ v}$ =1;

Q_k – качество обслуживания, обеспечиваемое путями (путем) на заданном ИНС;

$Q^{треб}$ – требуемый уровень качества обслуживания;

$T_{В\ i}$ – время восстановления i-го ИНС;

$T_{диагн\ i}$ – время диагностики отказа i-го ИНС;

$T_{зад\ v}$ – время задержки пакета в v-ом элементе j-го пути ИНС;

$T_{О\ i}$ – время между отказами в i-ом ИНС;

$T_{ож\ i}$ – время ожидания восстановления связи (удержания конфигурации) i-ого ИНС;

$t_{отк\ i}$ – время отказа i-го ИНС, заключающееся в утрате свойства связности;

$T_{перекл\ i}$ – время переключения информационных потоков с активных путей на резервные пути в составе i-го ИНС;

T_p – среднее время передачи пакета между отдельными узлами в СС СН;

$T_{рек\ i}$ – длительность реконфигурации путей или активации резервных путей в i-ом ИНС;

$T_{увед\ i}$ – время уведомления узла, ответственного за изменение конфигурации путей в i-ом ИНС;

u – вершина графа G;

v – ребро графа G;

x_u – показатель вершинной связности графа G;

x_v – показатель реберной связности графа G;

Y_u – коэффициент кластеризации вершины u;

z_j – количество элементов j-го пути в составе ИНС;

α_i – коэффициент важности i-го ИНС в сети;

δ_{min} – минимальная степень вершины;

δ_u – степень вершины u;

$\delta_{u\ \Sigma}$ – суммарная степень вершин, инцидентных вершине u;

λ_i – интенсивность трафика, передаваемого в i-ом ИНС;

$\varphi(i, j)$ – общее количество путей между вершинами i и j;

$\varphi(i, u, j)$ – количество путей между вершинами i и j, проходящих через вершину u;

η – значение элемента множества B в окрестности точки (a, b);

Θ_A – ограниченное подмножество множества A;

Θ_a – окрестность точки (a, b) на множестве A;

Θ_B – ограниченное подмножество множества B;

Θ_b – окрестность точки (a, b) на множестве B;

λ_i – интенсивность трафика, передаваемого в i-ом ИНС;

μ – значение элемента множества A в окрестности точки (a, b);

$\varphi(i, j)$ – общее количество путей между вершинами i и j;

$\varphi(i, u, j)$ - количество путей между вершинами i и j, проходящих через вершину u;

Ω – некоторое отображение.

Обозначения, используемые в 7-ой главе

$\left|I\right|$ – число элементов множества I;

$\left|J\right|$ – число элементов множества J;

$\left|S\right|$ – число элементов множества S;

A – матрица приоритетности ИНС;

$a_{\lambda,\lambda}$ – коэффициент важности λ-го ИНС;

$H(S_j, V_i)$ – фазовая траектория, которая соответствует динамике совместного изменения состояний S_j и V_i в процессе развития многоэтапного конфликта метасистемы «система связи – система дестабилизирующих воздействий»;

$H^{\text{сдв}}(S_j, V_i)$ – состояние метасистемы $H(S_j, V_i)$, наблюдаемое системой дестабилизирующих воздействий;

$H^{\text{сс}}(S_j, V_i)$ – состояние метасистемы $H(S_j, V_i)$, наблюдаемое системой связи;

I – множество стратегий нападения на систему связи со стороны системы дестабилизирующих воздействий;

i – стратегия нападения на систему связи со стороны системы дестабилизирующего воздействия;

J – множество стратегий защиты системы связи;

j – стратегия защиты системы связи;

K – количество вариантов дестабилизирующего воздействия;

k – номер дестабилизирующего воздействия;

L – количество иерархий в системе управления;

l – номер иерархии системы управления;

m – счетчик;

M – общее количество элементов (узлов и линий связи) в системе связи;

N – количество этапов в многоэтапной информационном конфликте;

n – счетчик;

N_Λ – количество ИНС организуемых в системе связи;

$P_i(V_i)$ – вероятность применения системой дестабилизирующих воздействий i-го варианта нападения, который соответствует использованию V_i структуре использования средств разведки и нападения;

$P_j(S_j)$ – вероятность применения системой связи j-го варианта защиты, который соответствует использованию S_j структуре организации связи;

$P_{У\,i}$ – вероятность устойчивости i-го ИНС;

$P_{У\,ср}$ – итоговый показатель устойчивости системы связи – среднесетевая вероятность устойчивости ИНС;

$P_{У\,ср}(S_j, V_i)$ – показатель устойчивости системы связи в условиях когда против системы связи реализован вариант нападения V_i, а система связи использует структуру организации связи S_j;

Q – матрица показателей качества функционирования ИНС в системе связи;

q – показатель качества системы связи;

$q_{\lambda,j,i}$ – показатель качества λ-го ИНС, если на нем используется j-ый вариант распределения линий и узлов связи, подвергающийся i-му варианту дестабилизирующего воздействия;

$S=S_{ус}\cup S_{лс}$ – структура защищаемой системы связи, состоящей из структуры размещения узлов связи $S_{ус}$ и линий связи между узлами $S_{лс}$;

S_j – структура системы связи, реализуемое в рамках j-ой стратегии защиты;

$S_j(t_n)$ – структура системы связи, соответствующая j-ой стратегии защиты, на n-ом этапе конфликта;

$S_j^{опт}(t_n)$ – структура системы связи, соответствующая j-ой стратегии защиты, которая является оптимальной на n-ом этапе конфликта;

$s_{n,m}$ – элемент множества $S=S_{ус}\cup S_{лс}$, задающий принадлежность конкретного узла или линии связи к ИНС от n-го узла связи к m-му узлу;

$S_{лс}$ – подмножество S, задающее структуру размещения линий связи;

$S_{ус}$ – подмножество S, задающее структуру размещения узлов связи;

$V=\{V_i\}=\{v_{s,k}\}_i$ – множество вариантов воздействия, которые может реализовать субъект нападения;

$V_i(t_n)$ – вариант воздействия, который соответствует i-ой стратегии нападения, на n-ом этапе конфликта;

$V_i=\{v_{s,k}\}$ – воздействие на систему связи, реализуемое в рамках i-ой стратегии нападения;

$v_{s,k}$ – элемент множества V, задающий воздействие k-го типа на s-ый элемент (узел или линию связи) системы связи;

γ – оператор, которой описывает процесс эволюции метасистемы $H(S_j, V_i)$ в фазовом пространстве $V\times S$;

η – отображение, задающие наблюдение (мониторинг) параметров метасистемы со стороны системы связи;

λ – номер ИНС;

$\Lambda=\{\lambda_{n,m}\}$ – структура ИНС организуемых в системе связи;

$\lambda_{n,m}$ – элемент множества Λ, задающий наличие ИНС от n-го узла связи к m-му узлу;

μ – отображение, задающие наблюдение (разведку) параметров метасистемы со стороны системы дестабилизирующих воздействий.

Глоссарий терминов и определений

Абонент – лицо или техническое средство, использующее систему связи для обмена информацией.

Адаптивность (*адаптируемость*) – в теории систем: способность системы изменять свое поведение с целью сохранения, улучшения или приобретения новых характеристик в условиях воздействий изменяющейся среды [387].

Адекватность управления – уровень соответствия управляющих воздействий, формируемых органами управления, реальному состоянию управляемого объекта, среды и цели управления.

Активная преднамеренная радиоэлектронная помеха – см. помеха радиоэлектронная преднамеренная активная.

Активное информационно-техническое воздействие – см. воздействие информационно-техническое активное.

Алгоритмическая компьютерная разведка – см. разведка компьютерная алгоритмическая.

Антагонистический конфликт – см. конфликт антагонистический.

Аппаратная закладка – см. закладка аппаратная.

Аппаратная компьютерная разведка – см. разведка компьютерная аппаратная.

Аппаратное средство – см. средство аппаратное.

Аппаратура – комплекс технических средств, имеющих общее эксплуатационное назначение [390].

Асимметричные действия – реализация собственной стратегии действий, отличных от реализуемых или навязываемых противником, которая позволяет добиться преимуществ, использовать уязвимые места противника, завоевать инициативу и достичь большей свободы собственных действий. Асимметричные действия также могут быть связанны с уходом одной из сторон от прямого противоборства к концентрации усилий в областях, где удалось выявить уязвимость и слабость противника [10].

Атака сетевая удаленная – это атакующее информационно-техническое воздействие, осуществляемое по каналам связи удаленным относительно атакуемой системы субъектом и характерное для структурно- и пространственно-распределенных информационных систем [9].

Атака средств компьютерной разведки – как пассивные действия, направленные на добывание информации и, как правило, связанные с нарушением ее конфиденциальности, так и активные действия, направленные на создание условий, благоприятствующих добыванию информации [9].

Атакующее информационно-техническое воздействие – см. воздействие информационно-техническое атакующее.

Безопасность – состояние защищённости кого-либо или чего-либо от внутренних и внешних угроз; способность объекта, явления или процесса сохраняться при дестабилизирующих воздействиях.

Безопасность информационная – это состояние, при котором обеспечивается конфиденциальность, целостность и доступность информации [64].

Безопасность связи – свойство связи, которое характеризует ее способность обеспечить сохранение в тайне содержания передаваемых сообщений и самого факта их передачи.

Блокирующее информационно-техническое воздействие – см. воздействие информационно-техническое блокирующее.

Боевая готовность системы связи – см. готовность боевая системы связи.

Боевые действия – см. действия боевые.

Вид связи – классификационная группа связи, выделяемая по виду передаваемого сообщения. Основная часть современных средств связи относится к видам связи «передача данных», «телефонная связь», «видеотелефонная связь».

Вирус – программа, несанкционировано внедренная в информационную систему и способная осуществлять создание собственных дубликатов (не всегда совпадающих с оригиналом), несанкционированное самораспространение, несанкционированный доступ к информационным ресурсам, изменение логики функционирования зараженной программы, снижение качества или эффективности информационной системы.

Вирус компьютерный – см. вирус.

Вирусная компьютерная разведка – см. разведка компьютерная вирусная.

Внешнее воздействие – см. воздействие внешнее.

Внешний дестабилизирующий фактор – см. фактор дестабилизирующий внешний.

Внутреннее воздействие – см. воздействие внутреннее.

Внутренний дестабилизирующий фактор – см. фактор дестабилизирующий внутренний.

Внутриуровневый конфликт – см. конфликт внутриуровневый.

Военные действия – см. действия военные.

Воздействие – активное влияние субъекта (источника воздействия) на объект (реципиент), не обязательно явное или с обратной связью.

Воздействие внешнее – воздействие, источник которого расположен вне системы.

Воздействие внутреннее – воздействие, источник которого расположен внутри системы или ее элементов.

Воздействие дестабилизирующее – негативное влияние электрических, акустических, магнитных, электромагнитных или других полей, физических и информационных факторов, технологических процессов, которое нарушают работоспособность технических средств или программ, вызывает ухудшение их характеристик и параметров или снижет их эффективность.

Воздействие дестабилизирующее естественное – дестабилизирующее воздействие, создаваемое источником естественного (природного) происхождения.

Воздействие дестабилизирующее искусственное – дестабилизирующее воздействие, создаваемое источником искусственного происхождения.

Воздействие дестабилизирующее непреднамеренное – дестабилизирующее воздействие, создаваемое источником искусственного происхождения без конкретной цели нанесения вреда или ущерба.

Воздействие дестабилизирующее преднамеренное – дестабилизирующее воздействие, создаваемое источником искусственного происхождения с целью нарушить работоспособность технических средств или программ, вызывать ухудшение их характеристик и параметров или снизить их эффективность.

Воздействие информационно-техническое – воздействие на информационный ресурс, информационную систему, информационную инфраструктуру, на технические средства или на программы, решающие задачи формирования, передачи, обработки, хранения и воспроизведения информации, с целью вызвать заданные структурные или функциональные изменения.

Воздействие информационно-техническое активное – информационно-техническое воздействие, которое оказывает непосредственное влияние на функционирование информационной системы, проявляющиеся в активном изменении ее параметров, среды функционирования, нарушении принятой в ней политики безопасности.

Воздействие информационно-техническое атакующее – информационно-техническое воздействие, которое ориентировано на непосредственное воздействие на информацию, системы ее сбора, передачи, хранения, обработки и представления, а также на используемые в этих системах информационные технологии, как правило, с целью снижения уровня информационной безопасности или эффективности функционирования.

Воздействие информационно-техническое блокирующее – информационно-техническое воздействие, которое ориентировано на блокировку атакующих информационно-технических воздействий со стороны нарушителя/противника.

Воздействие информационно-техническое высокоточное – информационно-техническое воздействие, которое ориентировано на определенный информационный ресурс, процесс, технический объект или систему.

Воздействие информационно-техническое выявляющее – информационно-техническое воздействие, которое ориентировано на выявление, как самого факта, так и последовательности действий атакующих и обеспечивающих информационно-технических воздействий со стороны нарушителя/противника.

Воздействие информационно-техническое комплексное – информационно-техническое воздействие, которое ориентировано на несколько информационных ресурсов, процессов, технических объектов или систем.

Воздействие информационно-техническое контратакующее – информационно-техническое воздействие, которое ориентировано на блокировку атакующих информационно-технических воздействий со стороны нарушителя/противника.

Воздействие информационно-техническое обеспечивающее – информационно-техническое воздействие, которое ориентировано на сбор данных, обеспечивающих эффективное применение оборонительных или атакующих информационно-технических воздействий, а также на преодоление средств защиты атакуемой системы.

Воздействие информационно-техническое оборонительное – информационно-техническое воздействие, которое ориентировано на противодействие обеспечивающим и атакующим информационно-техническим воздействиям нарушителя/противника.

Воздействие информационно-техническое отвлекающее – информационно-техническое воздействие, которое ориентировано на дезинформацию нарушителя/противника, отвлечение его атакующих или обеспечивающих информационно-технических воздействий на незначащие или ложные объекты.

Воздействие информационно-техническое пассивное – информационно-техническое воздействие, которое не оказывает непосредственного влияния на функционирование информационной системы, но может нарушать ее политику безопасности.

Воздействие радиоэлектронное – электромагнитное излучение в виде отражающего, поглощающего, рассеивающего или модулирующего образования, которое, воздействуя на элементы радиоэлектронного средства или на среду распространения электромагнитных волн, снижает эффективность его функционирования.

Воздействие электромагнитное силовое преднамеренное – воздействие с применением излучателей электромагнитного поля, генераторов напряжения и тока путем генерирования в информационных системах электромагнитной энергии, уровень которой вызывает нарушение нормального функционирования технических и программных средств информационных систем [105].

Временная скрытность – см. скрытность временная.

Временные параметры радиоэлектронного средства – см. параметры радиоэлектронного средства временные.

Вторичная сеть связи – см. сеть абонентского доступа.

Выделенная сеть связи – см. сеть связи выделенная.

Высокоточное информационно-техническое воздействие – см. воздействие информационно-техническое высокоточное.

Высокоточное оружие (ВТО) – см. оружие высокоточное.

Выявляющее информационно-техническое воздействие – см. воздействие информационно-техническое выявляющее.

Готовность боевая системы связи – способность системы связи в любых условиях обстановки в установленные сроки приступить к выполнению задачи по переносу информации с требуемым качеством.

Граф – математическая модель сети, представляющий совокупность вершин, которые соответствуют узлам связи, и соединяющих их ребер, которые соответствуют линиям связи.

Данные – поддающееся многократной интерпретации представление информации в формализованном виде, пригодном для сбора, хранения, передачи обработки или представления. Фактически, данные – это формализованное представление информации в виде, удобном для ее обработки информационными системами.

Действия боевые – составная часть военных действий противоборствующих сторон, представляющих собой организованное применение сил и средств

объединений, соединений, частей, подразделений для выполнения поставленных боевых задач.

Действия военные – организованное применение вооружённых сил государства (включая различные действия военные военизированные формирования и силовые структуры) для ведения войны

Дестабилизирующее воздействие – см. воздействие дестабилизирующее.

Дестабилизирующий фактор – см. фактор дестабилизирующий.

Дестабилизирующий эффект – см. эффект дестабилизирующий.

Джиттер – нежелательные случайные отклонения параметров передаваемого сигнала, сообщения или пакета. В теории связи рассматривают фазовые, частотные или временные параметры. Данные отклонения возникают вследствие нестабильности параметров средств связи или изменений параметров линии связи.

Динамическая система – см. система динамическая.

Добывание информации – процесс сбора, обработки и анализа фактов, связанных со структурой, свойствами и взаимодействием объектов и явлений, извлекаемых из поступающих сигналов и данных [395].

Достоверность информации – истинность и точность информации в описании какого-либо факта, события или явления.

Достоверность связи – свойство связи, которое характеризует ее способность обеспечивать требуемую точность воспроизведения сообщений в пунктах доставки, а также сохранять эту точность при преобразовании информации.

Доступ несанкционированный – доступ к информации, нарушающий установленные правила разграничения доступа [389].

Доступность информации – состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа к информации, могут реализовывать их беспрепятственно [65].

Доступность системы связи – способность системы связи обеспечивать своим абонентам возможность организации связи с требуемым качеством при сохранении их приоритетности и способов установления связи между ними.

Дуэль – антагонистический конфликт двух сторон, в рамках решения одной строго определенной задачи [260, 261].

Единое информационное пространство – см. пространство информационное.

Естественная помеха – см. помеха естественная.

Естественное дестабилизирующее воздействие – см. воздействие дестабилизирующее естественное.

Живучесть – в теории систем: способность системы сохранять значение своих других показателей при разрушении части ее структуры [385].

Живучесть системы связи – способность системы связи обеспечивать связь с требуемым качеством в условиях воздействия на нее обычного и ядерного оружия.

Закладка аппаратная – электронное устройство, скрытно внедряемое к остальным элементам и способное вмешиваться в работу аппаратных или технических средств информационной системы.

Закладка программная – скрытно внедренная в защищенную информационную систему программа либо намеренно измененный фрагмент программы, которая позволяет осуществлять несанкционированный доступ к ресурсам системы на основе изменения свойств системы защиты [96].

Защита от средств радиоэлектронного поражения – снижение эффективности воздействия средств функционального поражения, средств радиоэлектронного подавления и самонаводящимся на излучение оружия на свои радиоэлектронные средства.

Защищенность – степень адекватности средств и способов защиты, реализованных в какой-либо системе, существующим для ее функционирования рискам, связанным с осуществлением угроз.

Защищенность системы связи – степень адекватности средств и способов защиты, реализованных в системе связи, существующим для ее функционирования рискам, связанным с осуществлением угроз.

Звено управления – уровень иерархии в системе управления войсками (силами) или государством.

Имитостойкость системы связи – способность системы связи противостоять вводу в нее ложной, в том числе и ранее переданной, информации и навязыванию ей ложных режимов работы.

Имитоустойчивость системы связи – способность системы связи обеспечивать требуемый уровень имитостойкости в условиях ввода в нее ложной, в том числе и ранее переданной информации, а также навязыванию ей ложных режимов работы [399-402].

Интегральный показатель – см. показатель интегральный.

Интерфейс – совокупность средств и правил взаимодействия отдельных систем.

Инфокоммуникационная система (ИКС) – см. система инфокоммуникационная.

Инфокоммуникационная система специального назначения (ИКС СН) – см. система инфокоммуникационная специального назначения.

Информационная безопасность – см. безопасность информационная.

Информационная инфраструктура – см. инфраструктура информационная.

Информационная операция – это комплекс взаимосвязанных по цели, месту и времени мероприятий, акций и воздействий, направленных на инициализацию и управление процессами манипулирования информацией, с целью достижения и удержания информационного превосходства путем воздействия на информационные процессы в информационных системах противника [9].

Информационная система – см. система информационная.

Информационная скрытность – см. скрытность информационная.

Информационная структура сети – см. структура сети информационная.

Информационная устойчивость системы связи – см. устойчивость системы связи информационная.

Информационно-вычислительная система – см. система информационно-вычислительная.

