МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 681.142.33:681.14

С.А. Агеев, А.С. Бушуев, Ю.П. Егоров, И.Б. Саенко

КОНЦЕПЦИЯ АВТОМАТИЗАЦИИ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В ЗАЩИЩЕННЫХ МУЛЬТИСЕРВИСНЫХ СЕТЯХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

***Агеев Сергей Александрович**, кандидат технических наук, доцент, докторант Военной академии связи им. С.М. Буденного (г. Санкт-Петербург). Окончил радиотехнический факультет Ульяновского политехнического института. Заместитель начальника научно-исследовательского отделения ФГУП «НПО «Сигнал». Специализируется в области проектирования телекоммуникационных систем. Имеет статьи, патенты в области систем передачи данных. [e-mail: serg123@mail.ru].*

***Бушуев Александр Сергеевич,** ведущий специалист отдела информационной безопасности Санкт-Петербургского филиала ВТБ 24, соискатель ФГУП «НПО «Рубин» (г. Санкт-Петербург). Окончил СПб ГТУ. Специализируется в области защиты информации в автоматизированных и телекоммуникационных системах. Имеет публикации в этой предметной области. [e-mail: bsn@telda.ru].*

***Егоров Юрий Петрович,** доктор технических наук, профессор. Окончил радиотехнический факультет Ленинградского высшего инженерного морского училища им. адмирала С.О. Макарова. Главный научный сотрудник ФНПЦ ОАО «НПО «Марс». Специализируется в области макропроектирования больших информационно-управляющих систем. Имеет монографии, статьи, патенты в области проектирования автоматизированных систем управления войсками. [e-mail: yupe@mail.ru].*

***Саенко Игорь Борисович**, доктор технических наук, профессор. Окончил Военную академию связи им. С.М. Буденного. Специализируется в области создания и разработки информационно-управляющих систем. Имеет монографии, статьи и патенты в этой предметной области. [e-mail: ibsaen@mail.ru].*

Аннотация

Рассматриваются концептуальные основы автоматизации управления информационной безопасностью защищенных мультисервисных сетей специального назначения. Обсуждаются концептуальная модель управления защищенными мультисервисными сетями (ЗМС), угрозы безопасности, задачи и механизмы защиты.

Ключевые слова: автоматизированная система управления сетью, защищенная мультисервисная сеть, информационная безопасность, модель TMN, модель угроз, телематические сетевые услуги.

***Sergey Alexanderovich Ageev,** Candidate of Engineering, Associate Professor; doctoral student at the Military Communications Academy named after S. Budenny (Saint-Petersburg); graduated from the Faculty of Radio-Engineering at the Ulyanovsk Polytechnic Institute; Deputy Head of R&D Department of Federal State Unitary Enterprise 'Research-and-Production Association 'Signal'; specializes in the field of telecommunications-system design; has articles, patents in the field of data-transfer systems. e-mail: serg123@mail.ru.*

Alexander Sergeevich Bushuev, *lead specialist of information-security department at the Saint-Petersburg VTB 24 branch, applicant at Federal State Unitary Enterprise 'Rubin' (Saint-Petersburg); graduated from the Saint-Petersburg State Technical University; specializes in the field of information security in computer-aided and telecommunications systems; author of publications in the above field. e-mail: bsn@telda.ru.*

Yury Petrovich Egorov, *Doctor of Engineering, Professor, graduated from the Faculty of Radio-Engineering at the Leningrad Maritime Engineering Academy named after S. Makarov; chief staff scientist of FRPC OJSC 'RPA "Mars'; specializes in the field of macro-design of large-scale information-management systems; has monographs, articles, patents in the field of design of computer-aided C2 systems for troops. e-mail: yupe@mail.ru.*

Igor Borisovich Saenko, *Doctor of Engineering, Professor, graduated from the Military Communications Academy named after S. Budenny; specializes in the field of creation and development of information-management systems; has monographs, articles and patents in this field. e-mail: ibsaen@mail.ru.*

Abstract

The article deals with conceptual basis for automation of information-security control for protected special-purpose multi-service networks. The authors discuss conceptual model of protected multi-service network control, security threats, protection tasks and mechanisms.

Key words: computer-aided network-control system, protected multi-service network, information security, TMN model, threat model, telematics network services.

