УДК 681.142.33:681.14

АГЕЕВ С.А., САЕНКО И.Б.

УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ ЗАЩИЩЕННЫХ МУЛЬТИСЕРВИСНЫХ СЕТЕЙ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Агеев С.А., Саенко И.Б. **Управление безопасностью защищенных мультисервисных сетей специального назначения.**

Аннотация. В статье рассматриваются концептуальные основы автоматизации управления безопасностью защищенных мультисервисных сетей специального назначения (ЗМС СН). Обсуждается пирамидальная модель управления ЗМС СН, основные функциональные задачи управления ЗМС. Приводится декомпозиция задачи защиты информации в ЗМС. Дана формальная постановка задачи управления безопасностью ЗМС СН. Рассматриваются угрозы безопасности, ее сервисы, их распределение по уровням эталонной модели взаимодействия открытых систем (ЭМВОС), взаимодействие функций и механизмов безопасности.

Ключевые слова: защищенная мультисервисная сеть, модель угроз, телематические сетевые услуги, автоматизация управления, модель сети управления телекоммуникациями (TMN-модель).

Ageev S.A., Saenko I.B. **Security management of protected multi-service networks for special purposes.**

Abstract. The article examines the conceptual framework of automation safety management of protected multi-service networks for special purposes (PMN SP). It discussed the pyramid model of management of PMN SP, major functional management tasks of PMN. The decomposition of the problem of the information security in PMN is given. A formal statement of the task of safety management PMN SP is presented. The security threats, security services, their distribution by level of model OSI, the interaction functions and security mechanisms are considered.

Keywords: protected multi-service network, the threat model, telematic network services, automation control, TMN model.

1. Введение. Прогресс развития общества в настоящее время во многих его областях жизни и деятельности невозможен без применения автоматизированных систем управления (АСУ) различного назначения, в том числе и специального (СН). АСУ СН активно внедряются и применяются в органах государственного и административного управления, в силовых министерствах и ведомствах, на критически важных промышленных объектах и т.д.

Для обоснованного принятия управленческих решений необходимо оперативно обрабатывать большой объем разнородной информации и в короткое время доводить выработанное решение до многих исполнителей. Вследствие этого появилась объективная необходимость объ-

единения различных информационных ресурсов в единое информационное пространство. Одним из основных системообразующих элементов подобного подхода являются защищенные мультисервисные сети (ЗМС). Поэтому разработка концептуальных положений автоматизации управления ЗМС, включая управления сетевой безопасностью, является актуальной научно-технической проблемой.

2. Концепция управления защищенной мультисервисной сетью. ЗМС является территориально распределенной гетерогенной телекоммуникационной системой, предоставляющей пользователям набор телематических услуг с заданным качеством. К основным телематическим услугам можно отнести файловый обмен, электронную почту, IP-телефонию, мультимедийные конференции, передачу командно-сигнальной информации и т.д. ЗМС создается на основе общих для всех ее элементов системных, функциональных и технических принципов функционирования и управления как единая сеть, структура которой приведена на рис. 1.

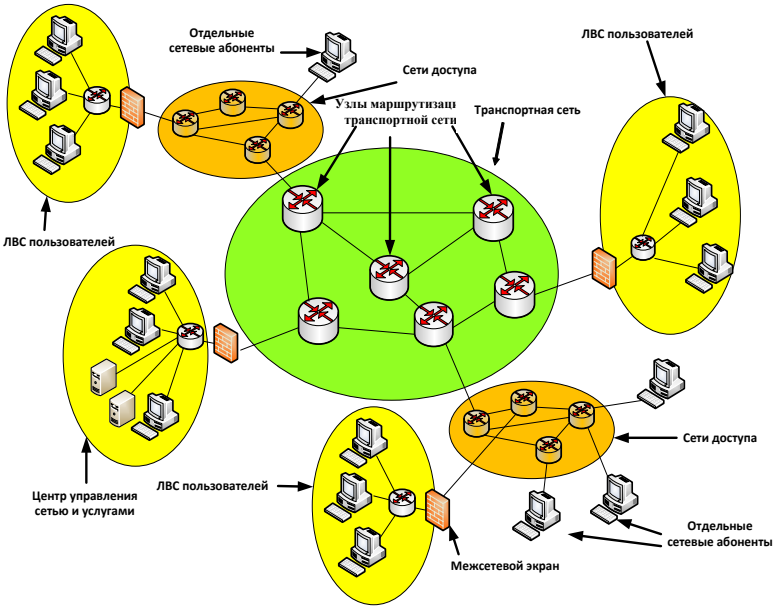

Рис. 1. Структура защищенной мультисервисной сети.

Для эффективного решения возложенных на нее задач ЗМС СН должна иметь АСУ связью (АСУС). АСУС предназначена для управления обеспечением требуемого качества услуг связи в интересах удовлетворения информационных потребностей пользователей за счет автоматизированного поддержания на необходимом уровне конфигурации сети, ее эксплуатационных характеристик, рационального использования ресурса системы связи, защиты информации, взаимодействия с другими телекоммуникационными системами.