Информационное дестабилизирующее воздействие – см. воздействие информационно-техническое.

Информационное направление связи (ИНС) – см. направление связи.

Информационное пространство – см. пространство информационное.

Информационное противоборство – конфликт в информационном пространстве с целью завоевания и удержание информационного превосходства над противоположной стороной, который предполагает проведение взаимоувязанных по целям, месту и времени информационных операций, основанных как на дестабилизирующих воздействиях на информацию, информационные системы и информационную инфраструктуру противоположной стороны, так и на одновременной защите собственной информации, информационных систем и информационной инфраструктуры от подобных воздействий [9].

Информационной процесс – см. процесс информационный.

Информационно-телекоммуникационная сеть – см. сеть информационно-телекоммуникационная.

Информационно-техническое воздействие – см. воздействие информационно-техническое.

Информационные параметры радиоэлектронного средства – см. параметры радиоэлектронного средства информационные.

Информационный конфликт – см. конфликт информационный.

Информационный ресурс – см. ресурс информационный.

Информация – сведения, независимо от формы их представления, относительно фактов, событий, вещей, идей и понятий, которые в определенном контексте имеют конкретный смысл (семантическое значение) и интерпретацию.

Инфраструктура информационная – организационно-техническое объединение пользователей, средств, способов и технологий, осуществляющих сбор, формирование, передачу, хранение, обработку, представление и интерпретацию информации.

Инфраструктура информационная критическая – совокупность информационных систем, информационно-телекоммуникационных сетей и автоматизированных систем управления, функционирующих в интересах государственных органов и государственных учреждений, организаций здравоохранения, науки, транспорта, связи, энергетики, банковской и финансовой сферы, топливно-энергетического комплекса, атомной энергетики, организаций оборонной, горнодобывающей, металлургической, химической, ракетно-космической промышленности, а также сети связи используемые для организации взаимодействия между ними.

Искусственная помеха – см. помеха преднамеренная.

Искусственное дестабилизирующее воздействие – см. воздействие дестабилизирующее искусственное.

Источник радиоизлучения (ИРИ) – объект, излучающий в радиодиапазоне электромагнитных волн.

Канал связи (КС) – совокупность средств связи и среды распространения, обеспечивающая передачу сигналов электросвязи между узлами связи в определенной полосе частот или с определенной скоростью.

Качественный показатель – см. показатель качественный.

Качество – степень соответствия совокупности присущих некоторому объекту характеристик определенным требованиям [390].

Качество связи – это свойство связи, которое характеризует ее способность обеспечивать своевременную, достоверную и безопасную передачу сообщений.

Качество обслуживания (QoS – Quality of Service) – способность системы связи обеспечить необходимый (требуемый) уровень множества параметров передачи пользовательских данных определенного типа путем использования различных связных технологий и протоколов.

Качество управления – это свойство системы управления, которое характеризует ее способность обеспечивать совокупность характеристик по адекватности, оперативности, непрерывности, скрытности и устойчивости управления.

Количественный показатель – см. показатель количественный.

Комплекс радиоэлектронного подавления – комплекс технических средств для радиоэлектронного подавления, представляющий собой совокупность функционально связанных средств радиоэлектронного подавления, средств технической разведки и средств управления этим комплексом [394].

Комплексное информационно-техническое воздействие – см. воздействие информационно-техническое комплексное.

Комплексный контроль защиты информации – совокупность мероприятий, направленных на: выявление демаскирующих признаков в деятельности войск в ходе их боевого применения и использования вооружения, военной техники и военных объектов; оперативное пресечение нарушений установленных норм и требований по противодействию разведкам.

Комплексный технический контроль – совокупность мероприятий, направленных на: оценку защищенности своих радиоэлектронных средств от технических средств разведки противника; защиту охраняемых сведений о своих средствах, комплексах и системах; обеспечение электромагнитной совместимости своих радиоэлектронных средств.

Компьютерная разведка – см. разведка компьютерная.

Компьютерная сеть – см. сеть компьютерная.

Компьютерная система – см. система компьютерная.

Компьютерный вирус – см. вирус.

Контратака – встречная атака, предпринимаемая обороняющимися, с целью отбить наступление противника или самому перейти в наступление.

Контратакующее информационно-техническое воздействие – см. воздействие информационно-техническое контратакующее.

Контрразведка – деятельность по пресечению разведывательной деятельности соответствующих сил и средств противоположной стороны.

Конфигурация – определенный набор параметров системы, функциональных и структурных связей ее элементов, задающий определенный режим ее работы.

Конфигурация системы связи – формализованное представление текущего состояния системы связи, описывающее распределение ресурсов на всех ее

уровнях, состава и взаимного расположения линий и узлов, оборудования узлов, протоколов, алгоритмов и их параметров, а также множество информационных структур, которые в настоящий момент реализованы в системе связи.

Конфиденциальность информации – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на это право [65].

Конфликт – специфический процесс взаимодействия двух или большего количества компонентов системы (или систем в целом), преследующих разные интересы (цели) [5].

Конфликт антагонистический – конфликт, в котором интересы (цели) конфликтующих систем (сторон) строго противоположны [5].

Конфликт внутриуровневый – между двумя элементами многоуровневой системе, которые расположены на одном и том же уровне.

Конфликт информационный – процесс столкновения сторон на этапах сбора, формирования, передачи, хранения, обработки, представления и интерпретации информации о состоянии, намерениях и действиях своей и противостоящей стороны, при этом каждая из сторон стремится к упреждающим действиям по отношению к противостоящей стороне и предпринимает определенные действия по снижению возможностей противостоящей стороны и обеспечению независимости и эффективности своей системы от вмешательства действий другой стороны.

Конфликт информационный многоэтапный – информационной конфликт, длительность которого может быть представлена в виде отдельных этапов – локальных конфликтов вида «стадия нападения – стадия защиты» в котором фиксированы выбранные сторонами стратегии нападения и защиты.

Конфликт локальный – конфликт строго определенного состава сторон и иерархического уровня при фиксированных и неизменных направлении конфликта, содержании действий и задач конфликтующих сторон [5].

Конфликт межуровневый – конфликт между двумя различными уровнями в многоуровневой системе, который характеризуется невозможностью достижения глобальной цели за счет реализации локальных задач уровней.

Криптостойкость системы связи – способность системы связи обеспечивать заданный уровень криптографической защиты и противостоять раскрытию смыслового содержания передаваемой информации.

Критерии безопасности – правила, которые по качественным и количественным параметрам позволяют сделать вывод о достигнутом уровне безопасности системы [395].

Критерий – это признак, правило, мера суждения, на основании которых проводится оценка или классификация чего-либо по значениям одного критериального показателя (простой критерий) или нескольких показателей (интегральный критерий) [390].

Критерий оптимальности – минимизируемый или максимизируемый показатель, по значению которого оценивается оптимальность найденного решения, то есть максимальное удовлетворение поставленным требованиям.

Критерий оптимизации – см. критерий оптимальности.

Критическая информационная инфраструктура – см. инфраструктура информационная критическая.

Линия связи – элемент системы связи, обеспечивающий образование каналов связи транспортной (первичной) сети связи, имеющих общую среду распространения, а также силы и средства их обслуживания.

Локальный конфликт – см. конфликт локальный.

Маршрут – конечная чередующаяся последовательность вершин и ребер в графе, начинающаяся и оканчивающаяся на вершинах, являющимися концевыми.

Межуровневый конфликт – см. конфликт межуровневый.

Многоуровневая система – см. система многоуровневая.

Многоэтапный информационный конфликт – см. конфликт информационный многоэтапный.

Мобильность системы связи – способность системы связи в установленные сроки развертываться, свертываться, изменять структуру и место (район) развертывания в соответствии с реально складывающейся обстановкой.

Мониторинг – процесс наблюдения, анализа и прогноза изменения состояния какого-либо объекта [390].

Мониторинг параметров – наблюдение за какими-либо параметрами. Результат мониторинга параметров представляет собой совокупность измеренных значений параметров, получаемых на интервалах времени, в течение которых значения параметров существенно не изменяются [390].

Мониторинг состояния – наблюдение за состоянием объекта для определения момента перехода в предельное состояние. Принципиальным отличием мониторинга состояния от мониторинга параметров является наличие интерпретатора измеренных параметров в терминах состояния объекта [390].

Наблюдаемость – в теории управления: свойство системы, показывающим, можно ли по выходным данным полностью восстановить информацию о состояниях системы.

Наблюдение – преднамеренное, систематическое и целенаправленное определение состояния или параметров системы, процесса, явления, без активного воздействия на них, с целью определения закономерностей их изменения в определенных условиях.

Надежность – в теории систем: способность системы сохранять свои характеристики при изменении параметров среды [385].

Надежность системы связи – способность системы связи обеспечивать связь с требуемым качеством, сохраняя во времени требуемые значения эксплуатационных показателей, технического обслуживания, восстановления и ремонта.

Направление связи – совокупность линий и узлов связи, обеспечивающая связь между конкретной парой узлов в сети.

Нарушение функционирования – прекращение выполнения объектом установленных функций или выполнение им несвойственных функций, не предусмотренных регламентом его работы.

Нарушитель – субъект, преднамеренно использующий уязвимости технических и нетехнических мер и средств контроля и управления безопасностью информационной системы с целью снижения их эффективности или снижения уровня конфиденциальности, доступности и целостности информационных ресурсов.

Непреднамеренное дестабилизирующее воздействие – см. воздействие дестабилизирующее преднамеренное.

Непрерывность управления – возможность органов управления постоянно взаимодействовать с объектами управления.

Несанкционированный доступ – см. доступ несанкционированный.

Обеспечивающее информационно-техническое воздействие – см. воздействие информационно-техническое обеспечивающее.

Оборонительное информационно-техническое воздействие – см. воздействие информационно-техническое оборонительное.

Объект воздействия – человек, группа лиц или техническое средство, которое подвергается воздействию со стороны субъекта воздействия.

Обычное оружие – см. оружие обычное.

Огневое поражение – см. поражение огневое.

Оперативность управления – способность получать, обрабатывать и преобразовывать информацию в соответствии с темпом изменения состояния объекта управления и текущих параметров среды.

Оптико-электронная разведка – см. разведка оптико-электронная.

Оптико-электронное подавление – см. подавление оптико-электронное.

Организационно-техническая система – см. система организационно-техническая.

Оружие высокоточное – вид оружия, оснащенного системой управления и обеспечивающего поражение цели одним боеприпасом в пределах дальности своего действия с высокой вероятностью.

Оружие на новых физических принципах – средства вооруженной борьбы, поражающее действие которых основывается на использовании направленных высокоэнергетических излучений и полей, нейтральных или заряженных частиц, доводимых до объектов поражения, а также на других нетрадиционных или принципиально новых способах поражения. Как правило, к такому виду оружия относятся лазерное, ускорительное, сверхвысокочастотное, информационное, инфразвуковое, геофизическое и т.д.

Оружие обычное – объединение видов оружия, не относящихся к оружию массового поражения, включающие в себя огнестрельное, реактивное, ракетное, бомбовое, минно-взрывное, огнеметно-зажигательное, торпедное оружие, средства непосредственного поражения, которые снаряжаются бризантными взрывчатыми веществами или зажигательными смесями, а также холодное оружие.

Оружие, самонаводящиеся на излучение – оружие с пассивной системой наведения по излучениям военной техники в диапазонах электромагнитных, оптических и акустических волн.

Основной цифровой канал (ОЦК) – цифровой канал связи со скоростью 64 кбит/с, позволяющий передавать оцифрованные с достаточным качеством голосовые сообщения в диапазоне 0,3-3,4 кГц.

Отвлекающее информационно-техническое воздействие – см. воздействие информационно-техническое контратакующее.

Отказ – нарушение работоспособности объекта, при котором он или его элемент перестает выполнять целиком или частично свои функции.

Отображение – закон, по которому каждому элементу одного множества ставится в соответствие вполне определенный элемент другого множества.

Параметр – количественная характеристика свойств чего-либо или кого-либо [390].

Параметры радиоэлектронного средства – совокупность энергетических, частотных, структурных, информационных, временных и пространственных параметров радиоэлектронного средства.

Параметры радиоэлектронного средства временные – параметры, описывающие время и длительность работы радиоэлектронного средства.

Параметры радиоэлектронного средства информационные – параметры, описывающие целевую и служебную информацию, передаваемую радиоэлектронным средством, а также информацию, формируемую радиоэлектронным средством по итогам приема и обработки сигналов.

Параметры радиоэлектронного средства пространственные – параметры, описывающие местоположение радиоэлектронного средства и пространственную ориентации направлений его работы.

Параметры радиоэлектронного средства структурные – параметры, описывающие структуру излучаемых радиоэлектронным средством сигналов.

Параметры радиоэлектронного средства частотные – параметры, описывающие частоты и спектр излучаемых радиоэлектронным средством сигналов.

Параметры радиоэлектронного средства энергетические – параметры, описывающие мощность (энергию) излучаемых радиоэлектронным средством сигналов.

Пассивная преднамеренная радиоэлектронная помеха – см. помеха радиоэлектронная преднамеренная пассивная.

Пассивное информационно-техническое воздействие – см. воздействие информационно-техническое пассивное.

Первичная сеть связи – см. сеть связи транспортная.

Подавление оптико-электронное – радиоэлектронное подавление, ведущееся в оптическом диапазоне и заключающееся в снижении эффективности функционирования оптико-электронных систем противника путем воздействия на них преднамеренными оптико-электронными помехами. Результатом оптико-электронного подавления может быть нарушение работы тепловых, телевизионных, лазерных и оптико-визуальных систем и средств разведки, наблюдения и связи [394].

Подавление радиоэлектронное – снижение эффективности функционирования радиоэлектронных средств путем воздействия на них преднамеренными радиоэлектронными помехами [394].

Показатель – характеристика, функция характеристик или величина, выбранная для оценки некоторого свойства объекта или совокупности его свойств. Показатель обычно имеет наименование, обозначение и значение. Показатели разделяют на количественные и качественные [390].

Показатель интегральный – обобщающий, сводный показатель, объединяющий частные показатели и характеризующий всю группу показателей в целом [390].

Показатель качественный – показатель, в виде понятия какой-либо установленной шкалы суждений, отражающей качественные предпочтения (например: хуже, лучше, больше, меньше и т.п.), либо бальной шкалы или шкалы весовых коэффициентов [390].

Показатель количественный – показатель, выражающийся в виде величины, являющейся функцией от параметров объекта, и определяющий абсолютную или относительную (долю, часть) числовую меру проявления свойства или совокупности свойств [390].

Полнота информации – состав и объем информации достаточный для правильного принятия решения или понимания какого-либо явления.

Пользователь – лицо или организация, которое использует действующую систему для выполнения конкретной функции [391].

Пользовательская компьютерная разведка – см. разведка компьютерная *пользовательская.*

Помеха – нежелательное физическое явление или воздействие электрических, акустических, магнитных, электромагнитных или других полей, электрических токов или напряжений внешнего или внутреннего источника, которое нарушает работоспособность технических и радиоэлектронных средств, вызывает ухудшение технических характеристик и параметров этих средств или снижет их эффективность.

Помеха естественная – помеха, создаваемая в условиях природы, природным источником или источником искусственного происхождения без цели преднамеренного нарушения работоспособности других технических средств.

Помеха искусственная – см. помеха преднамеренная.

Помеха преднамеренная – помеха, создаваемая источником искусственного происхождения с целью нарушить работоспособность технического средства, вызывать ухудшение технических характеристик и параметров этого средства или снизить его эффективность.

Помеха радиоэлектронная – электромагнитное излучение в виде отражающего, поглощающего, рассеивающего или модулирующего образования, которое, воздействуя на элементы радиоэлектронного средства или на среду распространения электромагнитных волн, снижает эффективность его функционирования [9].

Помеха радиоэлектронная преднамеренная активная – преднамеренная радиоэлектронная помеха, создаваемая непосредственно средством радиоэлектронного подавления [394].

Помеха радиоэлектронная преднамеренная пассивная – преднамеренная радиоэлектронная помеха, создаваемая отражением излучения подавляемого радиоэлектронного средства или формированием в среде распространения этого излучения отражающих, поглощающих, рассеивающих или модулирующих образований снижает эффективность функционирования подавляемого радиоэлектронного средства [394].

Помехозащищенность системы связи – способность системы связи обеспечивать связь с требуемым качеством в условиях воздействия на нее преднамеренных помех.

Помехоустойчивость – в теории систем: способность системы выполнять свои функции в условиях помех [387].

Помехоустойчивость системы связи – способность системы связи обеспечивать связь с требуемым качеством в условиях воздействия на нее всех видов помех.

Поражение огневое – уничтожение (подавление) противника огнём различных видов оружия, ударами ракетных войск и авиации с применением боеприпасов в обычном снаряжении.

Поражение радиоэлектронное – совокупность мероприятий и действий по функциональному радиоэлектронному поражению, радиоэлектронному подавлению, поражению самонаводящимся на излучение оружием радиоэлектронных средств противника [394].

Поражение самонаводящимся на излучение оружием – уничтожение или повреждение элементов радиоэлектронных средств оружием с пассивной системой наведения по излучениям военной техники в диапазонах электромагнитных, оптических и акустических волн.

Поражение функциональное – разрушение, повреждение или необратимое нарушение функционирования элементов радиоэлектронных средств путем использования электромагнитного излучения или информационно-технического воздействия.

Поражение функциональное электромагнитным излучением – разрушение и/или повреждение элементов радиоэлектронных средств путем использования однократных или многократных импульсных электромагнитных воздействий, приводящих к необратимым изменениям электрофизических параметров в полупроводниковых или оптико-электронных элементах в результате их перегрева или пробоя [9].

Потоковая компьютерная разведка – см. разведка компьютерная потоковая.

Преднамеренная помеха – см. помеха преднамеренная.

Преднамеренное дестабилизирующее воздействие – см. воздействие дестабилизирующее преднамеренное.

Преднамеренное силовое электромагнитное воздействие (ПС ЭМВ) – см. воздействие электромагнитное силовое преднамеренное.

Программная закладка – см. закладка программная.

Программное обеспечение (ПО) – программы, процедуры и, возможно, соответствующая документация и данные, относящиеся к функционированию компьютерной системы [393].

Программное средство – см. средство программное.

Пропускная способность сети – максимально возможная суммарная скорость передачи сообщений по всем информационным направлениям связи для конкретных условий функционирования.

Пропускная способность системы связи – способность системы связи передавать и обрабатывать определенный объем сообщений, пакетов или данных в единицу времени.

Пространственная скрытность – см. скрытность пространственная.

Пространственные параметры радиоэлектронного средства – см. параметры радиоэлектронного средства пространственные.

Пространство информационное – совокупность функционально совместимых информационных ресурсов, технологий их сопровождения и использования, а также информационных систем и информационной инфраструктуры, функционирующих на основе общих принципов и обеспечивающих информационное взаимодействие пользователей, а также удовлетворение их потребностей в информации.

Противник – субъект, с которым ведется противоборство, соперничество или соревнование в военной, в информационной или в другой сфере с целью достижения победы над ним.

Протокол – формализованный набор правил, задаваемых алгоритмами его функционирования, а также их параметрами, которые позволяют осуществлять соединение и обмен данными между двумя или более функциональными элементами системы связи. Как правило, в рамках протокола рассматривается взаимодействие на одном уровне модели OSI.

Протокол неэффективно функционирующий – протокол не обеспечивающий требуемые значения показателей качества.

Протокол эффективно функционирующий – протокол обеспечивающий показатели качества не ниже требуемого.

Процесс информационный – процесс получения, создания, сбора, обработки, накопления, хранения, поиска, распространения, представления и использования информации.

Путь – открытая цепь, то есть цепь, концевые вершины которой различны.

Работоспособность – это состояние объекта, при котором он способен выполнять свои функции с требуемыми параметрами.

Радио- и радиотехническая разведка (РРТР) – см. разведка радио- и радиотехническая.

Радиолокационная разведка (РЛР) – см. разведка радиолокационная.