Введение

Переживаемый этап развития информационных технологий характеризуется тенденцией к объединению различных информационных ресурсов в единое информационное пространство предметной области. Одним из основных технических решений, обеспечивающих реализацию этой тенденции, являются мультисервисные сети. Наиболее востребованным классом мультисервисных сетей являются защищенные мультисервисные сети, например для таких предметных областей, как национальная оборона, государственное управление и т. д. Отличительной особенностью ЗМС являются жесткие требования к обеспечению информационной безопасности.

ЗМС является территориально распределенной гетерогенной телекоммуникационной системой, предоставляющей пользователям базовый набор услуг заданного качества по передаче информации. ЗМС создается на основе общих для всех ее элементов системных, функциональных и технических принципов и предназначена:

– для передачи командно-сигнальной информации с заданными вероятностно-временными характеристиками;

– для передачи информационно-справочной информации различного объема, содержания и представления;

– для оказания телематических услуг связи (электронная почта, файловый обмен, IP-телефония с выходом на телефоны общего пользования, передача видео в реальном масштабе времени, организация мультимедийных конференций и т. д.).

Информационная безопасность ЗМС характеризуется степенью защищенности перечисленных видов информации от случайного или преднамеренного вмешательства в процесс их передачи, хранения или обработки, а также от попыток их хищения, изменения или разрушения [1].

Обеспечение информационной безопасности предполагает:

– анализ ЗМС и информационных ресурсов, подлежащих защите;

– определение и анализ угроз безопасности информации;

– построение модели угроз;

– разработку политики безопасности;

– разработку (выбор) сервисов и механизмов безопасности.

До настоящего времени общепринятой методологии обеспечения информационной безопасности ЗМС не существует, поэтому рассмотрение на концептуальном уровне перечисленных вопросов представляется актуальным.

Анализ ЗМС и информационных ресурсов, подлежащих защите

Структура ЗМС представлена на рисунке 1.

ЗМС включает:

– транспортные сети, обеспечивающие обмен информацией и предоставление телематических услуг;

– локально-вычислительные сети (ЛВС) пользователей, инициирующие и потребляющие транспортные услуги;

– комплексы средств абонентского доступа, обеспечивающие техническое сопряжение ЛВС с транспортными сетями;

– центр управления сетью и услугами (ЦУСУ), обеспечивающий необходимые конфигурации сетей связи, их эксплуатационные характеристики, рациональное использование ресурса связи, защиту информации, взаимодействие с внешними телекоммуникационными системами.

ЦУСУ совместно с резидентными компонентами, представленными в узлах маршрутизации и комплексах средств абонентского доступа, образует автоматизированную систему управления сетью (АСУС), обеспечивающую требуемое качество услуг ЗМС путем управления:

– конфигурацией ЗМС;

– устранением последствий отказов;