Основные функциональные задачи АСУС ЗМС состоят в управлении следующими элементами:

1) конфигурацией (планированием, формированием и развитием системы, установкой и вводом в эксплуатацию нового оборудования, установлением и изменением соединений между элементами системы, предоставлением ресурсов пользователям и т.д.);

2) устранением неисправностей (обнаружением, локализацией, регистрацией и устранением неисправностей и т.д.);

3) качеством передачи информации (сбором, обработкой, регистрацией, хранением и отображением статистических данных о функционировании сети и ее элементов, анализом качественных показателей и т.д.);

4) защитой информации (обеспечением конфиденциальности и целостности передаваемой информации, выдачей сигналов тревоги при несанкционированном доступе к информации, блокированием скомпрометированного элемента сети и т.д.);

5) использованием ресурса (сбором, обработкой, регистрацией, хранением и отображением данных о выделенном в интересах пользователей ресурсе, предоставляемых услугах связи).

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.

АСУС ЗМС должна быть стационарно-мобильной, организационно и функционально самостоятельной, многоуровневой, открытой человеко-машинной системой, обеспечивающей управление объединенным ресурсом автоматизации в интересах АСУ СН.

В качестве системообразующей основы построения АСУС ЗМС целесообразно принять концепцию сети управления телекоммуникациями

(*TMN — Telecommunication Management Network*) [1]. 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 связи и обеспечить их требуемое качество.

АСУС должна быть самостоятельной выделенной системой, взаимодействующей с цифровыми транспортными сетями и сетями доступа по стандартным интерфейсам для своевременного получения информации об их состоянии и управляемости.

Концептуальная декомпозиция уровней (видов) управления и их соответствие с уровнями пирамидальных моделей АСУС ЗМС и модели *TMN* приведены на рис. 2.

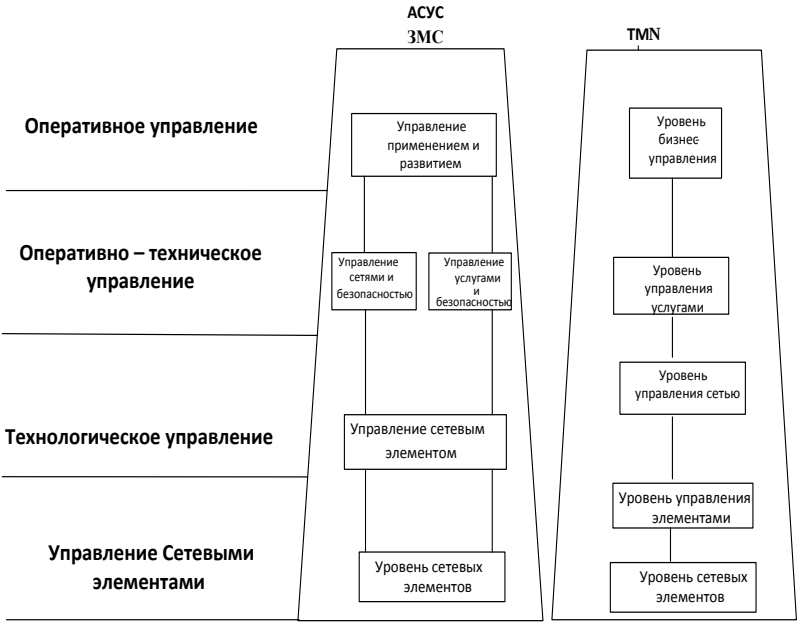

Рис. 2. Соотношение пирамидальных моделей управления по уровням.

Одной из ключевых задач, решаемых при построении и функционировании ЗМС, является управление безопасностью, сводящееся к защите обрабатываемой информации и управлению подсистемой защиты информации.

Целесообразно управлять безопасностью на следующих уровнях:

— оперативно-техническом,

— услуг и сети,

— сетевых элементов модели TMN.

Такой подход позволит реализовать единое сквозное управление безопасностью, взаимоувязанное с сетевым управлением, как единую систему управления. На рис. 3 приведены процессы управления и сетевого мониторинга, которые соответствуют функциональной декомпозиции и целевому предназначению ЗМС.

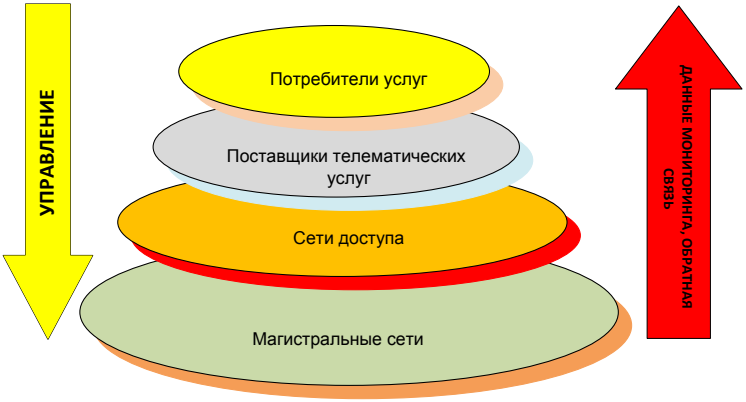

Рис. 3. Процессы управления и мониторинга в ЗМС.