Радиоподавление – радиоэлектронное подавление, ведущееся в диапазоне радиоволн и заключающееся в снижении эффективности функционирования

радиоэлектронных средств противника путем воздействия на них преднамеренными радиопомехами [394].

Радиопомеха – радиоэлектронная помеха в диапазоне радиоволн.

Радиоразведка (РР) – составная часть радиоэлектронной разведки, ориентированная на добывание сведений в системах радиосвязи, основным содержанием которой является: обнаружение и перехват открытых, засекреченных, кодированных передач; пеленгование их источников; анализ и обработка добываемой информации; снижение нагрузки или подрыв криптографических систем [117].

Радиотехническая разведка – см. разведка радиотехническая.

Радиоэлектронная борьба (РЭБ) – совокупность взаимосвязанных по цели, задачам, месту и времени мероприятий, действий, направленных на выявление радиоэлектронных средств и систем противника, их подавление, радиоэлектронную защиту своих радиоэлектронных систем и средств от средств РЭП противника, а также на радиоэлектронно-информационное обеспечение [394].

Радиоэлектронная защита (РЭЗ) – совокупность мероприятий и действий по устранению или ослаблению воздействия средств радиоэлектронного поражения на свои радиоэлектронные средства, защите их от технических средств разведки и обеспечению их электромагнитной совместимости [394].

Радиоэлектронная защита от технической разведки – исключение или существенное затруднение добывания противником с помощью технических средств разведки охраняемых сведений о радиоэлектронных средствах путем устранения разведывательных признаков по первичным и вторичным полям военных объектов, а также защите передаваемой, обрабатываемой и хранимой информации.

Радиоэлектронная разведка – см. разведка радиоэлектронная.

Радиоэлектронное воздействие – см. воздействие радиоэлектронное.

Радиоэлектронное дестабилизирующее воздействие – см. воздействие радиоэлектронное.

Радиоэлектронное подавление (РЭП) – подавление радиоэлектронное.

Радиоэлектронное поражение (РЭПр) – см. поражение радиоэлектронное.

Радиоэлектронное средство (РЭС) – см. средство радиоэлектронное.

Радиоэлектронно-информационное обеспечение – совокупность мероприятий и действий по выявлению функционирования радиоэлектронных средств противника в целях их радиоэлектронного поражения и контролю функционирования своих средств в целях их радиоэлектронной защиты [394].

Разведзащищенность системы связи – способность системы связи противостоять всем видам разведки.

Разведка – сбор сведений о противоположной стороне или конкуренте для обеспечения своей безопасности и получения преимуществ в области вооружённых сил, военных действий, политики, экономики или техники [117].

Разведка компьютерная – добывание информации из компьютерных систем и сетей, характеристик их программно-аппаратных средств и пользователей [123].

Разведка компьютерная алгоритмическая – разведка, обеспечивающая добывание информации путем использования заранее внедренных изготовителем программных или аппаратных закладок, ошибок и недекларированных возможностей компьютерных систем и сетей [123].

Разведка компьютерная аппаратная – разведка, обеспечивающая добывание информации путем обработки сведений, получения аппаратуры, оборудования, технических модулей и их анализа, испытания для выявления их технических характеристик и возможностей, полученных другими видами компьютерной разведки [123].

Разведка компьютерная вирусная – разведка, обеспечивающая добывание данных путем внедрения и применения вирусных программ в уже эксплуатируемые программные комплексы и в системы для перехвата управления компьютерными системами [123].

Разведка компьютерная пользовательская – разведка, обеспечивающая добывание информации о пользователях, их деятельности и интересах на основе определения их сетевых адресов, местоположения, организационной принадлежности, анализа их сообщений и информационных ресурсов, а также путем обеспечения им доступа к информации, циркулирующей в специально созданной ложной информационной инфраструктуре [123].

Разведка компьютерная потоковая – разведка, обеспечивающая добывание информации путем перехвата, обработки и анализа сетевого трафика, выявления структур компьютерных сетей, а также их технических параметров [123].

Разведка компьютерная разграничительная – разведка, обеспечивающая добывание информации из отдельных (локальных) компьютерных систем, которые могут не входить в состав сети, осуществляемая на основе преодоления средств разграничения доступа путем несанкционированного доступа к информации, физического доступа к компьютерной системе или к носителям информации [123].

Разведка компьютерная семантическая – разведка, обеспечивающая добывание фактографической и индексно-ссылочной информации путем поиска, сбора и анализа структурируемой и неструктурируемой информации из общедоступных информационных ресурсов или конфиденциальных источников компьютерных систем и сетей, а также путем семантической (аналитической) обработки полученных и накопленных массивов сведений и документов [123].

Разведка компьютерная сетевая – разведка, обеспечивающая добывание информации из компьютерных сетей путем мониторинга сети, инвентаризации и анализа уязвимостей сетевых ресурсов и объектов пользователей, а также последующего удаленного доступа к информации путем использования выявленных уязвимостей систем и средств сетевой (межсетевой) защиты ресурсов, а также блокирование доступа к ним, модификация, перехват управления либо маскировка своих действий [123].

Разведка компьютерная форматная – разведка, обеспечивающая добывание информации путем агрегированной обработки, фильтрации, декодирования, а также проведения других преобразований форматов (представления, пе-

редачи и хранения) добытых данных в сведения, а затем – в информацию для последующего ее наилучшего представления пользователям [123].

Разведка оптико-электронная – процесс добывания информации с помощью средств, включающих входную оптическую систему с фотоприемником и электронные схемы обработки электрического сигнала, которые обеспечивают прием и анализ электромагнитных волн видимого и ИК-диапазонов, излученных или отраженных объектами и местностью [117].

Разведка по открытым источникам – поиск, выбор и сбор разведывательной информации из общедоступных источников, а также её анализ.

Разведка радио- и радиотехническая – виды радиоэлектронной разведки, ориентированные на добывание сведений в системах радиосвязи и о радиоэлектронных системах противника по их собственным излучениям [117].

Разведка радиолокационная – вид технической разведки, в ходе которой информация добывается с помощью радиолокационных станций [117].

Разведка радиотехническая (РТР) – вид радиоэлектронной разведки, целью которой являются сбор и обработка информации, получаемой с помощью своих радиоэлектронных средств о радиоэлектронных системах противника по их собственным излучениям, и последующая их обработка с целью получения информации о положении источника излучения, его скорости, наличии данных в излучаемых сигналах [117].

Разведка радиоэлектронная – процесс получения информации в результате приема и анализа электромагнитных излучений радиодиапазона, создаваемых работающими радиоэлектронными средствами [117].

Разведка техническая – целенаправленная деятельность по добыванию информации с помощью соответствующих технических средств [117].

Разграничительная компьютерная разведка – см. разведка компьютерная разграничительная.

Разрушение информации – полная потеря хранящихся в информационных системах или передаваемых по информационным сетям данных или их изменение, исключающее возможность правильной их интерпретации и восстановления [395].

Режим – условия работы, деятельности, существования чего-либо.

Ресурс – количественно измеряемая возможность выполнения какой-либо деятельности; условия или средства, позволяющие с помощью определенных преобразований получить желаемый результат.

Ресурс информационный – отдельный массив информации, который представлен в форме документов, массивов сведений, баз данных, баз знаний или других форм организованного представления информации.

Ресурс связи – совокупность канальных, временных, частотных, энергетических и других ресурсов, требуемых для организации связи.

Ресурс сети – совокупность канальных, временных, частотных, энергетических и других ресурсов сети связи, затрачиваемых на передачу данных всех абонентов сети. На сетевом и транспортном уровне сети связи под ресурсом зачастую понимают суммарную пропускную способность выделенную направлению связи между парой абонентов.

Риск – сочетание вероятности и последствий наступления неблагоприятных событий. Также риском часто называют непосредственно предполагаемое событие, способное принести кому-либо ущерб или убыток.

Род связи – классификационная группировка связи, выделенная по среде распространения сигналов или по применяемым средствам связи.

Самонаводящиеся на излучение оружие (СНИО) – см. оружие, самонаводящиеся на излучение.

Самоорганизуемость – в теории систем: способность системы самостоятельно вследствие внутренних процессов изменять свое поведение или структуру приспосабливаясь к изменяющимся условиям среды, сохраняя при этом свою целостность [384, 388].

Сбой – кратковременная самоустраняющаяся утрата работоспособности объекта.

Своевременность связи – свойство связи, которое характеризует ее способность обеспечивать передачу или сообщений или ведение переговоров в заданные сроки.

Связь – обмен информацией или передача данных в виде сообщений в системе связи.

Семантическая компьютерная разведка – см. разведка компьютерная *семантическая.*

Сервис – набор услуг связи на определенном уровне модели OSI, который обеспечивает функции вышестоящего уровня модели OSI. Зачастую, если рассматриваемый уровень модели OSI не конкретизируется, то рассматривается сервис 7-го прикладного уровня который обеспечивается системой связи для ее абонентов.

Сетевая компьютерная разведка – см. разведка компьютерная сетевая.

Сетевой ресурс – см. ресурс сети.

Сеть абонентского доступа – совокупность технических средств и связей между ними, обеспечивающая потребителей различными видами услуг по доставке, хранению и обработке информации [2].

Сеть информационно-телекоммуникационная – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Сеть компьютерная – объединение компьютерных систем путем включения их в сеть связи или соединения их линиями связи [123].

Сеть связи – технологическая система, включающая в себя средства и линии связи и предназначенная для электросвязи или почтовой связи [59].

Сеть связи выделенная – сеть связи, которая организуется в интересах отдельных категорий должностных лиц, пунктов управления и специальных систем управления.

Сеть связи специального назначения – сеть связи, предназначенная для нужд органов государственной власти, нужд обороны страны, безопасности государства и обеспечения правопорядка [59].

Сеть связи транспортная – совокупность технических средств, комплексов, линий связи и обслуживающего персонала, обеспечивающая потребителей

стандартными каналами (трактами) передачи первичных электрических сигналов [2].

Сеть фельдъегерско-почтовой связи – сеть в которой доставка информации (в виде карт, схем, посылок, бандеролей, писем и т.д.) осуществляется специальными курьерами (фельдъегерями) с помощью обычных транспортных средств.

Сеть электросвязи – сеть связи, обеспечивающая электросвязь при помощи электромагнитных систем. Сеть электросвязи состоит из сетей следующих категорий: сети 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 [59].

Система – комбинация взаимодействующих элементов, организованных для достижения одной или нескольких поставленных целей [390].

Система государственного и военного управления – совокупность органов государственной власти обеспечивающих непрерывное и устойчивое управление государством в условиях мирного и военного времени.

Система дестабилизирующих воздействий – организационно-техническая система, состоящая из подсистем разведки, нападения и управления, целью которой является преднамеренное формирование дестабилизирующих воздействий, нарушающих работоспособность технических средств или программ, ухудшение их характеристик и параметров, снижение их эффективности. В частном случае, под системой дестабилизирующих воздействий, может пониматься, только подсистема нападения, реализующая такие воздействия как: физическое и функциональное поражение, радиоэлектронное подавление, информационно-технические воздействия.

Система динамическая – множество элементов, для которого задана функциональная зависимость между временем и положением в пространстве состояний каждого элемента системы.

Система инфокоммуникационная – информационная система, обеспечивающая предоставление набора как связных, так и информационных услуг с гибкими возможностями по управлению ими и их персонализации [37].

Система инфокоммуникационная специального назначения – информационная система, обеспечивающая предоставление набора как связных, так и информационных услуг с гибкими возможностями по управлению ими и их персонализации, и предназначенная для нужд органов государственной власти, обороны страны, безопасности государства и обеспечения правопорядка [37].

Система информационная – система, предназначенная для формирования, передачи, хранения, поиска, обработки и представления информации, а также соответствующие ресурсы (организационные, технические, финансовые и т.д.), которые обеспечивают данные процессы.

Система информационно-вычислительная – совокупность данных (или баз данных), систем управления базами данных и прикладных программ, функционирующих на вычислительных средствах как единое целое для решения задач обработки информации.

Система компьютерная – совокупность взаимосвязанных или смежных устройств, одно или более из которых, действуя в соответствии с программой, осуществляет автоматизированную обработку данных.

Система многоуровневая – система, состоящая из множества взаимодействующих подсистем (элементов) имеющих иерархическую структуру, при этом каждый уровень иерархии объединяет подсистемы (элементы) имеющие однородные характеристики по отношению к подсистемами (элементам) на других уровнях [390].

Система мониторинга – система реализующая процесс наблюдения, анализа и прогноза изменения состояния какого-либо объекта [390].

Система организационно-техническая – множество взаимосвязанных технических средств и персонала, обеспечивающего их функционирование, предназначенных для достижения для достижения одной или нескольких поставленных целей.

Система связи (СС) – это совокупность распределенных в пространстве взаимосвязанных технических средств и обслуживающего персонала, выполняющих задачи по обеспечению информационного обмена.

Система связи общего пользования (СС ОП) – совокупность распределенных в пространстве взаимосвязанных технических средств и обслуживающего персонала, выполняющих задачи по возмездному оказанию услуг связи любому пользователю.

Система связи специального назначения (СС СН) – это совокупность распределенных в пространстве взаимосвязанных технических средств и обслуживающего персонала, выполняющих задачи по обеспечению информационного обмена в системах государственного и военного управления, а также в системах управления обеспечением безопасности и правопорядка [2].

Система сложная – система, состоящая из множества взаимодействующих подсистем, вследствие чего она приобретает новые эмерджентные свойства как единое целое, которые не могут быть сведены к свойствам взаимодействия отдельных подсистем. К признакам сложной системы относят: 1) отсутствие строго формализованного описания системы или алгоритма ее функционирования; 2) трудность в наблюдаемости и управляемости такой системы, обусловленная большим числом второстепенных (по отношению к цели управления) процессов; 3) наличие множества целей функционирования (управления); 4) нестационарность системы, выражающаяся в изменении характеристик и параметров, а также структурная или функциональная эволюция системы во времени; 5) невоспроизводимость экспериментальных исследований с системой [390].

Система специального назначения – система предназначеная для нужд органов государственной власти, нужд обороны страны, безопасности государства и обеспечения правопорядка.

Система телекоммуникационная – это совокупность связанных линиями связи сетевых узлов, которая основана на единой транспортной технологии и эксплуатируется в соответствии с едиными принципами маршрутизации, адресации и управления, при этом в ее составе имеются граничные узлы, ответ-

ственные за допуск трафика в сеть или направление его в другие смежные телекоммуникационные системы.

Система технологическая – совокупность взаимосвязанных технологическими потоками и действующих как единое целое аппаратов, технических средств, предметов и исполнителей которыми осуществляется определенная последовательность технологических операций с целью выпуска конкретной продукции, выполнения регламентированных технологических процессов или операций.

Система управления – систематизированный набор сил и средств наблюдения за управляемым объектом, а также сил и средств воздействия на его поведение, в интересах достижения определенных целей [390].

Система управления воздействиями – часть системы дестабилизирующих воздействий, обеспечивающая ее функционирование с целью максимизации эффективности формируемых воздействий или достижения целевого эффекта от применения воздействий.

Система управления связью – часть системы связи, обеспечивающая ее функционирование с заданным качеством и состоящая из взаимоувязанных органов и пунктов управления системой связи, средств служебной связи и средств автоматизации.

Скрытность временная – способность противостоять вскрытию средствами радио- и радиотехнической разведки временных параметров работы радиоэлектронного средства.

Скрытность информационная – способность противостоять вскрытию смысла передаваемых сообщений средствами радио- и компьютерной разведки. К информационной скрытности также можно отнести способность противостоять вскрытию служебной информации протоколов и адресно-сетевой информации системы связи средствами сетевой и потоковой компьютерной разведки;

Скрытность пространственная – способность противостоять вскрытию местоположения радиоэлектронного средства и пространственной ориентации направлений ее работы.

Скрытность системы связи – способность системы связи противостоять раскрытию противником факта передачи, содержания передаваемой информации, мест расположения узлов связи, пунктов управления и режимов работы средств связи.

Скрытность структурная – способность противостоять вскрытию структуры сигнала (определяется используемым кодированием и модуляцией) средствами радио- и радиотехнической разведки.

Скрытность управления – способность сохранять в тайне информацию о процессах управления, конечной цели и решаемых задачах, имеющихся силах и средствах, а также их возможностей; факт, время и место передачи управляющей информации, ее содержание и принадлежность к конкретным объектам системы управления.

Скрытность энергетическая – способность противостоять обнаружению сигналов радиоэлектронного средства со стороны средств радио- и радиотехнической разведки.

Сообщение – форма представления информации (данных) имеющая формальную внутреннюю структуру, начало и конец, и предназначенная для передачи.

Состояние – совокупность стабильных значений переменных параметров объекта или системы.

Способ информационно-технического воздействия – порядок применения сил информационных операций и средств информационно-технического воздействия, вызывающий заданные структурные и/или функциональные изменения в объекте воздействия.

Способ радиоэлектронного подавления – порядок применения сил и средств радиоэлектронного подавления.

Средство аппаратное – часть аппаратуры, предназначенная для выполнения определенной функции, в основу функционирования которой положены принципы механики, радиотехники, электроники, электротехники, оптики или других разделов техники.

Средство информационно-технического воздействия – техническое, аппаратное или программное средство, реализующее информационно-техническое воздействие или защиту от него.

Средство поражения – оружие, которое основано на использовании энергии взрывчатых веществ и зажигательных смесей (артиллерийские, ракетные и авиационные боеприпасы, стрелковое вооружение, мины, зажигательные боеприпасы и огнесмеси), а также холодное оружие.

Средство программное – программа для выполнения определенной функции, реализованная в виде последовательности инструкций для выполнения в компьютерной системе или в электронно-вычислительной машине.

Средство радиоэлектронного подавления – техническое средство, реализующее радиоэлектронное подавление путем создания радиоэлектронных помех [394].

Средство радиоэлектронное – техническое средство, в основу функционирования которого положены принципы радиотехники и электроники и, как правило, предназначенное для передачи и/или приёма радиоволн, состоящие из одного или нескольких передающих и/или приёмных устройств либо комбинации таких устройств и включающие в себя вспомогательное оборудование изделие и/или его составные части.

Средство связи – техническое средство, предназначенное для передачи и/или приема, обработки и/или хранения сообщений в системе связи, сети связи, организованных на базе каналов передачи транспортной сети и обеспечивающая один из видов электросвязи.

Средство техническое – изделие, оборудование, аппаратура или их составные части, функционирование которых основано на законах механики, электротехники, радиотехники и электроники, предназначенное для выполнения определенной функции.

Степень вершины – число ребер, инцидентных этой вершине.

Стратегия – в теории игр, это полный план действий при всевозможных ситуациях, способных возникнуть. Стратегия определяет действие игрока в лю-

бой момент игры и для каждого возможного течения игры, способного привести к каждой ситуации.

Структура сети информационная – это формализованное представление в виде сети, наложенной на физическую структуру, которая обязуется множеством путей передачи информационных сообщений между узлами.

Структура сети физическая – это формализованное представление сети в виде совокупности узлов и каналов связи.

Структура системы – совокупность элементов системы и устойчивых связей между ними, обеспечивающих целостность системы и сохранение ее основных свойств при различных внешних и внутренних изменениях [390].

Структурная скрытность – см. скрытность структурная.

Структурная устойчивость системы связи – см. устойчивость системы связи структурная.

Структурные параметры радиоэлектронного средства – см. параметры радиоэлектронного средства структурные.

Субъект воздействия – источник, реализующий воздействия на объект целью достижения своих интересов.

Телекоммуникационная система (ТКС) – см. система телекоммуникационная.

Техническая разведка – см. разведка техническая.

Технический канал утечки информации – совокупность объекта технической разведки, физической среды распространения информационного сигнала и средств, которыми добывается защищаемая информация.

Техническое средство – см. средство техническое.

Технологическая система – см. система технологическая.

Топология сети – множество, в котором между любой парой узлов сети определено обладающее определенными свойствами расстояние, называемое метрикой.

Транспортная сеть связи – см. сеть связи транспортная.