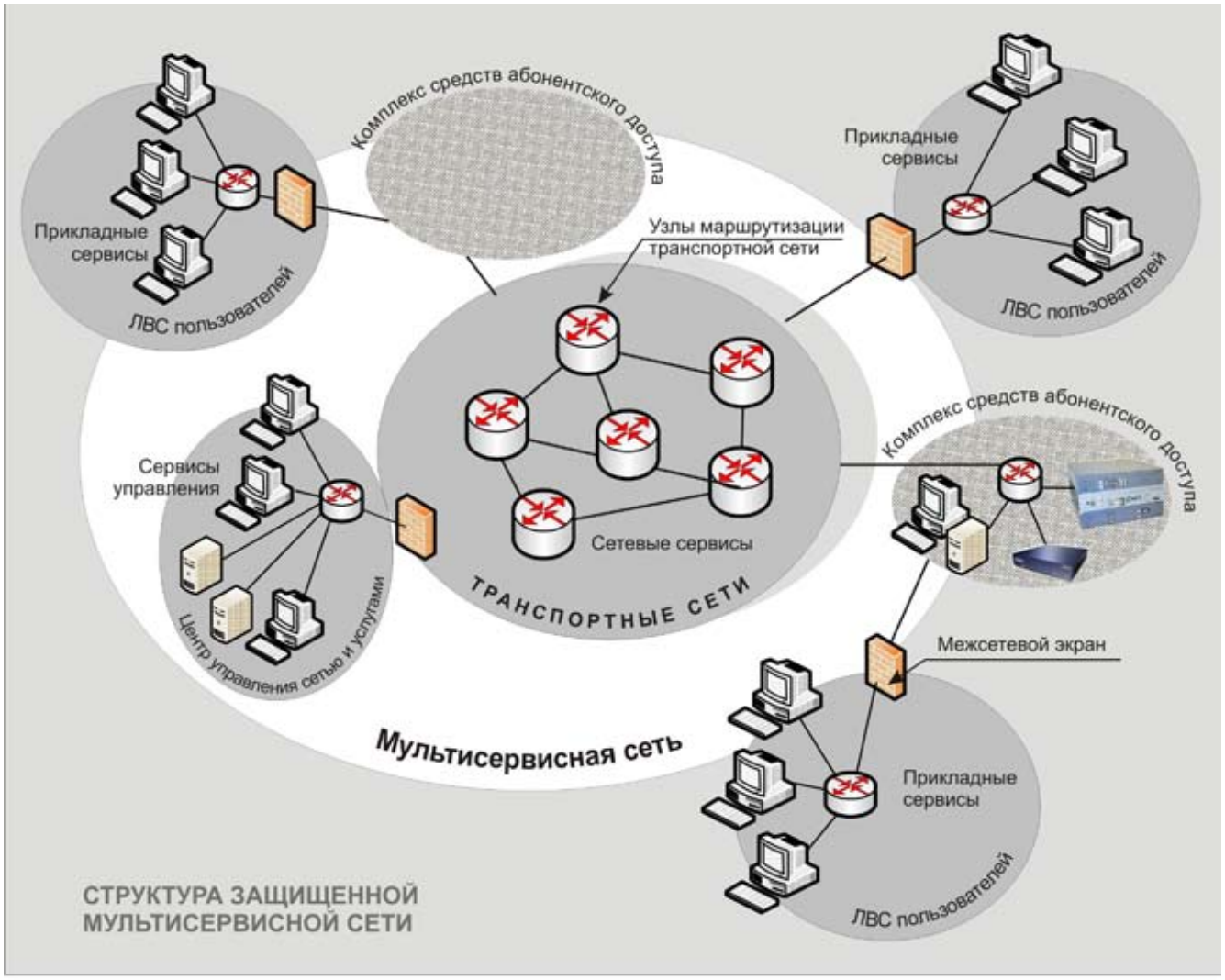

Рис. 1. Структура защищенной мультисервисной сети

– качеством работы ЗМС;

– информационной безопасностью.

При управлении информационной безопасностью АСУС ЗМС решает следующие задачи:

– обеспечение скрытности информации и контроль за ее осуществлением;

– защита баз данных узлов ЗМС от несанкционированного доступа (НСД);

– соблюдение конфиденциальности при предоставлении данных;

– установление уровней безопасности сетей связи и контроль за их соблюдением.

Одним из основных принципов, используемых при управлении ЗМС, является рациональное сочетание централизованного управления сетью в интересах всех ее пользователей с децентрализованным управлением входящими в ее состав сетями и подсистемами.

Существенными особенностями ЗМС как объекта управления информационной безопасностью являются:

– территориальная рассредоточенность ее элементов;

– наличие информационных ресурсов различной степени доступности и различного уровня конфиденциальности;

– наличие удаленных потребителей, использующих общедоступные сети передачи данных для доступа к информационным ресурсам отдельных ЛВС, входящих в состав АСУ специального назначения;

– разнообразие стандартов представления передаваемой информации.

В качестве системообразующей основы построения АСУС ЗМС представляется целесообразным принять концепцию TMN (Telecommunication Management Network) [2, 3]. Концепция TMN является базовой для реализации интегрированного управления любыми по структуре, составу и объему сетями связи и позволяет оптимизировать систему управления, обеспечить механизмы защиты и целостности данных, минимизировать время локализации и устранения неисправностей в сети, улучшить обслуживание и взаимодействие с пользователями, расширить диапазон услуг сети и обеспечить их требуемое качество.

Концептуальная композиция пирамидальных моделей управления АСУС ЗМС и TMN приведены на рисунке 2.