Трафик – нагрузка, создаваемая потоком вызовов, сообщений, пакетов и сигналов, поступающих на средства связи.

Угроза – совокупность условий, факторов и воздействий на систему, создающих потенциальную или реальную опасность нарушения ее работоспособности, ухудшение характеристик, снижения качества или эффективности ее функционирования [254].

Удаленная сетевая атака – см. атака сетевая удаленная.

Узел связи – элемент системы связи, представляющий собой организационно-техническое объединение сил и средств связи, а также средств автоматизированного управления, предназначенный для образования каналов, распределения и/или коммутации каналов, маршрутизации сообщений и пакетов, засекречивания сообщений, передаваемых по каналам сетей связи, предоставления абонентам сети услуг связи, а также эксплуатации технических средств.

Управляемость – в теории управления: свойство системы управления и объекта управления, описывающим возможность перевести систему из одного состояния в другое.

Управляемость системы связи – способность системы связи изменять свое состояние в заданных пределах при воздействии на нее органов управления связью или средств автоматизации управления в соответствии с изменениями обстановки;

Услуга связи – обеспечение определенного вида связи между абонентами.

Устойчивость – в теории систем: способность системы возвращаться в исходное состояние или в состояние равновесия после того, как она была из этого состояния выведена под влиянием внешних возмущающих воздействий. При этом под равновесием понимается состояние системы, которое оно может сохранять сколь угодно долго в отсутствие внешних возмущающих воздействий [384, 385].

Устойчивость сети электросвязи – способность сети электросвязи выполнять свои функции при выходе из строя части ее элементов в результате воздействия дестабилизирующих факторов [66].

Устойчивость системы связи – способность системы связи обеспечивать связь с требуемым качеством в условиях дестабилизирующих воздействий естественного и искусственного характера.

Устойчивость системы связи информационная – способность системы связи как организационно-технической системы в динамике информационного конфликта своевременно, достоверно и скрытно передавать информацию пользователей и осуществлять управление собственными элементами с учетом дестабилизирующих воздействий на эти элементы со стороны противника [5].

Устойчивость системы связи структурная – способность системы связи обеспечивать связь с требуемым качеством в условиях дестабилизирующих воздействий естественного и искусственного характера на элементы ее сети и структуру связей между ними.

Устойчивость системы связи функциональная – способность системы связи обеспечивать связь с требуемом качествам в условиях дестабилизирующих воздействий естественного и искусственного характера приводящих к нарушению функций системы, функций ее элементов или снижению их эффективности.

Устойчивость управления – способность органов управления выполнять свои функции в сложной, резко меняющейся обстановке в условиях помех и дестабилизирующих воздействиях.

Уязвимость – недостаток системы, использование которого делает возможным нанесение системе повреждений любой природы, либо снижение эффективности ее функционирования [390].

Уязвимость информации – объективное свойство информации подвергаться различного рода угрозам, нарушающим ее целостность, достоверность и конфиденциальность [395].

Фактор – это причина, обстоятельство, движущая сила, определяющая причинно-следственные связи в рассматриваемом явлении (процессе) [390].

Фактор дестабилизирующий – воздействие на систему, источником которого является процесс внутреннего или внешнего по отношению к системе характера, приводящий к отказу элементов системы.

Фактор дестабилизирующий внешний – дестабилизирующий фактор, источник которого расположен вне системы.

Фактор дестабилизирующий внутренний – дестабилизирующий фактор, источник которого внутри системы или ее элементов.

Физическая структура сети – см. структура сети физическая.

Физическое поражение – воздействие на объект, обычного или ядерного оружия, средств функционального поражения электромагнитным излучением, другого внешнего дестабилизирующего фактора физической природы, которое приводит к разрушению объекта или необратимому переходу его в такое состояние в котором он не может выполнять свои функции.

Форматная компьютерная разведка – см. разведка компьютерная форматная.

Функциональная устойчивость системы связи – см. устойчивость системы связи функциональная.

Функциональное поражение – см. поражение функциональное.

Функциональное поражение электромагнитным излучением (ФП ЭМИ) – см. поражение функциональное электромагнитным излучением.

Целостность информации – состояние информации, при котором обеспечивается ее достоверность и полнота [64].

Цепь – маршрут, в котором все его ребра (но не вершины) различны.

Частотные параметры радиоэлектронного средства – см. параметры радиоэлектронного средства частотные.

Эксплойт – потенциально безвредный набор данных или последовательности действий, которые некорректно обрабатывается информационной системой, вследствие ошибок в ней. Результатом некорректной обработки такого набора данных или последовательности действий может быть переход информационной системы в уязвимое состояние.

Электромагнитная совместимость системы связи – способность системы связи обеспечивать связь с требуемым качеством в условиях воздействия на нее непреднамеренных радиоэлектронных помех и не создавать таких помех другим системам.

Электросвязь – любые излучение, передача или прием знаков, сигналов, голосовой информации, письменного текста, изображений, звуков или сообщений любого рода по радиосистеме, проводной, оптической и другим электромагнитным системам [59].

Элемент сети связи – узел или линия связи входящая в состав сети связи.

Эмерджентность – в теории систем: наличие у какой-либо системы особых свойств, не присущих ее элементам, а также сумме элементов, не связанных особыми системообразующими связями; несводимость свойств системы к сумме свойств ее компонентов [390].

Энергетическая скрытность – см. скрытность энергетическая.

Энергетические параметры радиоэлектронного средства – см. параметры радиоэлектронного средства энергетические.

Эффект – закономерность протекания процессов или реакций, являющихся результатом или следствием какого-либо действия [390].

Эффект дестабилизирующий – нарушение работоспособности технических средств или программ, ухудшение их характеристик и параметров или снижение их эффективности.

Эффективность – это комплексное операционное свойство целенаправленного процесса функционирования системы, характеризующее его приспособленность к достижению цели операции или к выполнению задачи системы. Эффективность характеризуется степенью соответствия результатов операции её цели. Эффективность обуславливается качеством системы, качеством организации целенаправленного процесса функционирования системы, условиями применения системы. Эффективность измеряется на двух уровнях: показателем качества результатов операции (процесса); показателем эффективности операции (процесса). Эффективность оценивается по критериям пригодности или оптимальности. Необходимо отметить, что понятие «качества» применимо к объектам любой природы. Понятие «эффективности» применимо только к целенаправленным процессам [390].

Литература

1. Барашков П. Н., Родимов А. П., Ткаченко К. А., Чуднов А. М. Модель системы связи с управляемыми структурами в конфликтных условиях. – Л.: ВАС, 1986. – 52 с.

2. Боговик А. В., Игнатов В. В. Эффективность систем военной связи и методы ее оценки. – СПб.: ВАС, 2006. – 183 с.

3. Паршуткин А. В. Концептуальная модель взаимодействия конфликтующих информационных и телекоммуникационных систем // Вопросы кибербезопасности. 2014. № 5 (8). С. 2-6.

4. Паршуткин А. В., Святкин С. А., Бажин Д. А., Сазыкин А. М. Радиоэлектронные информационные воздействия в конфликтах информационных и телекоммуникационных систем // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2015. № 5-6. С. 13-17.

5. Владимиров В. И., Владимиров И. В. Основы оценки конфликтно-устойчивых состояний организационно-технических систем (в информационных конфликтах). – Воронеж: ВАИУ, 2008. – 231 с.

6. Будников С. А., Гревцев А. И., Иванцов А. В., Кильдюшевский В. М., Козирацкий А. Ю., Козирацкий Ю. Л., Кущев С. С., Лысиков В. Ф., Паринов М. Л., Прохоров Д. В. Модели информационного конфликта средств поиска и обнаружения. Монография / под ред. Ю.Л. Козирацкого. – М.: Радиотехника, 2013. – 232 с.

7. Козирацкий Ю. Л., Донцов А. А., Иванцов А. В., Козирацкий А. Ю., Кусакин О. В., Кущев С. С., Лысиков В. Ф., Мазилов С. Л., Паринов М. Л., Прохоров Д. В. Модели пространственного и частотного поиска. Монография / под ред. Ю.Л. Козирацкого. – М.: Радиотехника, 2014. – 344 с.

8. Макаренко С. И. Динамическая модель системы связи в условиях функционально-разноуровневого информационного конфликта наблюдения и подавления // Системы управления, связи и безопасности. 2015. № 3. С. 122-185. – URL: http://sccs.intelgr.com/archive/2015-03/07-Makarenko.pdf (дата обращения 17.02.2019).

9. Макаренко С. И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. Монография. – СПб.: Наукоемкие технологии, 2017. – 546 с.

10. Макаренко С. И., Иванов М. С. Сетецентрическая война – принципы, технологии, примеры и перспективы. Монография. – СПб.: Наукоемкие технологии, 2018. – 898 с.

11. Макаренко С. И. Аудит безопасности критической инфраструктуры специальными информационными воздействиями. Монография. – СПб.: Наукоемкие технологии, 2018. – 122 с.

12. Макаренко С. И. Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий // Системы управления, связи и безопасности. 2018. № 1. С. 1-29. – URL:

http://sccs.intelgr.com/archive/2018-01/01-Makarenko.pdf (дата обращения: 01.06.2019).

13. Макаренко С. И. Вычислительные системы, сети и телекоммуникации: учебное пособие. – Ставрополь: СФ МГГУ им. М.А. Шолохова, 2008. – 352 с.

14. Макаренко С. И., Чукляев И. И. Терминологический базис в области информационного противоборства // Вопросы кибербезопасности. № 1 (2). 2014. С. 13-21.

15. Антонович П. И., Макаренко С. И., Михайлов Р. Л., Ушанев К. В. Перспективные способы деструктивного воздействия на системы военного управления в едином информационном пространстве // Вестник Академии военных наук. 2014. № 3 (48). С. 93-101.

16. Макаренко С. И. Проблемы и перспективы применения кибернетического оружия в современной сетецентрической войне // Спецтехника и связь. 2011. № 3. С. 41-47.

17. Макаренко С. И. Информационное оружие в технической сфере: терминология, классификация, примеры // Системы управления, связи и безопасности. 2016. № 3. С. 292-376. – URL: http://sccs.intelgr.com/archive/2016-03/11-Makarenko.pdf (дата обращения: 01.06.2018).

18. Макаренко С. И. Перспективы и проблемные вопросы развития сетей связи специального назначения // Системы управления, связи и безопасности. 2017. № 2. С. 18-69. – URL: http://sccs.intelgr.com/archive/2017-02/02-Makarenko.pdf (дата обращения: 10.04.2019).

19. Макаренко С. И. Описательная модель сети связи специального назначения // Системы управления, связи и безопасности. 2017. № 2. С. 113-164. – URL: http://sccs.intelgr.com/archive/2017-02/05-Makarenko.pdf (дата обращения: 10.04.2019).

20. Макаренко С. И., Чаленко Н. Н., Крылов А. Г. Сети следующего поколения NGN // Системы управления, связи и безопасности. 2016. № 1. С. 81-102. – URL: http://sccs.intelgr.com/archive/2016-01/05-Makarenko.pdf (дата обращения 07.04.2019).

21. Лялюк И. Н. C4I: системы связи, АСУ и разведки вооруженных сил США. – М.: ВАТУ, 2000.

22. Будко П. А., Рисман О. В. Многоуровневый синтез информационно-телекоммуникационых систем. Математические модели и методы оптимизации: Монография. – СПб.: ВАС, 2011. – 476 с.

23. Будко П. А. Управление ресурсами информационно-телекоммуникационных систем. Методы оптимизации. – СПб.: ВАС, 2012. – 512 с.

24. Будко П. А., Чихачев А. В., Баринов М. А., Виноградeнко А. М. Принципы организации и планирования сильносвязной телекоммуникационной среды сил специального назначения // T-Comm: Телекоммуникации и транспорт. 2013. Т. 7. № 6. С. 8-12.

25. Будко П. А., Чихачев А. В., Баринов М. А., Виноградeнко А. М. Основные направления организации и планирования телекоммуникационной

среды сил специального назначения // Наукоемкие технологии в космических исследованиях Земли. 2013. Т. 5. № 4. С. 18-23.

26. Линец Г. И. Системные аспекты теории синтеза и практика построения телекоммуникационных сетей. – Ставрополь: Альфа-Принт, 2010. – 460 с.

27. Назаров А. Н., Сычев К. И. Модели и методы расчета показателей качества функционирования узлового оборудования и структурно-сетевых параметров сетей связи следующего поколения. – Красноярск: Изд-во ООО «Поликом», 2010. – 389 с.

28. Давыдов А. Е., Хейстонен Д. П. Построение модели системы управления телекоммуникационной сетью специального назначения // Вопросы радиоэлектроники. 2012. Т. 3. № 2. С. 124-130.

29. Давыдов А. Е. Концептуальные подходы к построению адаптивных мультисервисных сетей специального назначения // НИИ Масштаб [Электронный ресурс]. 10.12.2012. – URL: http://mashtab.org/company/massmedia/articles/konceptualnye_podhody_k_postroeniyu_adaptivnyh_multiservisnyh_setej_specialnogo_naznacheniya/ (дата обращения 08.06.2017).

30. Сухотеплый А. П., Давыдов А. Е., Савицкий О. К., Лукьянчик В. Н. К вопросу создания стационарной компоненты наземного эшелона ОАЦСС ВС РФ на территории РФ и сопредельных государств в условиях сетецентрических войн // НИИ Масштаб [Электронный ресурс]. 10.12.2012. – URL: http://mashtab.org/company/massmedia/articles/k_voprosu_sozdaniya_stacionarnoj_komponenty_nazemnogo_eshelona_oacss_vs_rf_na_territorii_rf_i_sopredelnyh_gosudarstv_v_usloviyah/ (дата обращения 08.06.2017).

31. Давыдов А. Е. Концептуальные подходы к построению автоматизированной системы управления связью адаптивных мультисервисных сетей специального назначения // НИИ Масштаб [Электронный ресурс]. 12.11.2012. – URL: http://mashtab.org/company/massmedia/articles/conceptual_approaches_to_constructing_an_automated_control_system_for_adaptive_multi-service_special-purpose_networks/ (дата обращения 08.06.2017).

32. Ермишян А. Г. Теоретические основы построения систем военной связи в объединениях и соединениях. Часть 1. Методологические основы построения организационно-технических систем военной связи. – СПб.: ВАС, 2005. – 740 с.

33. Ермишян А. Г., Сызранцев Г. В., Дыков В. В. Теоретические и научно-практические основы построения систем связи в локальных войнах и вооруженных конфликтах / под ред. А.Г. Ермишяна. – СПб.: ВАС, 2006. – 220 с.

34. Сызранцев Г. В. Теоретические и научно-методические основы обеспечения построения сложных организационно-технических систем военной связи в локальных войнах и вооружённых конфликтах. Монография. – СПб.: ВАС, 2007. – 180 с.

35. Иванов В. Г. Модель технической основы системы управления специального назначения в едином информационном пространстве на основе конвергентной инфраструктуры системы связи. Монография. – СПб.: Политех-пресс, 2018. – 214 с.

36. Легков К. Е. Многоуровневые модели инфокоммуникационных сетей специального назначения // T-Comm: Телекоммуникации и транспорт. 2015. Том 9. № 12. С. 32-36.

37. Легков К. Е. Организация и модели функционирования современных инфокоммуникационных сетей специального назначения // T-Comm: Телекоммуникации и транспорт. 2015. Т. 9. № 8. С. 14-20.

38. Легков К. Е., Мясникова А. И. Управление инфокоммуникационными услугами в мультисервисных сетях специального назначения // Наукоемкие технологии в космических исследованиях Земли. 2012. № 3. С. 20-22.

39. Легков К. Е., Емельянов А. В. Концепция управления сетями в модели взаимодействия открытых систем // Труды Ростовского государственного университета путей сообщения. 2015. № 3. С. 83-92.

40. Буренин А. Н., Легков К. Е. Особенности архитектур, функционирования, мониторинга и управления полевыми компонентами современных инфокоммуникационных сетей специального назначения // Наукоемкие технологии в космических исследованиях Земли. 2013. № 3. С. 12-17.

41. Буренин А. Н., Легков К. Е. Современные инфокоммуникационные системы и сети специального назначения. Основы построения управления. – М.: Медиа паблишер, 2015. – 348 с.

42. Буренин А. Н., Легков К. Е. Вопросы безопасности инфокоммуникационных систем и сетей специального назначения: основные угрозы, способы и средства обеспечения комплексной безопасности сетей // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 3. С. 46-61.

43. Исаков Е. Е. Устойчивость военной связи в условиях информационного противоборства. – СПб.: Изд-во Политехнического университета, 2009. – 400 с.

44. Михайлов Р. Л. Помехозащищенность транспортных сетей связи специального назначения. Монография. – Череповец: ЧВВИУРЭ, 2016. – 128 с.

45. Будко П. А., Линец Г. И., Мухин А. В., Фомин Л. А. Эффективность, цена и качество информационно-телекоммуникационных систем. Методы оптимизации. – Ставрополь: Аргус, 2011. – 512 с.

46. Шнепс-Шнеппе М. А. «Красный телефон» на DISN сети как родимое пятно в среде AS-SIP // International Journal of Open Information Technologies. 2015. Т. 3. № 6. С. 7-12.

47. Шнепс-Шнеппе М. А., Намиот Д. Е. Об эволюции телекоммуникационных сервисов на примере GIG // International Journal of Open Information Technologies. 2015. Т. 3. № 1. С. 1-13.

48. Шнепс-Шнеппе М. А. От IN к IMS. О сетях связи военного назначения // International Journal of Open Information Technologies. 2014. Т. 2. № 1. С. 1-11.

49. Шнепс-Шнеппе М. А., Намиот Д. Е, Цикунов Ю. В. Телекоммуникации для военных нужд: сеть GIG-3 по требованиям кибервойны // International Journal of Open Information Technologies. 2014. Т. 2. № 10. С. 3-13.

50. Шнепс-Шнеппе М. А. Телекоммуникации Пентагона: цифровая трансформация и киберзащита. – М.: Горячая линия – Телеком, 2017. – 272 с.

51. Соколов Н. А. Системные аспекты построения и развития сетей электросвязи специального назначения // International Journal of Open Information Technologies. 2014. Т. 2. № 9. С. 4-8.

52. Гольдштейн Б. С., Соколов Н. А. Потенциальные угрозы для сетей специального назначения // Вестник связи. 2015. № 1. С. 28-31.

53. Гольдштейн Б. С., Пинчук А. В., Соколов Н. А. Минимизация рисков устойчивости функционирования современных ССН // Вестник связи. 2015. № 6. С. 49-51.

54. Паращук И. Б., Бородакий Ю. В., Боговик А. В., Курносов В. И., Лободинский Ю. Г., Масановец В. В. Основы теории управления с системах специального назначения. – М.: УД Президента РФ, 2005. – 400 с.

55. Нетес В. А. Надежность сетей связи в период перехода к NGN // Вестник связи. 2007. № 9. С. 1-8.

56. Информационные технологии, связь и защита информации в МВД России – 2012 / Под ред. М.Л. Тюркина, М.И. Шадаева, А.С. Аджемова, И.П. Иванова, С.В. Дворянкина, А.В. Куц, А.В. Квитко, П.А. Важева, Ю.А. Быстрова. – М.: ООО «Компания «Информационный мост», 2013. – 156 с. – URL: www.informost.ru (дата обращения 03.02.2015).

57. Связь в Вооруженных силах Российской Федерации – 2013: тематический сборник. / Под ред. А.В. Абрамовича, А.В. Герасимова, С.В. Цибина, К.С. Ометова, Ю.А. Быстрова. – М.: ООО «Компания «Информационный мост», 2013. – 216 с. – URL: www.informost.ru (дата обращения 03.02.2015).

58. Оружие и технологии России. Энциклопедия. XXI век. Системы управления, связи и радиоэлектронной борьбы / Под общ. ред. С. Иванова. – М.: Изд. дом «Оружие и технологии», 2006. – 695 с.

59. О связи. Федеральный закон РФ от 07.07.2003 № 126-ФЗ // Собрание законодательства Российской Федерации от 14 июля 2003 г. № 28 ст. 2895.

60. Об информации, информационных технологиях и о защите информации. Федеральный закон от 27.07.2006 № 149-ФЗ // Собрание законодательства РФ, 31.07.2006, № 31 (1 ч.), ст. 3448.

61. Паращук И. Б., Одоевский С. М., Салюк Д. В., Рашич В. О., Боговик А. В., Скоропад А. В., Нестеренко А. Г. Новые информационные и сетевые технологии в системах управления военного назначения. Учебник.

Часть 1. Новые сетевые технологии в системах управления военного назначения / под ред. С.М. Одоевского. – СПб.: ВАС, 2010. – 432 с.

62. Макаренко С. И., Федосеев В. Е. Системы многоканальной связи. Вторичные сети и сети абонентского доступа: учебное пособие. – СПб.: ВКА имени А.Ф. Можайского, 2014. – 179 с.

63. Попков В. К., Блукке В. П., Дворкин А. Б. Модели анализа устойчивости и живучести информационных сетей // Проблемы информатики. 2009. № 4. С. 63-78.

64. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью. Национальный стандарт РФ. – М., 2007.

65. Рекомендации по стандартизации Р 50.1.053-2005. Информационные технологии. Основные термины и определения в области технической защиты информации. – М., 2006.

66. ГОСТ Р 53111-2008. Устойчивость функционирования сети связи общего пользования. Требования и методы проверки. – М., 2008.

67. Кобозев Ю. Н Перспективы развития систем связи и телекоммуникаций в информационно-управляющих системах специального назначения [Доклад] // Мат. Всероссийской научной конференции «Современные тенденции развития теории и практики управления в системах специального назначения». Том 4 «Телекоммуникации и связь в информационно-управляющих системах». Под ред. Ю.В. Бородакия. М.: ОАО «Концерн «Системпром», 2013. С. 7-9.

68. Шептура В. Н. Архитектура перспективной системы связи группировки войск (сил) для обеспечения управления адаптивными действиями войск (сил) [Доклад] // Мат. Всероссийской научной конференции «Современные тенденции развития теории и практики управления в системах специального назначения». Том 4 «Телекоммуникации и связь в информационно-управляющих системах». Под ред. Ю.В. Бородакия. – М.: ОАО «Концерн «Системпром», 2013. – С. 16-20.

69. Коробицин А. А., Кудрявцев А. М., Смирнов А. А. Информационные и сетевые технологии в автоматизированных системах специального назначения: Учебное пособие. – СПб.: ВАС, 2015. – 132 с.

70. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы. Учебник для вузов. 4-е изд. – СПб.: Питер, 2010. – 945 с.

71. Гордиенко В. Н., Тверецкий М. С. Многоканальные телекоммуникационные системы: учебник – М.: Горячая линия - Телеком, 2013. – 397 с.

72. Крухмалев В. В., Гордиенко В. Н., Моченов А. Д., Иванов В. И., Бурдин В. А., Крыжановский А. В., Марыкова Л. А. Основы построения телекоммуникационных систем и сетей / Под ред. В.Н. Гордиенко и В.В. Крухмалева. – М.: Горячая линия - Телеком, 2004. – 510 с.

73. Соколов Н. А. Телекоммуниционные сети. Монография в 4-х частях. – М.: Альварес Паблишинг, 2003, 2004.

74. Кучерявый Е. А. Управление трафиком и качество обслуживания в сети Интернет. – СПб.: Наука и техника, 2004. – 336 с.

75. Агеев С. А., Саенко И. Б. Управление безопасностью защищенных мультисервисных сетей специального назначения // Труды СПИИРАН. 2010. № 2 (13). С. 182-198.

76. Боговик А. В., Игнатов В. В. Теория управления в системах военного назначения. – СПб.: ВАС, 2008. – 460 с.

77. Norros I. A broad approach to the dependability of IP networks // European CUP Newsletter. 2006. Vol. 2. № 3.

78. Next Generation Networks Task Force Report // The President's National Security Telecommunications Advisory Committee. 2006.

79. ITU-T Recommendation G.1000 (11/2001). Communications Quality of Service: A framework and definitions. 2001.

80. Кархов А. SDH не умрет, но уже никогда не будет приоритетом. Интервью с директором по перспективному развитию сети Comstar United Telesystems // Connect! Мир связи. 2006. № 6. – URL: http://www.connect.ru/article.asp?id=4943 (дата обращения 09.06.2017).

81. Гольдштейн Б. С. 10 лет эволюции коммутационной техники // Вестник связи. 2007. № 5. С. 1-6.

82. Макаренко С. И., Афанасьев О. В., Баранов И. А., Самофалов Д. В. Экспериментальные исследования реакции сети связи и эффектов перемаршрутизации информационных потоков в условиях динамического изменения сигнально-помеховой обстановки // Журнал радиоэлектроники. 2016. № 4. – URL: http://jre.cplire.ru/jre/apr16/4/text.pdf (дата обращения 09.04.2019).

83. Волков В. Ф., Груздев Н. В., Колдунов А. И., Шилин М. П. Управление высокоточным оружием: учебное пособие. – СПб.: ВКА имени А.Ф. Можайского, 2006. – 96 с.

84. Щербинин Р. Перспективные боевые части высокоточного оружия США // Зарубежное военное обозрение. 2010. № 4. С. 58-63.

85. Дьяков А. С. «Быстрый глобальный удар» в планах развития стратегических сил США. Доклад центра по изучению проблем разоружения, энергетики и экологии при МФТИ. – М.: МФТИ, 2007.

86. Усачев В. А., Голов Н. А., Кудрявцев Н. В. Перспективные технические решения и тенденции развития радиоэлектронных систем наведения для высокоточного оружия класса «воздух-поверхность» // Наука и образование. 2011. № 10. С. 1-5.

87. Куприянов А. И., Шустов Л. Н. Радиоэлектронная борьба. Основы теории. – М.: Вузовская книга, 2011. – 800 с.

88. Семенов С. С., Чихачев А. В., Гусев А. П., Дорошенко Г. П. Перспективы развития вооружения, военной и специальной техники. Учебное пособие. – СПб.: ВАС, 2016. – 154 с.

89. Михайлов Р. Л. Радиоэлектронная борьба в вооруженных силах США: Военно-теоретический труд. – СПб.: Наукоемкие технологии, 2018. – 131 с.

90. Леньшин А. В. Бортовые системы и комплексы радиоэлектронного подавления. – Воронеж: Научная книга, 2014. – 590 с.

91. Перунов Ю. М., Мацукевич В. В., Васильев А. А. Зарубежные радиоэлектронные средства / Под ред. Ю.М. Перунова. В 4-х книгах. Кн. 2: Системы радиоэлектронной борьбы. – М.: Радиотехника, 2010. – 352 с.

92. Макаренко С. И., Иванов М. С., Попов С. А. Помехозащищенность систем связи с псевдослучайной перестройкой рабочей частоты. Монография. – СПб.: Свое издательство, 2013. – 166 с.

93. Добыкин В. Д., Куприянов А. И., Пономарев В. Г., Шустов Л. Н. Радиоэлектронная борьба. Силовое поражение радиоэлектронных систем / Под ред. А.И. Куприянова. – М.: Вузовская книга, 2007. – 468 с.

94. Радзиевский В. Г., Сирота А. А. Теоретические основы радиоэлектронной разведки. – М.. Радиотехника, 2004 – 432 с.

95. Буренок В. М., Ляпунов В. М., Мудров В. И. Теория и практика планирования и управления развитием вооружения / Под ред. А.М. Московского. – М.: Изд-во «Вооружение. Политика. Конверсия», 2005. – 418 с.

96. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. – М.: Стандартинформ, 2007. – 11 с.

97. Куприянов А. И., Сахаров А. В., Шевцов В. А. Основы защиты информации: учебное пособие. – М.: Издательский центр «Академия», 2006. – 256 с.

98. Дождиков В. Г., Салтан М. И. Краткий энциклопедический словарь по информационной безопасности. – М.: ИАЦ Энергия, 2010. – 240 с.

99. Виноградов А. А. Функциональность, надежность, киберустойчивость в системах автоматизации критических инфраструктур [Доклад] // Конференция «Региональная информатика-2012». – СПб.: ОАО «НПО «Импульс», 2012.

100. Сухоруков С. А. Защита компьютеризированных систем критических объектов от кибернетических атак с помощью преднамеренных маломощных импульсных электромагнитных воздействий // Технологии ЭМС. 2011. № 4 (39). С. 53-67.

101. Сухоруков С. А., Горячевский В. В. Исследование функционирования СВТИ при испытаниях на устойчивость к намеренному силовому воздействию методами электромагнитного терроризма. Часть 1. Однократные наносекундные импульсы электромагнитного поля // Технологии ЭМС. 2008. № 1. С. 3-11.

102. Сухоруков С. А. Исследование функционирования СВТИ при испытаниях на устойчивость к намеренному силовому воздействию методами электромагнитного терроризма. Часть 2. Устойчивость СВТИ к однократным наносекундным импульсам электромагнитного поля // Технологии ЭМС. 2008. № 1. С. 12-15.

103. Сухоруков С. А., Горячевский В. В. Исследование функционирования СВТИ при испытаниях на устойчивость к намеренному силовому воздействию методами электромагнитного терроризма. Часть 3. Низковольтные однократные миллисекундные импульсы напряжения. Степень жесткости испытаний I // Технологии ЭМС. 2009. № 3. С. 7-17.

104. Сухоруков С. А. Исследование функционирования СВТИ на устойчивость к преднамеренным силовым электромагнитным воздействиям. Часть 4. Высоковольтные однократные наносекундные импульсы напряжения. Степень жесткости испытаний I // Технологии ЭМС. 2011. № 3 (38). С. 36-45.

105. ГОСТ Р 52863-2007. Защита информации. Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования. – М.: Изд-во стандартов, 2008. – 33 с.

106. Сухоруков С. А. Электромагнитная совместимость: сверхмощные электромагнитные воздействия. – Тула: Гриф и К, 2013. – 441 с.

107. Электромагнитный терроризм на рубеже тысячелетий / Под ред. Т.Р. Газизова. – Томск: Томский государственный университет, 2002. – 206 с.

108. Газизов Т. Р. Искажения в межсоединениях и электромагнитный терроризм. Моделирование и решение проблем. – Saarbrucken: Lambert Academic Publisshing, 2011. – 368 с.

109. Акбашев Б. Б., Балюк Н. В., Кечиев Л. Н. Защита объектов телекоммуникаций от электромагнитных воздействий. – М.: Грифон, 2014. – 472 с.

110. Киричек Р. В. Исследование влияния сверхкоротких электромагнитных импульсов на процесс передачи данных в сетях Ethernet / Киричек Руслан Валентинович. Дис. … канд. техн. наук по спец.: 05.12.13. – СПб.: СПбГУТ им. проф. М.А. Бонч-Бруевича, 2011. – 142 с.

111. Жабина А. В. Разработка методов повышения эффективности функционирования телекоммуникационных систем при внешних импульсных электромагнитных воздействиях / Жабина Анна Валерьевна. Дис. … канд. техн. наук по спец.: 05.12.13. – Омск, 2009. – 137 с.

112. Михеев О. В. Средства измерений и методы испытаний телекоммуникационных систем в условиях воздействия электромагнитных импульсов с субнаносекундной длительностью фронта / Михеев, Олег Викторович. Дис. … канд. техн. наук по спец.: 05.12.13. – М., 2006. – 167 с.

113. Сидоров А. В. Оценка устойчивости средств радиосвязи и управления органов внутренних дел к деструктивным электромагнитным воздействиям / Сидоров Александр Викторович. Дис. … канд. техн. наук по спец.: 05.12.04. – Воронеж, 2015. – 149 с.

114. Гизатуллин З. М. Помехоустойчивость средств вычислительной техники внутри зданий при широкополосных электромагнитных воздействиях: Монография. – Казань: Изд-во Казанского государственного технического университета, 2012. – 254 с.

115. Михайлов В. А. Разработка методов и моделей анализа и оценки устойчивого функционирования бортовых цифровых вычислительных комплексов в условиях преднамеренного воздействия сверхкоротких электромагнитных излучений / Михайлов Виктор Алексеевич. Дис. … докт. техн. наук по спец.: 05.12.13. – М.: НИИ «Аргон», 2014. – 390 с.

116. Фомина И. А. Метод тестирования устойчивости телекоммуникационной системы управления беспилотных летательных аппаратов к воздействию сверхкоротких электромагнитных импульсов / Фомина Ирина Андреевна. Дис. … канд. техн. наук по спец.: 05.12.13. – М., 2015. – 139 с.

117. Меньшаков Ю. К. Теоретические основы технических разведок: учеб. пособие / Под ред. Ю.Н. Лаврухина. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2008. – 536 с.

118. Хорошко В. А., Чекатков А. А. Методы и средства защиты информации. — К.: Юниор, 2003. — 504 с.

119. Емельянов С. Л. Техническая разведка и технические каналы утечки информации // Системи обробки інформації. 2010. № 3 (84). С. 20-23.

120. Чукляев И. И., Морозов А. В., Болотин И. Б. Теоретические основы оптимального построения адаптивных систем комплексной защиты информационных ресурсов распределенных вычислительных систем: монография. – Смоленск: ВА ВПВО ВС РФ, 2011. – 227 с.

121. Пиунов О., Щербинин Р. Американский стратегический разведывательный самолёт RC-135 и его модификации // Зарубежное военное обозрение. 2012. № 3. С.70-76.

122. Максименко А. Американистике системы радиоэлектронной разведки // Зарубежное военное обозрение. 2004. № 9. С.45-49.

123. Варламов О. О. О системном подходе к созданию модели компьютерных угроз и ее роли в обеспечении безопасности информации в ключевых системах информационной инфраструктуры // Известия ЮФУ. Технические науки. 2006. № 7 (62). С. 216-223.

124. Пахомова А. С., Пахомов А. П., Юрасов В. Г. Об использовании классификации известных компьютерных атак в интересах разработки структурной модели угрозы компьютерной разведки // Информация и безопасность. 2013. Т. 16. № 1. С. 81-86.

125. Barnum S. Common Attack Pattern Enumeration and Classification (CAPEC) Schema Description. Version 1.3. Cigital Inc. 2008. – URL: https://capec.mitre.org/documents/documentation/CAPEC_Schema_Description_v1.3.pdf (дата обращения 09.04.2019).

126. Ларина Е. С., Овчинский В. С. Кибервойны XXI века. О чем умолчал Эдвард Сноуден. – М.: Книжный мир, 2014. – 352 с.

127. Ададуров С. Е., Чатоян С. К., Зелинский А. Е. Показатели устойчивости информационного обмена в защищенных телекоммуникационных системах // Проблемы информационной безопасности. Компьютерные системы. 1999. № 2. С. 100-107.

128. Громов Ю. Ю., Драчев В.О., Набатов К. А., Иванова О.Г. Синтез и анализ живучести сетевых систем: монография. – М.: «Издательство Машиностроение-1», 2007. – 152 с.

129. Попков В. К. Математические модели связности. Монография. – Новосибирск: ИВМиМГ СО РАН, 2006. – 490 с.

130. Пасечников И. И. Методология анализа и синтеза предельно нагруженных информационных сетей. Монография. – М.: «Издательство Машиностроение-1», 2004. – 216 с.

131. Егунов М. М., Шувалов В. П. Анализ структурной надежности транспортной сети // Вестник СибГУТИ. 2012. № 1. С. 54-60.

132. Грызунов В. В. Оценивание живучести неоднородных структур // Вестник СибГУТИ. 2011. № 1. С. 28-36.

133. Ковальков Д. А. Математические модели оценки надежности мультисервисного узла доступа // Радиотехнические и телекоммуникационные системы. 2011. № 2. С. 64-71.

134. Корячко В. П., Перепелкин Д. А. Анализ и проектирование маршрутов передачи данных в корпоративных сетях. – М.: Горячая линия – Телеком, 2012. – 236 с.

135. Корячко В. П., Перепелкин Д.А. Корпоративные сети: технологии, протоколы, алгоритмы. – М.: Горячая линия – Телеком, 2011. – 216 с.

136. Перепелкин Д. А. Алгоритм адаптивной ускоренной маршрутизации на базе протокола OSPF при динамическом добавлении элементов корпоративной сети // Вестник Рязанского государственного радиотехнического университета. 2010. № 34. С. 65-71.

137. Перепелкин Д. А. Алгоритм парных перестановок маршрутов на базе протокола OSPF при динамическом подключении узлов и линий связи корпоративной сети // Вестник Рязанского государственного радиотехнического университета. 2013. № 4-1 (46). С. 67-75.

138. Перепелкин Д. А. Алгоритм парных перестановок маршрутов на базе протокола OSPF при динамическом отказе узлов и линий связи корпоративной сети // Вестник Рязанского государственного радиотехнического университета. 2014. № 47. С. 84-91.

139. Перепелкин Д. А. Алгоритм адаптивной ускоренной маршрутизации на базе протокола OSPF при динамическом отказе элементов корпоративной сети // Вестник Рязанского государственного радиотехнического университета. 2011. № 37. С. 53-58.

140. Перепелкин Д. А., Перепелкин А. И. Повышение качества функционирования корпоративных сетей на базе протокола OSPF // Качество. Инновации. Образование. 2010. № 12 (67). С. 51-56.

141. Перепелкин Д. А. Алгоритм адаптивной ускоренной маршрутизации при динамическом отказе элементов корпоративной сети // Известия Тульского государственного университета. Технические науки. 2011. № 5-3. С. 262-269.

142. Перепелкин Д. А. Повышение качества функционирования корпоративных сетей на базе протокола EIGRP // Качество. Инновации. Образование. 2012. № 5 (84). С. 99-106.

143. Перепелкин Д. А., Перепелкин А. И. Алгоритм парных перестановок маршрутов на базе протокола IGRP в корпоративных сетях // Вестник Воронежского государственного технического университета. 2010. Т. 6. № 12. С. 39-43.

144. Перепелкин Д. А. Алгоритм адаптивной ускоренной маршрутизации на базе протокола IGRP при динамическом отказе узлов и линий связи корпоративной сети // Вестник Рязанского государственного радиотехнического университета. 2012. № 42-1. С. 33-38.

145. Перепелкин Д. А., Цыганов И. Ю. Алгоритм парных переходов в компьютерных сетях на основе метода маршрутизации по подсетям // Вестник Рязанского государственного радиотехнического университета. 2016. № 57. С. 56-62.

146. Перепелкин Д. А., Цыганов И. Ю. Применение алгоритма парных переходов для решения задачи адаптивной шлюзовой маршрутизации в корпоративных сетях с несколькими зонами конфигурирования трафика // Проблемы передачи и обработки информации в сетях и системах телекоммуникаций. Материалы 18-й Международной научно-технической конференции. 2015. С. 188-190.

147. Перепелкин Д. А., Цыганов И. Ю. Система моделирования быстрой перемаршрутизации трафика территориально-распределенных корпоративных сетей с несколькими зонами конфигурирования // Новые информационные технологии в научных исследованиях. Материалы XX Юбилейной Всероссийской научно-технической конференции студентов, молодых ученых и специалистов. – Рязань: Рязанский государственный радиотехнический университет, 2015. – С. 125-126.

148. Ануфренко А. В., Волков Д. В., Канаев А. К. Механизмы обеспечения отказоустойчивости пакетно-ориентированных сетей связи // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сборник научных статей в 2 томах. 2015. С. 198-202.

149. Логин Э. В., Канаев А. К. Модель транспортной сети связи как составляющая мультиагентной системы управления // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. № 2. С. 34-42.

150. Канаев А. К., Бенета Э. В. Сценарий управления неисправностями в сетях с технологией Carrier Ethernet с помощью механизмов OAM // 72-я Всероссийская научно-техническая конференция, посвященная Дню радио. Труды конференции. 2017. С. 243-244.