Одной из ключевых задач, решаемых при построении и функционировании ЗМС, является задача управления информационной безопасностью, которая сводится к за-

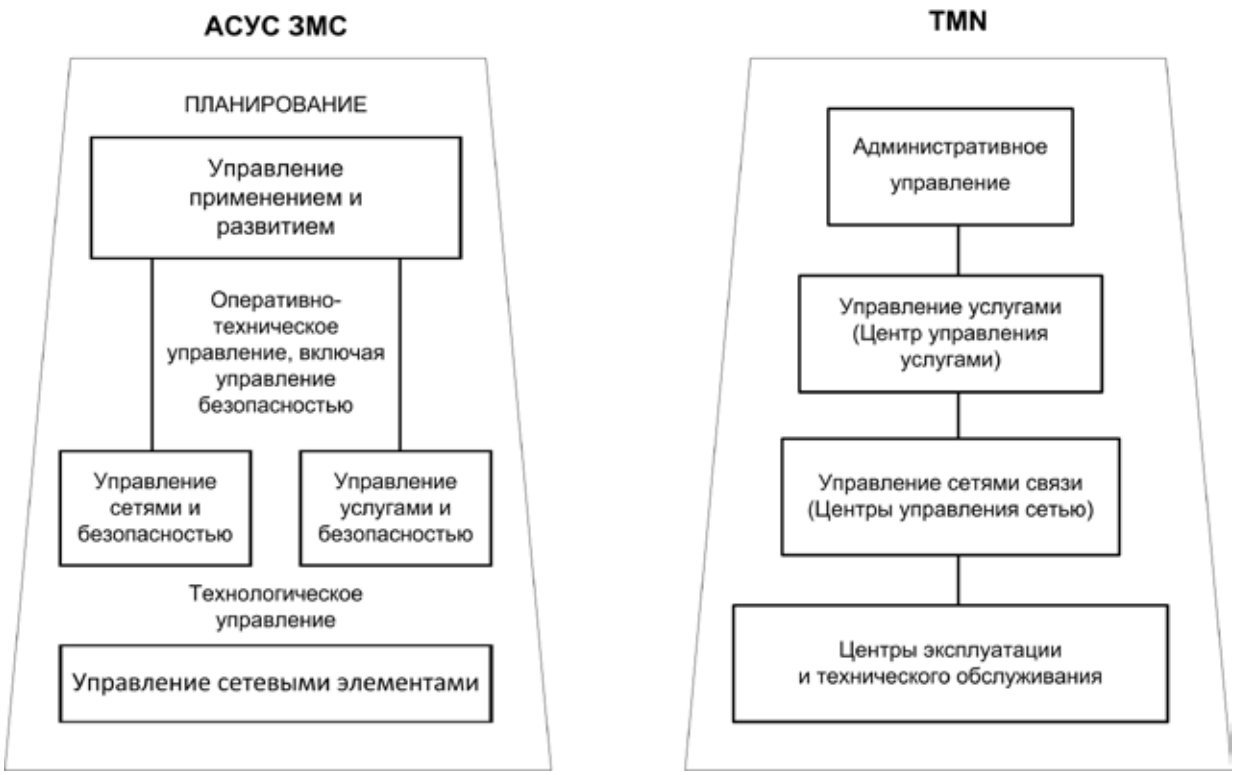

Рис. 2. Соотношение пирамидальных моделей АСУС ЗМС и TMN

щите обрабатываемой информации и управлению средствами защиты информации. Под защитой информации в ЗМС понимается деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию [4]. Управление средствами защиты обеспечивает первоначальную загрузку и периодическое обновление средств защиты (таблиц допусков, ключей доступа, меток конфиденциальности, настройку средств регистрации, средств контроля целостности программного и информационного обеспечения), контроль за их состоянием и оповещение о фактах нарушений.

Для обеспечения информационной безопасности в ЗМС создается подсистема защиты информации (ПсЗИ), которая представляет собой комплекс технических и программных средств защиты, а также организационных мер [4].

Определение и анализ угроз безопасности информации

Создание ПсЗИ требует, с одной стороны, подробного анализа требований к ПсЗИ в части используемых в ней технических и программных средств, видов обрабатываемой информации и принятых технологических схем ее

Таблица 1

Классификация угроз безопасности информации ЗМС

Классификационный признак	Виды угроз
Источник угрозы	Угрозы, источником которых является человек
	Угрозы, источником которых являются аппаратные или программные средства
	Угрозы, источником которых является окружающая среда
Принадлежность источника угрозы	Внутренние угрозы
	Внешние угрозы
Направленность угрозы	Угрозы конфиденциальности
	Угрозы целостности
	Угрозы доступности
Тип объекта угрозы	Угрозы технологической информации
	Угрозы передаваемой информации
Характер происхождения угрозы	Преднамеренные угрозы
	Непреднамеренные угрозы
Предпосылки возникновения	Угрозы, возникающие вследствие качественной недостаточности элементов системы
	Угрозы, возникающие вследствие количественной недостаточности элементов системы
Длительность воздействия	Постоянные угрозы
	Кратковременные угрозы

преобразования, а с другой – анализа возможностей существующих средств защиты информации, используемых в них механизмов, применимости для решения тех или иных задач защиты в составе ПсЗИ.

Существует ряд подходов к декомпозиции направлений защиты информации в ЗМС. Различие подходов определяется классификационными признаками угроз безопасности информации, положенными в основу выделения направлений защиты. В частности, один из известных подходов, изложенный в [5], в качестве результата классификации использует виды угроз защищаемой информации. Другим подходом к декомпозиции направлений защиты информации в ЗМС является подход, предлагаемый в [6]. В соответствии с ним результат классификации представляется возможными способами (каналами) реализации угроз информации.

Компромиссная классификация угроз безопасности ЗМС приведена в таблице 1.

Результаты анализа структурных и функциональных особенностей ЗМС позволяют сформировать перечень угроз безопасности информации, представленный в таблице 2.

В таблице 2 приняты следующие обозначения:

Вш – внешняя угроза;

П – угроза пользовательской информации;

К – угроза конфиденциальности информации;

Д – угроза доступности информации;

Сл – случайная угроза;

Вт – внутренняя угроза;

Т – угроза технологической информации;

Ц – угроза целостности информации;

Пр – преднамеренная угроза.

При наличии уточненных данных о структуре, программных и технических средствах ЗМС, используемых протоколах и регламенте функционирования ЗМС, а также о применяемых технологических схемах преобразования информации возможна дальнейшая детализация выделенных угроз безопасности информации путем построения для каждого из них соответствующего дерева угроз.

Построение модели угроз

Модель угроз, согласно ГОСТ Р ИСО 7498-2-99 [7], представляется как неформальный перечень возможных методов и способов несанкционированных действий нарушителя и возможных последствий этих действий. Модель угроз применительно к ЗМС приводится на рисунке 3.

Действия нарушителя, осуществляемые им в непо-

Таблица 2

Угрозы безопасности информации в ЗМС

№	Наименования угроз	Характеристики угроз				Возможные зависимости между угрозами
		Принадлежность источника угрозы	Тип объекта угрозы	Направленность угрозы	Происхождения угрозы	
1. При передаче информации						
1.1	Перехват передаваемой информации	Вш	П, Т	К	Пр	1.6
1.2	Удаление передаваемых сообщений	Вш	П, Т	Ц, Д	Пр, Сл	1.1
1.3	Переупорядочивание сообщений	Вш	П, Т	Ц, Д	Пр, Сл	1.1
1.4	Дублирование сообщений	Вш	П, Т	Ц	Пр	1.1
1.5	Вставка сообщений	Вш	П, Т	Ц	Пр	1.1
1.6	Навязывание ложного маршрута	Вш	П, Т	Ц, Д	Пр	1.1
1.7	Подмена адреса источника передаваемой информации	Вш	П, Т	Ц	Пр	1.6
1.8	Модификация сообщений	Вш	П, Т	Ц	Пр	1.1
2. При обработке и хранении информации						
2.1	Несанкционированное получение полномочий в системе	Вш, Вт	Т	К	Пр	1.6, 2.2, 2.3, 2.5
2.2	Подбор ключевой информации и информации аутентификации	Вш	Т	К	Пр	
2.3	Чтение, изменение, уничтожение параметров конфигурации элементов системы	Вш, Вт	Т	К, Ц, Д	Пр, Сл	2.1, 2.2
2.4	Обмен информацией между абонентами без применения средств защиты	Вт	П, Т	К	Пр, Сл	2.3
2.5	Передача информации пользователям, не имеющим к ней доступа	Вт	П, Т	К	Пр, Сл	2.3
2.6	Отказ источника/получателя информации от передачи/получения информации	Вт	П, Т	Д, Ц	Пр, Сл	
2.7	Перерасход ресурсов общего пользования	Вш, Вт	П, Т	Д	Пр	