151. Бенета Э. В., Канаев А. К. Формирование алгоритма управления отказами в телекоммуникационной сети связи, построенной по технологии Carrier Ethernet // Информационные технологии на транспорте. Сборник

материалов юбилейной XV Санкт-Петербургской международной конференции «Региональная информатика – 2016». 2016. С. 95-101.

152. Канаев А. К., Привалов А. А., Сахарова М. А., Скуднева Е. В. Функционирование системы управления сетью передачи данных в условиях конечной надежности сетевого оборудования // Информационные технологии и телекоммуникации. 2015. № 3 (11). С. 6-16.

153. Ануфриенко А. В., Баранцев А. В., Канаев А. К. Обеспечение отказоустойчивости сетей связи, функционирующих на базе пакетно-ориентированных технологий // Юбилейная 70-я всероссийская научно-техническая конференция, посвященная Дню радио. 2015. С. 304-306.

154. Канаев А. К., Лукичев М. М. Анализ различных подходов к формированию ранжированных множеств маршрутов на транспортной сети связи // Юбилейная 70-я всероссийская научно-техническая конференция, посвященная Дню радио. 2015. С. 268-270.

156. Присяжнюк С. П., Мигалин В. Н., Овчинников Т. Р. Интегральные сети АСУВ. Системы коммутации пакетов. – Л.: ВИКИ им. А.Ф. Можайского, 1989. – 93 с.

157. Большаков А. А., Присяжнюк С. П. Понятие и основные свойства класса зондовых алгоритмов решения задач контроля и анализа ситуации в сети пакетной коммутации // Материалы международной научно-технической конференции. 1991. Ч. 2. С. 254-261.

158. Аванесов М. Ю., Присяжнюк С. П. Оперативное управление потоками данных в мультисервисных сетях связи. – СПб.: БГТУ «Военмех», 2007. – 80 с.

159. Поповский В. В., Волотка В. С. Методы анализа динамических структур телекоммуникационных систем // Восточно-Европейский журнал передовых технологий. 2013. № 5/2 (65). С. 18-22.

160. Поповский В. В., Волотка В. С. Математическое моделирование надежности инфокоммуникационных систем // Телекомунікаційні та інформаційні технології. 2014. № 3. С. 5-9.

161. Поповский В. В., Лемешко А. В., Мельникова Л. И. и др. Обзор и сравнительный анализ основных моделей и алгоритмов многопутевой маршрутизации в мультисервисных телекоммуникационных сетях // Прикладная радиоэлектроника. 2005. Т. 4. № 4. С. 372-382. – URL: http://alem.ucoz.ua/_ld/0/10_Lemeshko_PRE_20.pdf (дата обращения 01.04.2019).

162. Поповский В. В., Лемешко А. В., Евсеева О. Ю. Динамическое управление ресурсами ТКС: математические модели в пространстве состояний // Наукові записки УНДІЗ. 2009. № 1 (9). С. 3-26.

163. Лемешко А. В., Евсеева О. Ю., Дробот О. А. Методика выбора независимых путей с определением их количества при решении задач многопутевой маршрутизации // Праці УНДІРТ. 2006. № 4 (48). С. 69-73. – URL: http://alem.ucoz.ua/_ld/0/14_Lemeshko_UNIIRT.pdf (дата обращения 01.04.2019).

164. Лемешко А. В., Козлова Е. В., Романюк А. А. Математическая модель отказоустойчивой маршрутизации, представленная алгебраическим

уравнениями состояния MPLS-сети // Системи обробки інформації. 2013. № 2 (109). С. 217-220.

165. Михайлов Р. Л. Модели и алгоритмы маршрутизации в транспортной наземно-космической сети связи военного назначения // Системы управления, связи и безопасности. 2015. № 3. С. 52-82.

166. Михайлов Р. Л., Макаренко С. И. Оценка устойчивости сети связи в условиях воздействия на неё дестабилизирующих факторов // Радиотехнические и телекоммуникационные системы. 2013. № 4. С. 69-79.

167. Михайлов Р. Л., Владимиров Е. С. Методика обоснования показателя устойчивости связи // I-methods. 2015. Т. 7. № 3. С. 24-28.

168. Макаренко С. И., Рюмшин К. Ю., Михайлов Р. Л. Модель функционирования объекта сети связи в условиях ограниченной надежности каналов связи // Информационные системы и технологии. 2014. № 6 (86). С. 139-147

169. Макаренко С. И., Михайлов Р. Л. Адаптация параметров сигнализации в протоколе маршрутизации с установлением соединений при воздействии на сеть дестабилизирующих факторов // Системы управления, связи и безопасности. 2015. № 1. С. 98-126.

170. Goyal M., Soperi M., Baccelli E., Choudhury G., Shaikh A., Hosseini S. H., Trivedi K. Improving Convergence Speed and Scalability in OSPF: A Survey // IEEE Communications Surveys & Tutorials. 2012. № 14 (2). pp. 443-463.

171. Goyal M., Xie W., Hosseini S. H., Vairavan K., Rohm D. Improving OSPF Dynamics on a Broadcast LAN // Simulation. 2006. vol. 82. № 2. pp. 107-129.

172. Goyal M., Xie W., Soperi M., Hosseini S. H., Scheduling routing table calculations to achieve fast convergence in OSPF protocol // Proceedings IEEE BROADNETS 2007. 2007. pp. 863-872.

173. Goyal M., Ramakrishnan K. K., Feng W. Achieving Faster Failure Detection in OSPF Networks // Proceedings IEEE International Conference on Communications (ICC-2003). 2003. Vol. 1. pp. 296-300.

174. Amir S., Biswajit N. Improving Network Convergence Time and Network Stability of an OSPF-Routed IP Network // Lecture Notes in Computer Science. 2005. Vol. 3462. pp. 469-485.

175. Basu A., Riecke J. Stability issues in OSPF routing // ACM SIGCOMM Computer Communication Review. 2001. Vol. 31. № 4. pp. 225-236.

176. Pu J., Manning E., Shoja G. C. Routing Reliability Analysis of Partially Disjoint Paths // Proc. IEEE Conference on Communications, Computers, and Signal Processing. Victoria, BC, Canada. 2001. Vol. 1. pp. 79-82.

177. Huang S., Kitayama K., Cugini F., Paolucci F., Giorgetti A., Valcarenghi L., Castoldi P. An Experimental Analysis on OSPF-TE Convergence Time // Asia Pacific Optical Communications – International Society for Optics and Photonics. 2008. Vol. 7137.

178. Pun H. Convergence Behavior of RIP and OSPF Network Protocols. Ph.D. thesis. – University of British Columbia. 2001. – 59 p.

179. Ayari N., Barbaron D., Lefevre L., Primet P. Fault tolerance for highly available internet services: concepts, approaches, and issues // IEEE Communication Surveys and Tutorials. 2008. vol. 10. № 2. pp. 34-46.

180. Dilber M. N., Raza A. Analysis of successive Link Failures effect on RIP and OSPF Convergence time delay // International Journal of Advances in Science and Technology. 2014. pp. 42-48.

181. Zhao D., Hu X., Wu C. A Study on the Impact of Multiple Failures on OSPF Convergence // International Journal of Hybrid Information Technology. 2013. vol. 6. № 3. pp. 75-74.

182. Sankar D., Lancaster D. Routing Protocol Convergence Comparison using Simulation and Real Equipment // Advances in Communications, Computing, Networks and Security. 2013. Vol. 10. pp. 186-194.

183. Labovitz C., Ahuja A., Bose A., Jahanian F. Delayed Internet Routing Convergence // IEEE/ACM Transactions on Networking (TON). 2001. Vol. 9. № 3. pp. 293-306.

184. Labovitz C. Ahuja A., Wattenhofer R., Venkatachary S. The impact of Internet policy and topology on delayed routing convergence // Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings (INFOCOM 2001). – IEEE, 2001. Vol. 1. pp. 537-546.

185. Tsegaye Y., Geberehana T. OSPF Convergence Times. Master of Science Thesis in the Programme Networks and Distributed Systems. – Göteborg: Chalmers University of Technology, 2012. – 77 p.

186. Fang W., Shanzhi C., Xin L., Yuhong L. A Route Flap Suppression Mechanism Based on Dynamic Timers in OSPF Network // The 9-th International Conference for Young Computer Scientists – IEEE, 2008.

187. Додонов А. Г., Ландэ Д. В. Живучесть информационных систем. – К.: Наук. думка, 2011. – 256 с.

188. Свами М., Тхуласираман К. Графы, сети и алгоритмы. – М.: Мир, 1984. – 454 с.

189. Перунов Ю. М., Куприянов А. И. Радиоэлектронная борьба: радиотехническая разведка. – М.: Вузовская книга, 2017. – 190 с.

190. Борисов В. И., Зинчук В. М., Лимарев А. Е., Немчилов А. В., Чаплыгин А. А. Пространственные и вероятностно-временные характеристики эффективности станций ответных помех при подавлении систем радиосвязи / Под ред. В.И. Борисова. – Воронеж: ОАО «Концерн «Созвездие», 2007. – 354 с.

191. Борисов В. И., Зинчук В. М., Лимарев А. Е., Мухин Н. П., Шестопалов В. И. Помехозащищенность систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты. – М.: Радио и связь, 2000. – 384 с.

192. Макаренко С. И., Михайлов Р. Л. Информационные конфликты – анализ работ и методологии исследования // Системы управления, связи и безопасности. 2016. № 3. С. 95-178.

193. Стародубцев Ю. И., Бухарин В. В., Семенов С. С. Техносферная война // Военная мысль. 2012. № 7. С. 22-31.

194. Стародубцев Ю. И., Бухарин В. В., Семенов С. С. Техносферная война // Информационные системы и технологии. 2011. № 1. С. 80-85.

195. Стародубцев Ю. И., Семенов С. С., Бухарин В. В. Техносферная война // Научно-информационный журнал Армия и общество. 2010. № 4. С. 6-11.

196. Владимиров В. И., Докторов А. Л., Елизаров Ф. В. и др. Электромагнитная совместимость радиоэлектронных средств и систем / Под ред. Н.М. Царькова. – М.: Радио и связь, 1985. – 272 с.

197. Дружинин В. В., Конторов А. С., Конторов Д. С. Введение в теорию конфликта. – М.: Радио и связь, 1989. – 288 с.

198. Михайлов Р. Л., Ларичев А. В., Смыслова А. Л., Леонов П. Г. Модель распределения ресурсов в информационном конфликте организационно-технических систем // Вестник Череповецкого государственного университета. 2016. № 6 (75). С. 24-29.

199. Михайлов Р. Л. Анализ подходов к формализации показателя информационного превосходства на основе теории оценки и управления рисками // Системы управления, связи и безопасности. 2017. № 3. С. 98-118.

200. Антонович П. И., Шаравов И. В., Лойко В. В. Сущность операций в кибернетическом пространстве и их роль в достижении информационного превосходства // Вестник академии военных наук. 2012. № 1 (38). С. 41-45.

201. Стюгин М. А. Методика достижения информационного превосходства в конфликтных системах // Информационные войны. 2013. № 3 (27). С. 17-21.

202. Гапенко О. Ю. Защита информации: основы организационного управления. – СПб.: Дом «Сентябрь», 2001. – 228 с.

203. Захарченко Р. И., Королев И. Д., Саенко И. Б. Синергетический подход к обеспечению устойчивости функционирования автоматизированных систем специального назначения // Системы управления, связи и безопасности. 2018. № 4. С. 207-225.

204. Радзиевский В. Г., Сирота А. А. Информационное обеспечение радиоэлектронных систем в условиях конфликта. – М.: ИПРЖР, 2001. – 456 с.

205. Михайлов Р. Л. Модель динамической координации подсистем наблюдения и воздействия в информационном конфликте в виде иерархической дифференциальной игры трех лиц // Наукоемкие технологии. 2018. Т. 19. № 10. С. 44-51.

206. Михайлов Р. Л. Двухуровневая модель координации подсистем радиоэлектронного мониторинга и радиоэлектронной борьбы // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. № 2. С. 43-50.

207. Михайлов Р. Л., Поляков С. Л. Модель оптимального распределения ресурсов и исследование стратегий действий сторон в ходе информационного конфликта // Системы управления, связи и безопасности. 2018. № 4. С. 323-344.

208. Михайлов Р. Л., Шишков А. И. Принципы координации подсистем наблюдения и воздействия // Научная мысль. 2017. Т. 1. № 3 (25). С. 38-43.

209. Михайлов Р. Л. Анализ научно-методического аппарата теории координации и его использования в различных областях исследований // Системы управления, связи и безопасности. 2016. № 4. С. 1-30.

210. Семенов С. С., Гусев А. П., Барботько Н. В. Оценка информационно-боевого потенциала сторон в техносферных конфликтах // Наукоемкие технологии в космических исследованиях Земли. 2013. Т. 5. № 6. С. 10-21.

211. Стародубцев Ю. И., Бречко А. А. Моделирование сетей связи, функционирующих в условиях деструктивных программных воздействий // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2019. № 1-2 (127-128). С. 21-28.

212. Стародубцев Ю. И., Чукариков А. Г., Корсунский А. С., Сухорукова Е. В. Принципы безопасного использования инфраструктуры связи применительно к условиям техносферной войны // Интегрированные системы управления: сборник научных трудов научно-технической конференции. – Ульяновск: НПО «Марс», 2016. – С. 199-206.

213. Гуревич И. М. Многоуровневая модель сети связи // Вопросы кибернетики. Протоколы и методы коммутации в вычислительных сетях. 1986. С. 72-88.

214. Абраменков А. Н., Петухова Н. В., Фархадов М. П., Фрисов А. В., Гуревич И. М. Многоуровневые модели сетевых систем и комплекс программ расчета их статических и динамических характеристик // XII Всероссийское совещание по проблемам управления ВСПУ-2014. – М., 2014. – С. 7375-7386.

215. Гуревич И. М. Динамическая модель сети связи // Теория телетрафика в системах информатики. 1989. С. 77-86.

216. Гуревич И. М. Динамические свойства сетевых систем // Вопросы кибернетики. Архитектура и протоколы вычислительных сетей. 1990. С. 22-44.

217. Вакуленко А. А., Шевчук В. И. Математическая модель динамики конфликта радиоэлектронных систем // Радиотехника. 2011. № 1. С. 56-59.

218. Маевский Ю. И. Основные положения методологии синтеза многофункциональной конфликтно-устойчивой системы радиоэлектронной борьбы // Радиотехника. 2010. № 6. С. 61-66.

219. Поповский В. В., Лемешко А. В., Евсеева О. Ю. Математические модели телекоммуникационных систем. Часть 1. Математические модели функциональных свойств телекоммуникационных систем // Проблемы телекоммуникаций. 2011. № 2 (4). С. 3-41.

220. Калинин В. Н., Резников Б. А., Варакин Е. И. Теория систем и оптимального управления. Часть 1: Основные понятия, математические модели и методы анализа систем. – Л.: ВИКИ им. А.Ф. Можайского, 1979. – 319 с.

221. Калинин В. Н., Резников Б. А. Теория систем и управления (структурно-математический подход). – Л.: ВИКИ, 1987. – 417 с.

222. Дружинин В. В., Конторов Д. С. Вопросы военной системотехники. – М. Воениздат, 1976. – 224 с.

223. Рубинштейн М. И. Оптимальная группировка взаимосвязанных объектов. Монография. – М.: Наука, 1989. – 168 с.

224. Гурин Л. С., Дымарский Я. С., Меркулов А. Д. Задачи и методы оптимального распределения ресурсов. – М.: Сов. радио, 1968. – 463 с.

225. Кини Р. Л., Райфа Х. Принятие решений при многих критериях, предпочтения и замещения. Пер. с англ. / Под ред. И.Ф. Шахнова. – М.: Радио и связь, 1981. – 560 с.

226. Владимиров В. И. Информационные основы радиоподавления линий радиосвязи в динамике радиоэлектронного конфликта. – Воронеж: ВИРЭ, 2003. – 276 с.

227. Месарович М., Мако Д., Такахара И. Теория иерархических многоуровневых систем. – М.: Мир, 1973. – 344 с.

228. Угольницкий Г. А. Иерархическое управление устойчивым развитием. – М.: Издательство физико-математической литературы, 2010. – 336 с.

229. Усов А. Б. Борьба с коррупцией в динамических системах управления иерархической структуры // Известия Южного федерального университета. Технические науки. 2012. № 6 (131). С. 224-228.

230. Алферов А. Г., Толстых И. О., Толстых Н. Н., Поздышева О. В., Мордовин А. И. Усточивость инфокоммуникационных систем в условиях информационного конфликта // Информация и безопасность. 2014. Т. 17. № 4. С. 558-567.

231. Алферов А. Г., Власов Ю. Б., Толстых И. О., Толстых Н. Н., Челядинов Ю. В. Формализованное представление эволюционирующего информационного конфликта в телекоммуникационной системе // Радиотехника. 2012. № 8. С. 27-33.

232. Власов Ю.Б., Николаев В. И., Толстых И. О., Толстых Н. Н., Челядинов Ю. В. Оценка потенциальной опасности потоков данных в инфокоммуникационной системе // Радиотехника. 2012. № 8. С. 33-40.

233. Белицкий А. М., Степанец Ю. А., Толстых Н. Н. Перехват управления инфокоммуникационных систем // В сборнике: Радиолокация, навигация, связь XXI. Международная научно-техническая конференция. 2015. С. 1470-1475.

234. Иванкин М. П., Толстых Н. Н., Савинков А. Ю., Свердел В. Ф. Практические аспекты оценки эффективности функционирования систем программно-определяемого радио в условиях информационного конфликта // Теория и техника радиосвязи. 2019. № 1. С. 18-22.

235. Стюгин М.А. Постановка задачи дезинформации в информационных системах // Информационные войны. 2014. № 3 (31). С. 6-11.

236. Стюгин М. А. Методика достижения информационного превосходства в конфликтных системах // Информационные войны. 2013. № 3 (27). С. 17-21.

237. Стюгин М. А. Рефлексивно-сигнатурный анализ конфликта // Искусственный интеллект и принятие решений. 2012. № 2. С. 39-50.

238. Стюгин М. А. Планирование действий в конфликте на уровне функциональных структур // Информационные войны. 2009. № 2. С. 16-21.

238. Сирота А. А., Гончаров Н. И. исследование конфликта коалиций систем с использованием формализма гибридных автоматов // Вестник воронежского государственного университета. Серия: Системный анализ и информационные технологии. 2017. № 4. С. 56-70.

239. Сирота А. А., Гончаров Н. И. Модели информационных процессов несиметричного конфликтного взаимодействия систем и их применение в задачах исследования безопасности использования облачных технологий // Вестник воронежского государственного университета. Серия: Системный анализ и информационные технологии. 2018. № 3. С. 103-118..

240. Вялых А. С., Вялых С. А., Сирота А. А. Оценка уязвимости информационной системы на основе ситуационной модели динамики конфликта // Информационные технологии. 2012. № 9. С. 15-21.

241. Вялых А. С., Вялых С. А., Сирота А. А. Алгоритм анализа надежности программного обеспечения информационных систем в условиях внутренних уязвимостей и негативных воздействий // Фундаментальные проблемы системной безопасности: материалы V Международной научной конференции. – М.: Вычислительный центр им. А.А. Дородницына. 2014. – С. 158-163.

242. Кирсанов Э. А., Сирота А. А. Обработка информации в пространственно-распределенных системах радиомониторинга: статистический и нейросетевые подходы. – М.: Физико-математическая литература, 2012. – 344 с.

243. Бойко А. А., Храмов В. Ю. Модель информационного конфликта информационно-технических и специальных программных средств в вооруженном противоборстве группировок со статичными характеристиками // Радиотехника. 2013. № 7. С. 5-10.

244. Бойко А. А. Способ разработки тестовых удаленных информационно-технических воздействий на пространственно распределенные системы информационно-технических средств // Информационно-управляющие системы. 2014. № 3. С. 84-92.

245. Бойко А. А. Способ аналитического моделирования процесса распространения вирусов в компьютерных сетях различной структуры // Труды СПИИРАН. 2015. № 5 (42). С. 196-211.