средственном контакте с ЗМС, рассматриваются как атака (реализация сценария воздействия). При этом нарушителем могут применяться как пассивное, так и активное воздействие на элементы ЗМС. Под пассивным воздействием понимается воздействие, которое не оказывает непосредственного влияния на работу элементов ЗМС, но может привести к нарушению безопасности обрабатываемой в ней информации. Примером пассивного воздействия на ЗМС служит «прослушивание» канала связи в сети (анализ сетевого трафика). Под активным воздействием понимается воздействие, нарушающее безопасность циркулирующей в сети информации и оказывающее непосредственное влияние на работу элементов ЗМС. Примерами такого воздействия могут служить изменение конфигурации элементов ЗМС, искажение, уничтожение информации.

Политика безопасности

Управление информационной безопасностью целесообразно осуществлять на уровнях оперативно-технического и технологического управления АСУС ЗМС. При этом используются механизмы управления услугами, сетью и сетевыми элементами, предусмотренные моделью TMN. Такой подход позволяет реализовать единое сквозное управление информационной безопасностью, взаимоувязанное с сетевым управлением в рамках единой системы управления ЗМС.

Основными задачами ПсЗИ ЗМС является своевременное выявление потенциальных угроз ресурсам ЗМС (мониторинг угроз), идентификация пользователей, сервисов и приложений на основе системы открытых ключей, защита ресурсов сети от несанкционированного доступа и модификации, протоколирование отправки и получения сообщений, а также всех событий в ЗМС в части НСД, криптографическое закрытие информации и управление ключевой информацией.

Задача управления информационной безопасностью в ЗМС может быть сформулирована следующим образом.

Пусть $\mathbf{S}\langle \mathbf{A}, \mathbf{Z}, \mathbf{G}, \mathbf{R} \rangle$ – требуемое состояние ЗМС в части обеспечения сетевой безопасности, где $\mathbf{A}$ – состояния сетевых элементов; $\mathbf{Z}$ – состояние топологии сети; $\mathbf{G}$ – состояние сетевых информационных фондов и информационных фондов телематических услуг; $\mathbf{R}$ – требуемые телекоммуникационные ресурсы.

Пусть $\overline{\mathbf{U}}$ – вектор деструктивных воздействий на ЗМС. В результате действия $\overline{\mathbf{U}}$ состояние ЗМС станет $\hat{\mathbf{S}}\langle \hat{\mathbf{A}}, \hat{\mathbf{Z}}, \hat{\mathbf{G}}, \hat{\mathbf{R}} \rangle$, т. е.:

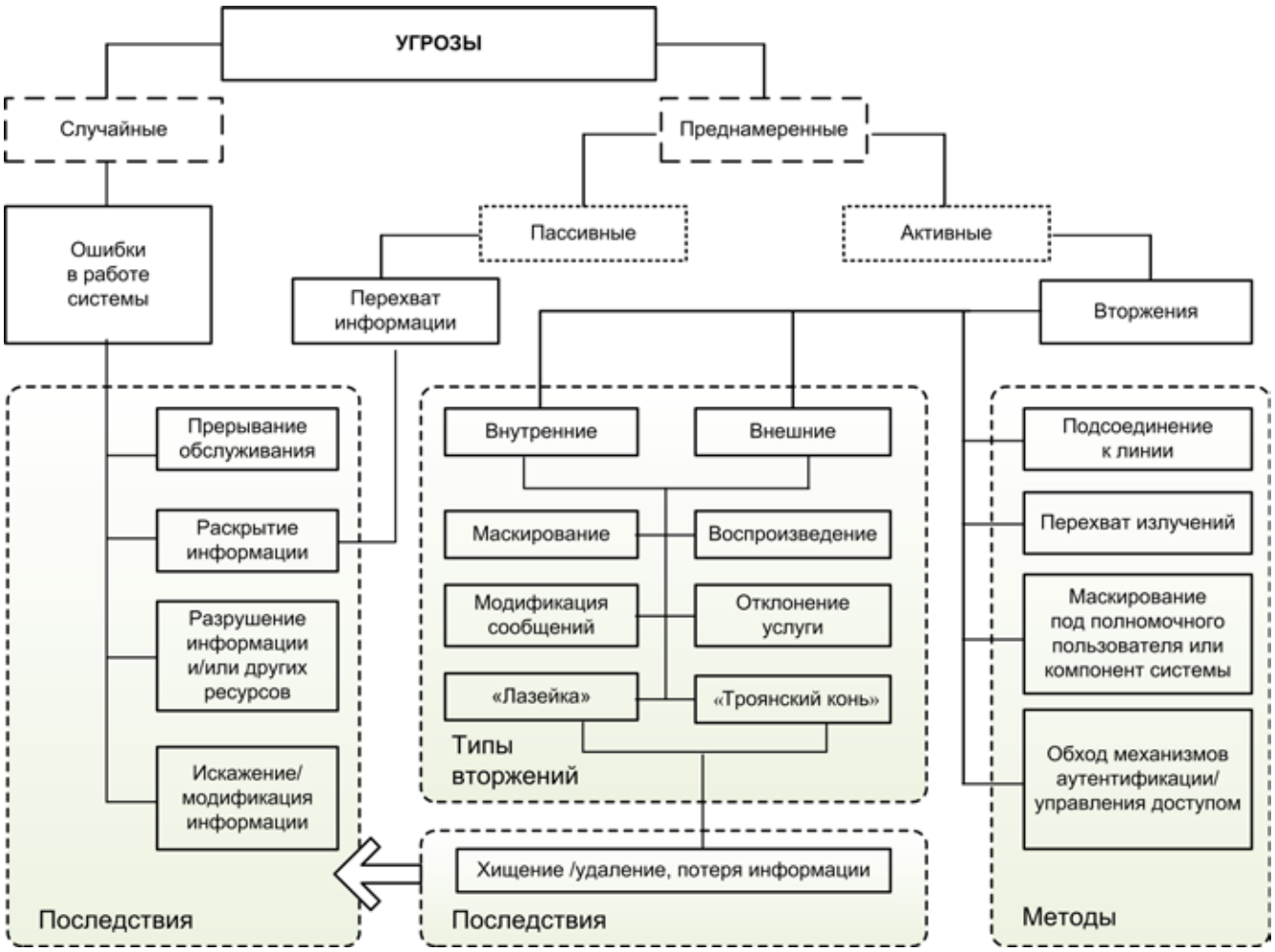

Рис. 3. Модель угроз информации в ЗМС

Таблица 3

Распределение сервисов безопасности по уровням ЭМВОС

Сервисы безопасности	Уровни ЭМВОС						
	1	2	3	4	5	6	7
Аутентификация			+	+			+
Управление доступом			+	+			+
Конфиденциальность соединения	+	+	+	+		+	+
Конфиденциальность вне соединения		+	+	+		+	+
Избирательная конфиденциальность						+	+
Конфиденциальность трафика	+		+				+
Целостность с восстановлением				+			+
Целостность без восстановления			+	+			+
Избирательная целостность							+
Целостность вне соединения			+	+			+
Безотказность							+

$$\hat{\mathbf{S}}\left\langle \hat{\mathbf{A}}, \hat{\mathbf{Z}}, \hat{\mathbf{G}}, \hat{\mathbf{R}} \right\rangle = \mathbf{S}\left\langle \mathbf{A}, \mathbf{Z}, \mathbf{G}, \mathbf{R} \right\rangle + \theta\left(\overline{\mathbf{U}}\right),$$

где $\theta\left(\overline{\mathbf{U}}\right)$ – мера рассогласования.

Требуется сформировать вектор управления $\overline{\mathbf{V}}$ такой, чтобы выполнялось условие $\overline{\Delta} = \left\| \hat{\mathbf{S}} - \mathbf{S} \right\| \to \mathbf{min}$, при этом $\overline{\mathbf{\Delta}} = \varphi(\overline{\mathbf{V}}, \mathbf{t})$, $t \le t_{треб}$, т. е. необходимо минимизировать рассогласование состояния ЗМС за время, не больше требуемого, которое определяется временем актуальности защищаемой информации.

Данная задача относится к классу задач многоуровневой оптимизации. Наиболее эффективное ее решение можно получить с помощью методов динамического программирования. Технически решение задачи обеспечивается применением сервисов и механизмов безопасности.

Сервисы и механизмы безопасности ЗМС

Для ЗМС характерны следующие услуги (сервисы) безопасности:

1) аутентификация (обеспечивает взаимоопознавание партнеров по общению и идентификацию источника данных);

2) управление доступом (позволяет ограничить режимы взаимодействия сетей и обеспечить сокрытие информации о структуре и особенностях сети путем фильтрации пакетов и сообщений на сетевом, транспортном и прикладном уровнях по соответствующим группам служебных атрибутов, извлекаемых из этих сообщений);

3) конфиденциальность и целостность потока данных в режиме с установлением и без установления соединения (криптографическая защита

Таблица 4

Взаимосвязь сервисов и механизмов безопасности ЗМС

Механизмы / Сервисы безопасности	Шифрование	Электронная подпись	Управление доступом	Целостность	Аутентификация	Дополнение трафика	Управление маршрутизацией	Нотаризация
Аутентификация партнеров	+	+			+			
Идентификация источника	+	+						
Управление доступом			+					
Конфиденциальность	+						+	
Избирательная конфиденциальность	+							
Конфиденциальность трафика	+					+	+	
Целостность соединения	+			+				
Целостность вне соединения	+	+		+				
Безотказность		+		+				+

данных на физическом, канальном, сетевом, транспортном и прикладном уровнях);

4) целостность соединений с обеспечением и без обеспечения возможности восстановления (функции, позволяющие обнаружить любые изменения данных, передаваемых в рамках установленных соединений);

5) безотказность, или защита от отказа источника или получателя сообщений (функция, основанная на использовании криптографических протоколов, обеспечивающих гарантии отправки/прочтения сообщений для их получателя/источника).

В таблице 3 указаны уровни эталонной модели взаимодействия открытых систем (ЭМВОС), на которых могут быть реализованы указанные выше сервисы безопасности.

Для большинства задач, предъявляющих повышенные требования к сетевой безопасности, необходимо минимизировать доверенную функциональность оконечных систем. Уровневая структура ЗМС должна выбираться таким образом, чтобы минимизировать зависимость от допущений о режимах функционирования и пользователях абонентов сети.

Для реализации функций безопасности могут использоваться следующие механизмы защиты информации и их комбинации [8]: шифрование, электронная цифровая подпись, управление доступом, контроль целостности данных, аутентификация, дополнение трафика, управление маршрутизацией, нотаризация.

В таблице 4 сведены основные сервисы и механизмы безопасности ЗМС. Данная таблица показывает, какие механизмы или их комбинации могут использоваться для реализации того или иного сервиса.

Эффективная реализация перечисленных выше концептуальных положений информационной безопасности ЗМС предполагает создание подсистемы защиты информации, компоненты которой распределены по элементам ЗМС и управляются из единого центра. Основой ПсЗИ должны быть сертифицированные аппаратно-программные средства и руководства по эксплуатации, разработанные в соответствии с российским законодательством, ГОСТ, руководящими и нормативными документами ФСТЭК, Минобороны и ФСБ в области защиты информации (обеспечения информационной безопасности).

СПИСОК ЛИТЕРАТУРЫ

1. Концептуальные основы обеспечения устойчивости сетей связи / Л.К. Киселев [и др.] // Электросвязь. – 1994. – № 2. – С. 23–26.

2. Вторичные сети военной связи / А.В. Лисовский [и др.]. – М. : Изд-во Минобороны, 2002. – 463 с.

3. ГОСТ РВ 5819-112-2008. ОАЦСС ВС РФ. Общие требования к автоматизированной системе управления связью.

4. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – М. : Изд-во стандартов, 2006.

5. ГОСТ Р ИСО/МЭК 15408-1-2008. Информационная технология. Методы и средства обеспечения безопасности информации. Критерии оценки безопасности информационных технологий. Часть I. Введение и общая модель. – М. : Стандартинформ, 2009.

6. Руководящий документ Гостехкомиссии России. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. – М. : Военное изд-во, 1992. – 12 с.

7. ГОСТ Р ИСО 7498-2-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. – М. : ИПК Издательство стандартов, 1999.

8. Коняев И., Беляев А. Информационная безопасность предприятия. – СПб. : БХВ-Петербург, 2003. – 752 с.