246. Бойко А. А., Дегтярев И. С. Метод оценки весовых коэффициентов элементов организационно-технических систем // Системы управления, связи и безопасности. 2018. № 2. С. 245-266.

247. Бойко А. А. Способ оценки уровня информатизации образцов вооружения // Системы управления, связи и безопасности. 2019. № 1. С. 264-275.

248. Бойко А. А. Способ аналитического моделирования боевых действий // Системы управления, связи и безопасности. 2019. № 1. С. 264-275.

249. Бойко А. А., Дьякова А. В. Способ разработки тестовых удаленных информационно-технических воздействий на пространственно-распределенные

системы информационно-технических средств // Информационно-управляющие системы. 2014. № 3 (70). С. 84-92.

250. Бойко А. А., Будников С. А. Модель информационного конфликта специального программного средства и подсистемы защиты информации информационно технического средства // Радиотехника. 2015. № 4. С. 136-141.

251. Андреещев И. А., Будников С. А., Гладков А. В. Полумарковская модель оценки конфликтной устойчивости информационной инфраструктуры // Вестник воронежского государственного университета. Серия: Системный анализ и информационные технологии. 2017. № 1. С. 10-17.

252. Андреещев И. А., Будников С. А., Пиндус А. М. Полумарковская модель оценки надежности функционирования информационно-телекоммуникационных систем в органах внутренних дел // Охрана, безопасность, связь. 2016. № 1-6. С. 41-48.

253. Будников С. А. Оценка вероятностных показателей в конфликте информационно-управляющих систем // Системы управления и информационные технологии. 2009. № 3(37). С. 27-31.

254. Жуматий В. П., Будников С. А., Паршин Н. В. Угрозы программно-математического воздействия. – Воронеж: ЦПКС ТЗИ, 2010. – 230 с.

255. Козирацкий Ю. Л., Будников С. А., Островский Д. Б., Кильдюшевский В. М. Модель процесса возникновения и протекания конфликта информационных средств разных видов // Радиотехника. 2011. № 8. С. 6-11.

256. Малышева И. Н., Козирацкий Ю. Л., Панов С. А. К вопросу о синтезе автоматической системы управления в комплексах критических приложений // Теория и техника радиосвязи. 2017. № 2. С. 72-77.

257. Козирацкий Ю. Л., Иванцов А. В. Влияние оперативности и достоверности ведения разведки на исход информационного конфликта в условиях активного двустороннего противодействия // Военная мысль. 2014. № 9. С. 23-28.

258. Козирацкий Ю. Л., Кущев С. С., Чернухо И. И., Донцов А. А. Модель конфликтного взаимодействия систем управления противоборствующих сторон в условиях преднамеренных помех // Радиотехника. 2012. № 5. С. 56-61.

259. Владимиров В. И., Лихачев В. П., Шляхин В. М. Антагонистический конфликт радиоэлектронных систем. – М.: Радиотехника, 2004. – 384 с.

260. Владимиров В. И., Владимиров И. В., Шацких В. М. Статистическая модель распределения относительных информационных потерь на выходе канала передачи информации для оценки вероятности радиоподавления к исходу информационного конфликта // Радиотехника. 2013. № 7. С. 11-15.

261. Владимиров В. И., Владимиров И. В., Шацких В. М. Результаты оценки влияния шумов естественного происхождения на исход информационного конфликта линии радиосвязи и средства радиоподавления // Радиотехника. 2015. № 12. С. 7-12.

262. Владимиров В. И., Владимиров И. В., Шацких В. М. Подход к оценке состояния линий радиосвязи с обратной связью в информационном конфликте // Радиотехника. 2014. № 9. С. 15-19.

263. Владимиров В. И., Владимиров И. В., Стучинский В. И. Статистическая модель оценки (прогнозирования) исхода информационной блокады средствами радиоэлектронного подавления приемо-передающих пунктов информационно-управляющих систем // Двойные технологии. 2017. № 1 (78). С. 42-52.

264. Владимиров И. В. Устойчивость организационно-технических систем специального назначения. направления развития методов ее оценки // Вопросы радиоэлектроники. 2012. Т. 3. № 1. С. 110-120.

265. Деттмер У. Теория ограничений Голдратта: Системный подход к непрерывному совершенствованию / Пер. с англ. 2-е изд. – М.: Альпина Бизнес Букс, 2008. – 444 с.

266. Коцыняк М.А., Осадчий А. И., Коцыняк М. М., Лаута О. С., Дементьев В. Е., Васюков Д. Ю. Обеспечение устойчивости информационно-телекоммуникационных систем в условиях информационного противоборства. – СПб.: ЛО ЦНИИС, 2015. – 126 с.

267. Дементьев И. В., Чаркин Д. Ю. К вопросу об определении точек бифуркации в инфокоммуникационной системе в условиях информационного противоборства // Теория и техника радиосвязи. 2018. № 3. С. 32-36.

268. Жидко Е. А., Разиньков С. Н. Имитационное моделирование и анализ конфликтного компонента информационно-телекоммуникационной системы с управляемой структурой // Радиолокация, навигация, связь. Сборник трудов XXIV Международной научно-технической конференции. В 5-и томах. – Воронеж, 2018. – С. 327-334.

269. Бобрусь А. В. Анализ конфликта систем на основе моделей Абрамова // Техника машиностроения. 2016. Т. 23. № 4 (100). С. 29-31.

270. Бобрусь А. В. Анализ конфликта систем на основе моделей Абрамова // Информационные технологии. Проблемы и решения. 2015. № 1-2. С. 151-155.

271. Мистров Л. Е., Павлов В. А., Шерстяных Е. С. Устойчивость информационных систем в конфликтном взаимодействии организационно-технических систем // Стратегическая стабильность. 2017. № 2 (79). С. 43-49.

272. Мистров Л. Е. Конфликтная устойчивость взаимодействия организационно-технических систем: общие понятия, научные подходы, метод синтеза // Наукоемкие технологии. 2011. Т. 12. № 9. С. 70-80.

273. Мистров Л. Е., Сербулов Ю. С. Методологические основы синтеза информационно-обеспечивающих функциональных организационно-технических систем. – Воронеж: Научная книга, 2007. – 232 с.

274. Величко С. В., Мистров Л. Е., Сербулов Ю. С. Методологические основы синтеза решений по управлению экологическими конфликтами. – Воронеж: Научная книга, 2008. – 386 с.

275. Сербулов Ю. С. Модели выбора и распределения ресурсов технологических систем в условиях их замещения и конфликта. Дис. … д-ра техн. наук. – Воронеж, 1999. – 306 с.

276. Бирюков Д. Н., Ломако А. Г. Подход к построению ИБ-систем, способных синтезировать сценарии упреждающего поведения в информационном конфликте // Защита информации. Инсайд. 2014. № 6 (60). С. 42-49.

277. Бирюков Д. Н., Ломако А. Г. Метод синтеза сценариев упреждения на основе ассоциативно-рефлекторного поведения // Проблемы информационной безопасности. Компьютерные системы. 2015. № 1. С. 52-56.

278. Жидко Е. А., Леонов П. М., Попова Е. С. Разработка модели идентификации конфликтного компонента и метода ситуационного управления информационными ресурсами информационно-телекоммуникационной системы критически важного объекта в условиях информационного противоборства. Монография. – Воронеж, 2019. – 124 с.

279. Морозов А. В., Чукляев И. И. Информационная безопасность вычислительных систем боевого управления в аспекте информационного противоборства // Проблемы безопасности российского общества. 2013. № 2-3. С. 85-90.

280. Чукляев И. И. Игровая модель обоснования применения средств комплексной защиты информационных ресурсов иерархической информационно-управляющей системы // T-Comm: Телекоммуникации и транспорт. 2015. №2. С. 64-68.

281. Морозов А. В., Майбуров Д. Г., Чукляев И. И. Информационное оружие: теория и практика применения // Проблемы безопасности российского общества. 2014. № 2. С. 177-183.

282. Остапенко Г. А., Колбасов С. М. Модели тактик реализации информационного конфликта // Информация и безопасность. 2006. Т. 9. № 1. С. 46-50.

283. Остапенко Г. А. Структурно-параметрическая модель информационного конфликта систем // Безопасность информационных технологий. 2007. № 2. С. 93-94.

284. Остапенко Г. А. Информационные операции и атаки в социотехнических системах. Монография. – Воронеж: Воронежский гос. технический ун-т, 2005. – 204 с.

285. Остапенко Г. А., Плотников Д. Г., Гузеев Ю. Н. Разновидности сетевых конфликтов // Информация и безопасность. 2016. Т. 19. № 1. С. 126-129.

286. Остапенко Г. А., Плотников Д.Г., Гузеев Ю. Н. Особенности конфликтологии взвешенных сетей: понятие сетевого конфликта // Информация и безопасность. 2016. Т. 19. № 1. С. 136-137.

287. Остапенко Г. А., Плотников Д. Г., Гузеев Ю. Н. Формализация описания сетевого конфликта // Информация и безопасность. 2016. Т. 19. № 2. С. 232-237.

288. Остапенко Г. А., Плотников Д.Г., Гузеев Ю. Н. Формализация описания сетевого конфликта // Информация и безопасность. 2016. Т. 19. № 2. С. 250-253.

289. Остапенко Г. А., Плотников Д.Г., Гузеев Ю. Н. Динамика развития сетевого конфликта // Информация и безопасность. 2016. Т. 19. № 2. С. 278-279.

290. Остапенко Г. А., Мишина Я. С., Белоножкин В. И., Шевченко И. В. Алгоритмизация живучести сетевых информационных структур // Информация и безопасность. 2014. Т. 17. № 2. С. 304-307.

291. Привалов А. А., Попов П. В. Электромагнитная совместимость средств связи и её влияние на устойчивость функционирования системы связи ВМФ в условиях воздействия противника оружием функционального поражения // Технологии электромагнитной совместимости. 2004. № 4. С. 65-68.

292. Привалов А. А., Попов П. В. Электромагнитная совместимость средств связи и её влияние на устойчивость функционирования системы связи ВМФ в условиях воздействия противника оружием функционального поражения // Технологии электромагнитной совместимости. 2004. № 11. С. 65-67.

293. Привалов А. А., Евглевская Н. В., Зубков К. Н. Модель процесса вскрытия параметров сети передачи данных оператора IP-телефонной сети компьютерной разведкой организованного нарушителя // Известия Петербургского университета путей сообщения. 2014. № 2 (39). С. 106-111.

294. Евглевская Н. В., Привалов А. А., Привалов А. А. Обобщенная модель информационного воздействия на автоматизированные системы управления техническими объектами // Вопросы радиоэлектроники. 2013. Т. 3. № 1. С. 155-164.

295. Евглевская Н. В., Привалов А. А., Привалов А. А. Модель процесса вскрытия каналов утечки информации на объектах телекоммуникаций // Вопросы радиоэлектроники. 2014. Т. 3. № 1. С. 156-161.

296. Евглевская Н. В., Привалов А. А., Скуднева Е. В. Марковская модель конфликта автоматизированных систем обработки информации и управления с системой деструктивных воздействий нарушителя // Известия Петербургского университета путей сообщения. 2015. № 1 (42). С. 78-84.

297. Евглевская Н. В., Привалов А. А. Модель информационного воздействия на объекты телекоммуникационной сети // Известия Петербургского университета путей сообщения. 2015. № 1 (42). С. 72-77.

298. Привалов А. А., Привалов А. А., Скуднева Е. В., Чалов И. В. Подход к оценке вероятности вскрытия пространственно-временной и информационной структуры СПД-ОТН // Известия Петербургского университета путей сообщения. 2015. № 3 (44). С. 165-172.

299. Добрышин М. М. Предложение по совершенствованию систем противодействия DDOS-атакам // Телекоммуникации. 2018. № 10. С. 32-38.

300. Добрышин М. М., Закалкин П. В. Способ мониторинга защищенности информационно-телекоммуникационных сетей от

информационно технических воздействий // Информационные системы и технологии. 2018. № 5 (109). С. 74-82.

301. Добрышин М. М. Предложения по противодействию компьютерной разведке и информационно-техническим воздействиям // Телекоммуникации. 2017. № 9. С. 2-7.

302. Бегаев А. Н., Гречишников Е. В., Добрышин М. М., Закалкин П. В. Предложение по оценке способности узла компьютерной сети функционировать в условиях информационно-технических воздействий // Вопросы кибербезопасности. 2018. № 3 (27). С. 2-8.

303. Гречишников Е. В., Добрышин М. М., Закалкин П. В. Модель узла доступа VPN как объекта сетевой и потоковой компьютерных разведок и DDOS-атак // Вопросы кибербезопасности. 2016. № 3 (16). С. 4-12.

304. Гречишников Е. В., Добрышин М. М. Оценка эффективности деструктивных программных воздействий на сети связи // Системы управления, связи и безопасности. 2015. № 2. С. 135-146.

305. Гречишников Е. В., Горелик С. П., Добрышин М. М. Способ обеспечения требуемой защищенности сети связи от внешних деструктивных воздействий // Телекоммуникации. 2015. № 6. С. 32-37.

306. Гречишников Е. В., Добрышин М. М., Горелик С. П. Способ защиты элементов виртуальных частных сетей связи от DDOS-атак // Патент на изобретение RUS 2636640. 11.03.2016.

307. Гречишников Е. В., Добрышин М. М., Шугуров Д. Е., Берлизев А. В., Макаров В. Н. Способ мониторинга сетей связи в условиях ведения сетевой разведки и информационно технических воздействий // Патент на изобретение RUS 2612275 09.12.2015

308. Иванов В. А., Гречишников Е. В., Двилянский А. А. Устройство активной защиты и обеспечения технической готовности элементов локальной вычислительной сети при воздействии электромагнитного импульса // Вестник компьютерных и информационных технологий. 2006. № 2 (20). С. 44-46.

309. Гречишников Е. В., Комолов Д. В. Способ защиты объекта от управляемых ракет // Патент на изобретение RUS 2390721. 24.11.2008.

310. Скоредова Ю. В., Гречишников Е. В., Кравченко А. С., Ланкин О. В. Анализ методик автоматизированной оценки угроз и рисков информационной безопасности информационно-телекоммуникационных систем // Вестник Воронежского института ФСИН России. 2017. № 3. С. 128-133.

311. Гречишников Е. В., Гусев А. П. Обеспечение устойчивости системы связи в условиях сверхвысокочастотного электромагнитного излучения // Телекоммуникации. 2011. № 10. С. 37-41.

312. Стародубцев Ю. И., Гречишников Е. В., Комолов Д. В. Использование нейронных сетей для обеспечения устойчивости сетей связи в условиях внешних воздействий // Телекоммуникации. 2009. № 2. С. 24-31.

313. Гречишников Е. В., Дыбко Л. К., Ерышов В. Г., Жуков А. В., Стародубцев Ю. И. Способ обеспечения устойчивого функционирования системы связи // Патент на изобретение RUS 2405184. 12.05.2009.

314. Стародубцев Ю. И., Гречишников Е. В., Комолов Д. В. Способ обеспечения устойчивости сетей связи в условиях внешних деструктивных воздействий // патент на изобретение RUS 2379753. 21.04.2008.

315. Гречишников Е. В., Ерышов В. Г., Панкин А. А., Стародубцев П. Ю. Способ обнаружения специальных электронных устройств на объектах связи // Телекоммуникации. 2011. № 7. С. 38-41.

316. Белов А. С., Иванов В. А., Будилкин С. А., Стародубцев Ю. И., Гречишников Е. В., Стукалов И. В. Способ построения защищенной системы связи // Патент на изобретение RUS 2459370. 28.06.2010.

317. Гречишников Е. В., Стародубцев Ю. И., Белов А. С., Гусев А. П. Способ (варианты) защиты системы связи от внешних деструктивных воздействий // Патент на изобретение RUS 2451416. 21.04.2011.

318. Иванов В. А., Белов А. С., Гречишников Е. В., Стародубцев Ю. И., Ерышов В. Г., Алашеев В. В., Иванов И. В. Способ контроля демаскирующих признаков системы связи // Патент на изобретение RUS 2419153. 30.06.2009.

320. Гречишников Е. В., Стародубцев Ю. И., Белов А. С., Стукалов И. В., Васюков Д. Ю., Иванов И. В. Способ (варианты) управления демаскирующими признаками системы связи // Патент на изобретение RUS 2450337. 03.05.2011.

321. Гречишников Е. В., Белов А. С., Скубьев А. В. Способ обеспечения живучести сети связи в зоне обслуживания подвижных абонентов // Телекоммуникации. 2016. № 7. С. 13-18.

322. Гречишников Е. В., Белов А. С., Шумилин В. С. Способ управления защищенностью сетей связи в условиях деструктивных программных воздействий // Телекоммуникации. 2014. № 3. С. 18-22.

323. Горелик С. П., Гречишников Е. В., Белов А. С. Предложения по обеспечению живучести элементов сетей связи в чрезвычайных ситуациях // Телекоммуникации. 2013. № 4. С. 23-26.

324. Гречишников Е. В., Белов А. С., Иванов В. А., Жидков С. А., Загородников М. А. Устройство для оценки технического состояния и обеспечения устойчивости каналов и средств связи в телекоммуникационных системах // Патент на изобретение RUS 2385537. 30.06.2008.

325. Гречишников Е. В., Иванов В. А., Белов А. С., Соловьёв А. М., Жидков С. А. Способ моделирования процессов обеспечения живучести системы связи в условиях огневого поражения и радиоэлектронной борьбы // Патент на изобретение RUS 2406146. 06.04.2009.

326. Гречишников Е. В., Белов А. С., Добрышин М. М. Способ моделирования оценки ущерба, наносимого сетевыми и компьютерными атаками виртуальным частным сетям // Патент на изобретение RUS 2625045. 11.03.2016.

327. Гасюк Д. П., Белов А. С., Трахинин Е. Л. Научно-методический подход по оцениванию живучести компьютерных систем в условиях внешних специальных программно-технических воздействий // Проблемы информационной безопасности. Компьютерные системы. 2018. № 4. С. 86-90.

328. Белов А. С. Моделирование разноуровневых систем управления с распределенными элементами в условиях информационного противоборства // Телекоммуникации. 2018. № 3. С. 10-17.

329. Белов А. С., Скубьев А. В. Научно-техническое решение по обеспечению структурной живучести распределенных сетей связи в условиях деструктивных воздействий // Телекоммуникации. 2018. № 7. С. 11-15.

330. Белов А. С., Прутков Г. М., Сазыкин А. М. Способ обеспечения живучести распределенных сетей связи в условиях деструктивных воздействий // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2018. № 7-8 (121-122). С. 69-76.

331. Белов А. С., Скубьев А. В. Теоретический подход по оцениванию и обеспечению живучести распределенных сетей связи в условиях информационного противоборства // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. № 2. С. 22-33.

332. Белов А. С., Зубачев А. Б., Скубьев А. В. Предложение по обеспечению живучести распределенной абонентской сети связи // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2016. № 11-12 (101-102). С. 58-62.

333. Войцеховский А. И., Белов А. С., Киселев А. А., Иванов В. А., Кривенцов О. Б., Мельнов А. И. Способ моделирования преднамеренных повреждений элементов сети связи // Патент на изобретение RUS 2449366. 21.01.2011.

334. Вознюк В. В., Ворона С. Г., Маслаков П. А., Куценко Е. В. Математическая модель многоуровневого конфликта радиоподавления многоканальной системы радиосвязи множеством организованных помех // Радиотехника. 2017. № 9. С. 89-100.

335. Буренин А. Н., Воробьев С. П., Давыдов А. Е., Курносов В. И. Инфокоммуникационные сети: энциклопедия. Том 2: Основы управления и обеспечения безопасности связи и информации в инфокоммуникационных сетях / Под ред. А. Ю. Рунеева. – М.: Наука, 2015. – 611 с.

336. Фокин В. Г. Оптические системы передачи и транспортные сети. Учебное пособие. – М.: Эко-Трендз, 2008. – 288 с.

337. Фокин В. Г. Проектирование оптической мультисервисной транспортной сети: учебное пособие. – Новосиборск: СибГУТИ, 2009. – 205 с.

338. Макаренко С. И., Сапожников В. И., Захаренко Г. И., Федосеев В. Е. Системы связи: учебное пособие для студентов (курсантов) вузов. – Воронеж: ВАИУ, 2011. – 285 с.

339. Аганесов А. В. Модель сети воздушной радиосвязи на основе протокола случайного множественного доступа CSMA/CA // Системы управления, связи и безопасности. 2015. № 1. С. 67-97.

340. Силяков В. А., Красюк В. Н. Системы авиационной радиосвязи: Учебное пособие / Под ред. В.А. Силякова. – СПб.: ГУАП, 2004. – 160 с.

341. Кузьмин Б. И. Сети и системы авиационной цифровой электросвязи: учебное пособие. В 3-х частях.– СПб.: ОАО «НИИЭИР», 1999, 2000, 2003.

342. Кульчицкий В. К., Мешалов Р. О., Журавлев С. С. Системы, комплексы и средства авиационной электросвязи / Под ред. С.А. Кудрякова. – СПб.: Свое издательство, 2015.

343. Кудряков С. А., Кульчицкий В. К., Поваренкин Н. В., Пономарев В. В., Рубцов Е. А., Соболев Е. В., Сушкевич Б. А. Радиотехническое обеспечение полетов воздушных судов и авиационная электросвязь. Учебное пособие. – СПб.: Свое издательство, 2016.

344. Бреслер И. Б., Горбач А. Н., Ланчев В. М., Полушин К. В., Пшеницын А. А., Смирнова Е. В., Угловский Е. П. Средства связи противовоздушной обороны ВВС / Под ред. В.М. Ланчева. – Тверь: ВУ ПВО, 2003.

345. Верба В. С., Меркулов В. И. Теоретические и прикладные проблемы разработки систем радиоуправления нового поколения // Радиотехника. 2014. № 5. С. 39-44.

346. Меркулов В. Н., Дрогалин В. В., Канащенков А. Н., Лепин В. Н., Самарин О. Ф., Соловьев А. А. Авиационные системы радиоуправления. Том 1. Принципы построения систем радиоуправлсния. Основы синтеза и анализа / Под ред. А.И. Канащенкова и В.И. Меркулова. – М.: Радиотехника, 2003. – 192 с.

347. Меркулов В. И., Канащенков А. И., Чернов В. С., Дрогалин В. В., Антипов В. Н., Анцев Г. В., Кулабухов В. С., Лепин В. Н., Сарычев В. А., Саблин В. Н., Самарин О. Ф., Тупиков В. А., Турнецкий Л. С., Харьков В. П. Авиационные системы радиоуправления. Том 3. Системы командного радиоуправления. Автономные и комбинированные системы наведения / под ред. А.И. Канащенкова и В.И. Меркулова – М.: Радиотехника, 2004. – 320 с.

348. Войткевич К. Л. Методы управления трафиком в наземно-воздушных сетях связи. Дис. … докт. техн. наук. – Н.Новгород: НПП «Полет», 1998. – 375 с.

349. Белоусов Е. Л., Кейстович А. В., Войткевич К. Л., Брянцев В. Ф., Сайфетдинов Х. И. Современное оборудование сети авиационной электросвязи // Системы и средства связи, телевидения и радиовещания. 2012. № 1-2. С. 70-73.

350. Войткевич К. Л. Сулима А. А., Зац П. А. Проблемы построения канала управления беспилотными летательными аппаратами на основе ДКМВ-радиолинии // Электросвязь. 2014. № 7. С. 9-11.

351. Головченко Е. В., Федюнин П. А., Дьяченко В. А., Стафеев М. А. Авиационные инфокоммуникационные сети: монография. – Воронеж: ВУНЦ ВВС «ВВА», 2018. – 157 с.

352. Смирнов С. В. Анализ исследований в области авиационной радиосвязи и обоснование перспективных путей совершенствования сетей радиосвязи управления авиацией с авиационного комплекса радиолокационного дозора и наведения // Системы управления, связи и безопасности. 2017. № 3. С. 1-27.

353. Смирнов С. В. Анализ способов и средств управления авиацией с авиационного комплекса радиолокационного дозора и наведения // Системы управления, связи и безопасности. 2017. № 2. С. 69-100.

354. Смирнов С. В. Модель сети воздушной радиосвязи для управления авиацией с авиационного комплекса радиолокационного дозора и наведения // Системы управления, связи и безопасности. 2017. № 2. С. 165-181.

355. Тестоедов Н. А., Косенко В. Е., Выгонский Ю. Г., Кузовников А. В., Мухин В. А., Чеботарев В. Е., Сомов В. Г. Космические системы ретрансляции. Монография / Под ред. А.В. Кузовникова. – М.: Радиотехника, 2017. – 448 с.

356. Сомов А. М., Корнев С. Ф. Спутниковые системы связи: Учебное пособие для вузов / Под ред. А.М. Сомова. − М.: Горячая линия - Телеком, 2012. – 244 с.

357. Камнев В. Е., Черкасов В. В., Чечин Г. В. Спутниковые сети связи: Учебное пособие. – М.: «Альпина Паблишер», 2004. – 536 с.

358. Современные технологии радиомониторинга спутниковых систем связи ретрансляции. Монография / Под ред. А.В. Кузовникова. – М.: Радиотехника, 2015. – 216 с.

359. Макаренко С. И. Описательная модель системы спутниковой связи Iridium // Системы управления, связи и безопасности. 2018. № 4. С. 1-34.

360. Макаренко С. И. Описательная модель системы спутниковой связи Inmarsat // Системы управления, связи и безопасности. 2018. № 4. С. 64-91.

361. Давыдов А. Е., Максимов Р. В., Савицкий О. К. Защита и безопасность ведомственных интегрированных инфокоммуникационных систем. – М.: ОАО Воентелеком, 2015. – 520 с.

362. Голуб Б. В., Кузнецов Е. М., Максимов Р. В. Методика оценки живучести распределенных информационных систем // Вестник Самарского университета. Естественнонаучная серия. 2014. № 7 (118). С. 221-232.

363. Искольный Б. Б., Максимов Р. В., Шарифуллин С. Р. Оценка живучести распределенных информационно-телекоммуникационных сетей // Вопросы кибербезопасности. 2017. № 5 (24). С. 72-82.

364. Максимов Р. В., Выговский Л. С. Модель преднамеренных деструктивных воздействий на информационную инфраструктуру интегрированных систем связи // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2008. № 3 (60). С. 166-173.

365. Максимов Р. В., Выговский Л. С. Модель преднамеренных деструктивных воздействий на информационную инфраструктуру интегрированных систем связи // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2009. № 1 (72). С. 181-187.

366. Лыков Н. Ю., Максимов Р. В., Шарифуллин С. Р. Маскирование структуры и алгоритмов функционирования интегрированных инфокоммуникационных систем // В сборнике: Технические и технологические

системы. Материалы восьмой международной научной конференции «ТТС-16». – Краснодар: КГТУ, 2016. – С. 203-206.

367. Шерстобитов Р. С., Шарифуллин С. Р., Максимов Р. В. Маскирование интегрированных сетей связи ведомственного назначения // Системы управления, связи и безопасности. 2018. № 4. С. 136-175.

368. Куликов О. Е., Липатников В. А., Максимов Р. В., Можаев О. А. Способ защиты информационно-вычислительных сетей от компьютерных атак // Патент на изобретение RUS 2285287. 04.04.2005.

369. Волков В. А., Пономаренко Е. Н., Чопоров О. Н., Радько Н. М., Язов Ю. К. Рекомендации по управлению рисками и структурной живучестью при угрозе распространения деструктивного контента в корпоративной информационно-телекоммуникационной сети с ярко выраженной кластеризацией // Управление информационными рисками и обеспечение безопасности инфокоммуникационных систем. 2017. Т. 15. № 1. С. 98-103.

370. Нестеровский И. П., Язов Ю. К. Возможный подход к оценке ущерба от реализации угроз безопасности информации, обрабатываемой в государственных информационных системах // Вопросы кибербезопасности. 2015. № 2 (10). С. 20-25.

371. Язов Ю. К., Сердечный А. Л., Шаров И. А. Методический подход к оцениванию эффективности ложных информационных систем // Вопросы кибербезопасности. 2014. № 1 (2). С. 55-60.

372. Язов Ю. К., Сигитов В. Н. Информационные риски в условиях применения технологии виртуализации в информационно-телекоммуникационных системах // Информация и безопасность. 2013. Т. 16. № 3. С. 403-406.

373. Шивдяков Л. А., Бозарный И. Н., Головин С. А., Язов Ю. К. Структура, базовые функции и возможности специализированной экспертной системы оценки состояния обеспечения безопасности информации в критически важных системах информационной инфраструктуры // Информация и безопасность. 2010. Т. 13. № 3. С. 381-386.

374. Язов Ю. К., Седых И. М. Методический подход к оценке возможности обнаружения сетевых атак на основе последовательного анализа их сигнатур // Телекоммуникации. 2006. № 5. С. 29-34.

375. Язов Ю. К., Седых И. М. Использование статистических критериев принятия решений в интересах обнаружения сетевых атак по их сигнатурам // Информация и безопасность. 2005. Т. 8. № 1. С. 141-146.

376. Язов Ю. К., Панфилов А. П. Марковская модель динамики реализации сетевых атак типа "подмена доверенного объекта" // Информация и безопасность. 2005. Т. 8. № 1. С. 130-134.

377. Жижелев А. В., Панфилов А. П., Язов Ю. К., Батищев Р. В. К оценке эффективности защиты информации в телекоммуникационных системах посредством нечетких множеств // Известия высших учебных заведений. Приборостроение. 2003. Т. 46. № 7. С. 22-29.

378. Герасименко В. Г., Язов Ю. К., Батищев Р. В., Седых И. М. Об оценке возможности обнаружения сетевых атак с использованием искусственных нейронных сетей // Информация и безопасность. 2002. Т. 5. № 1. С. 20-24.

379. Герасименко В. Г., Седых И. М., Язов Ю. К. Принципы построения адаптивных систем защиты компьютерных сетей от несанкционированного доступа // Информация и безопасность. 2002. Т. 5. № 2. С. 106-107.

380. Батищев Р. В., Язов Ю. К., Остапенко Г. А., Ференец С. С. Формализация описания угроз безопасности информации в информационно-телекоммуникационных системах // Информация и безопасность. 2002. Т. 5. № 3. С. 119-122.

381. Воробьев С. П., Давыдов А. Е., Ефимов В. В., Курносов В. И. Инфокоммуникационные сети: энциклопедия. Том 1: Инфокоммуникационные сети: классификация, структура, архитектура, жизненный цикл, технологии / Под ред. С. П. Воробьева. – СПб.: Наукоемкие технологии, 2019. – 739 с.

382. Макаренко С. И. Описательная модель системы спутниковой связи MUOS // Системы управления, связи и безопасности. 2019. № 3. С. 89-116. DOI: 10.24411/2410-9916-2019-10306.

383. Михайлов Р. Л. Описательные модели систем спутниковой связи как космического эшелона телекоммуникационных систем специального назначения. Монография. – СПб.: Наукоемкие технологии, 2019. – 150 с.

384. Острейковский В. А. Теория систем: учебник для вузов по специальности «Автоматические системы обработки информации и управления». – М.: Высшая школа, 1997. – 240 с.

385. Сурмин Ю. П. Теория систем и системный анализ: Учебное пособие. – К.: МАУП, 2003. –368 с.

386. Месарович М., Такахара И. Общая теория систем: математические основы. – М.: Мир, 1978. – 311 с.

387. Павлов А. Н., Соколов Б. В., Москвин Б. В., Верзилин Д. Н. Военная системотехника и системный анализ: учебник / под общ. ред. А.Н. Павлова. – СПб.: ВКА им. А.Ф. Можайского, 2010. – 251 с.

388. Мануйлов Ю. С., Новиков Е. А. Методология системных исследований. − СПб.: ВКА им. А.Ф. Можайского, 2008. – 159 с.

389. ГОСТ Р 50922-96 Защита информации. Основные термины и определения. – М, 1996.

390. Макаренко С. И. Справочник научных терминов и обозначений. – СПб.: Наукоемкие технологии, 2019. – 254 с.

391. ГОСТ Р ИСО/МЭК 12207-99. Процессы жизненного цикла программных средств. – М.: ИПК Издательство стандартов, 2000.

392. ГОСТ РВ 0158-006-2018. Связь военная. Термины и определения. – М.: Стандартинформ, 2018. – 23 с.

393. IEEE Std 829 – 2008. IEEE Standard for Software and System Test Documentation. 2008.

394. Леньшин А. В. Бортовые системы и комплексы радиоэлектронного подавления – Воронеж: Научная книга, 2014. – 590 с.

395. Информационная война и защита информации. Словарь основных терминов и определений. – М.: ЦСОиП, 2011. – 68 с.

396. Одоевский С. М., Калюка В. И. Адаптивно-игровое моделирование военных сетей беспроводного абонентского доступа. Монография. Часть 1. – Новочеркаск: Учебно-производственный центр «Набла» Южно-Российского государственного политехнического университета (НПИ) имени М.И. Платова, 2009. – 216 с.

397. Одоевский С. М., Калюка В. И. Адаптивно-игровое моделирование военных сетей беспроводного абонентского доступа. Монография. Часть 2 / Под ред. А.М. Чуднова. – СПб.: Издательство Политехнического университета, 2017. – 342 с.

398. Инфокоммуникационные сети: энциклопедия. Том 3: Методы анализа и оптимизации структуры, архитектуры и жизненного цикла инфокоммуникационных сетей / С.П. Воробьев, А.Е. Давыдов, В.В. Ефимов, В.И. Курносов, Н.Н. Мошак; Под ред. С.П. Воробьева. – Изд. 2-е, перераб и доп. – СПб.: Наукоемкие технологии, 2019. – 376 с.

399. Самойленко Д. В., Еремеев М. А., Финько О. А. Система криптокодовой защиты информации для имитоустойчивой передачи данных // Методы и технические средства обеспечения безопасности информации. 2017. № 26. С. 24-26.

400. Петлеванный А. А., Финько О. А. Имитоустойчивое кодирование информации в радиоканалах с активным аналитиком // Нейрокомпьютеры: разработка, применение. 2016. № 10. С. 13-21.

401. Самойленко Д. В., Финько О. А., Еремеев М. А., Диченко С. А. Способ и устройство имитоустойчивой передачи информации по каналам связи // Патент на изобретение RU 2669144, 08.10.2018. Заявка № 2017141540 от 28.11.2017.

402. Самойленко Д. В., Финько О. А. Имитоустойчивая передача данных в защищенных системах однонаправленной связи на основе полиномиальных классов вычетов // Нелинейный мир. 2013. Т. 11. № 9. С. 647-658.

403. ГОСТ Р 58494-2019. Оборудование горно-шахтное. Многофункциональные системы безопасности угольных шахт. Система дистанционного контроля опасных производственных объектов. – М., 2020.

404. Куприянов А. И. Ракеты против РЛС. конструкция, компоновка, действие и противодействие. Монография. – М.: Вузовская книга, 2015. – 189 с.

405. Рябов К. «Тополь-М» и Minuteman III. К давнему спору о ракетах // Военное обозрение [Электронный ресурс]. 15.02.2017. – URL: https://topwar.ru/109233-topol-m-i-minuteman-iii-k-davnemu-sporu-o-raketah.html (дата обращения: 20.03.2020).

406. Баллистическая ракета подводных лодок Trident-2 D5 // Ракетная техника [Электронный ресурс]. 2020. – URL: https://missilery.info/missile/trident2 (дата обращения: 20.03.2020).

407. Крылатая ракета Tomahawk BGM-109 A/C/D // Ракетная техника [Электронный ресурс]. 2020. – URL: https://missilery.info/missile/bgm109c-d (дата обращения: 20.03.2020).

408. Макаренко С. И. Информационный конфликт системы связи с системой дестабилизирующих воздействий. Часть I: Концептуальная модель конфликта с учетом ведения разведки, физического, радиоэлектронного и информационного поражения средств связи // Техника радиосвязи. 2020. № 2 (45). С. 104-117. DOI: 10.33286/2075-8693-2020-45-104-117.

409. Макаренко С. И. Информационный конфликт системы связи с системой дестабилизирующих воздействий. Часть II: Формализация основных аспектов, определяющих выигрыш в конфликте // Техника радиосвязи. 2020. № 3 (46). С. 103-115. DOI: 10.33286/2075-8693-2020-46-103-115.

410. Макаренко С. И. Игровая модель информационного конфликта системы связи с системой дестабилизирующих воздействий // Автоматизация процессов управления. 2020. № 4 (62). С. 61-74. DOI: 10.35752/1991-2927-2020-4-62-61-74.

411. Палий А. И. Радиоэлектронная борьба. – М.: Воениздат, 1989. – 350 с.

412. Макаренко С. И. Информационный конфликт системы связи с системой дестабилизирующих воздействий. Часть III: Управление системой связи в условиях конфликта // Техника радиосвязи. 2021. № 1 (48). С. 103-116. DOI: 10.33286/2075-8693-2021-48-103-116.

Научное издание

Макаренко Сергей Иванович
(Санкт-Петербургский Федеральный исследовательский центр РАН;
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
им. В.И. Ульянова (Ленина))

Модели системы связи в условиях преднамеренных
дестабилизирующих воздействий и ведения разведки
Монография

Рецензенты:

Боговик Александр Владимирович, кандидат технических наук, профессор (Военная академия связи им. маршала Советского Союза С.М. Буденного);

Гречишников Евгений Владимирович, доктор технических наук, профессор (Воронежский институт правительственной связи – филиал Академии Федеральной службы охраны Российской Федерации);

Михайлов Роман Леонидович, кандидат технических наук (Военный ордена Жукова университет радиоэлектроники);

Финько Олег Анатольевич, доктор технических наук, профессор (Краснодарское высшее военное училище им. генерала армии С.М. Штеменко);

Цимбал Владимир Анатольевич, доктор технических наук, профессор (Серпуховский филиал Военной академии Ракетных войск стратегического назначения им. Петра Великого).

Издательство «Наукоемкие технологии»
ООО «Корпорация «Интел групп»
197372, Санкт-Петербург, пр. Богатырский, дом 32, к. 1 лит. А, пом. 6Н.
http://publishing.intelgr.com
Тел.: +7 (812) 945-50-63
E-mail: publishing@intelgr.com

ISBN 978-5-6044429-5-1

9 785604 442951

Гарнитура «TimesNewRoman». 18,16 п.л.
Тираж 600 экз. Подписано в печать 27.10.2020.

Материалы изданы в авторской редакции

Макаренко Сергей Иванович – доктор технических наук, доцент. Член-корреспондент Академии военных наук.

Родился в 1980 году в Ставрополе. В 2002 году окончил Военный авиационный технический университет имени проф. Н. Е. Жуковского (филиал в г. Ставрополь) по специальности «Автоматизированные системы управления и обработки информации».

В 2007 году в Ставропольском высшем военном авиационном инженером училище защитил диссертацию на соискание ученой степени кандидата технических наук по специальности «Вооружение и военная техника. Комплексы и системы военного назначения». С 2015 года – доцент по специальности «Военные системы управления, связи и навигации». В 2018 году в НИИ «Рубин» защитил диссертацию на соискание ученой степени доктора технических наук по специальности «Системы, сети и устройства телекоммуникаций».

В период с 2007 по 2017 годы проходил военную службу на научных и преподавательских должностях в Ставропольском высшем военном авиационном инженером училище, в ВУНЦ ВВС «Военно-воздушная академия имени проф. Н.Е. Жуковского и Ю.А. Гагарина», в Военно-космической академии имени А.Ф. Можайского. После увольнения из вооруженных сил работает на предприятиях оборонно-промышленного комплекса России, в учреждениях РАН, а также в системе высшего образования и подготовки научно-педагогических кадров высшей квалификации.

ISBN 978-5-6044429-5-1

9 785604 442951