Существенными особенностями ЗМС как объектов управления являются:

— территориальная рассредоточенность их элементов;

— наличие информационных ресурсов различной степени доступности (и общедоступных, и ограниченного доступа) и различного уровня конфиденциальности;

— наличие удаленных пользователей, использующих открытые каналы сетей передачи данных общего пользования для доступа к ин-

формационным ресурсам отдельных локальных вычислительных сетей, входящих в состав АСУ СН.

В связи с этим построение эффективной системы защиты информации в ЗМС требует, с одной стороны, подробного анализа используемых в ней технических и программных средств, видов обрабатываемой информации и принятых технологических схем ее преобразования, а с другой — анализа возможностей существующих средств защиты информации, используемых в них механизмов, степени применимости для решения тех или иных задач защиты.

3. Концепция управления безопасностью информации в защищенной мультисервисной сети. Существует ряд подходов к декомпозиции задачи защиты информации в ЗМС СН. Различие подходов заключается в признаке, используемом для выделения направлений защиты информации. В частности, один из известных подходов в качестве признака использует вид угрозы защищаемой информации [2]. При этом выделяются направления защиты информации от следующих угроз:

1) разглашения, под которым понимается несанкционированное доведение защищаемой информации до неконтролируемого числа ее получателей;

2) несанкционированного доступа, под которой понимается получение защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником (владельцем) информации прав или правил доступа к ней;

3) разведки, под которой понимается деятельность по получению защищаемой информации с применением методов технических средств разведки, агентуры и т.д.;

4) несанкционированного воздействия, под которым понимается воздействие на защищаемую информацию с нарушением установленных прав и/или правил на ее изменение, приводящее к искажению, уничтожению, копированию, блокированию доступа к ней, а также к утрате, уничтожению или сбою функционирования носителя информации;

5) непреднамеренного воздействия, под которым понимается воздействие на защищаемую информацию ошибок пользователя, сбоев технических и программных средств информационных систем, а также природных явлений или иных нецеленаправленных на изменение ин-

формации воздействий, связанных с функционированием технических средств, систем или с деятельностью людей, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Другим подходом к декомпозиции задачи защиты информации в ЗМС является подход, предлагаемый в работе [3]. В соответствии с ним направления защиты информации формируются согласно возможным способам (каналам) реализации угроз информации. При этом выделяются следующие направления исследования проблемы безопасности информации: радиотехническое; побочные электромагнитные излучения и наводки; акустическое; оптическое; физический доступ; несанкционированный доступ (НСД).

При этом НСД определяется как доступ к информации, нарушающий установленные правила разграничения доступа с использованием штатных средств, предоставляемых АСУ СН.

Под защитой информации в ЗМС СН понимается регулярное использование в них средств и методов, принятие мер и осуществление мероприятий с целью обеспечения требуемой безопасности информации, под которой понимается состояние защищенности информации и средств ее преобразования и передачи от возможных угроз. Для реализации этой цели в ЗМС создается система защиты информации, которая представляет собой комплекс технических, программных средств защиты, направленных на обеспечение безопасности информации [4].

Важнейшими начальными этапами построения системы защиты информации ЗМС СН являются: анализ ЗМС и информационных ресурсов, подлежащих защите; определение и анализ угроз безопасности информации; построение модели угроз. Классификация угроз безопасности ЗМС СН приведена в табл. 1.

Результаты анализа структурных и функциональных особенностей ЗМС СН позволяют сформировать перечень видов угроз безопасности информации (табл. 2).

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

Таблица 1. **Классификация угроз безопасности информации в ЗМС СН**

Классификационный признак	Характеристика угроз
Источник угрозы	Человеческий фактор Аппаратные или программные средства Окружающая среда
Принадлежность источника угрозы	Внутренний
	Внешний
Направленность угрозы	Конфиденциальность
	Целостность
	Доступность
Тип объекта угрозы	Технологическая информация
	Пользовательская информация
Характер происхождения угрозы	Преднамеренная
	Непреднамеренная
Предпосылки возникновения	Недостаточность элементов системы: — качественная, — количественной
Длительность воздействия	Постоянная
	Периодическая

Таблица 2. **Виды угроз безопасности информации в ЗМС**

Угроза		Характеристика вида угроз				Возможные зависимости (см. номер угрозы)
Номер	Вид	ПИУ	ТОУ	НУ	ХПУ	
1. При передаче информации						
1.1	Перехват передаваемой информации	Внш	П, Т	К	Пр	1.6
1.2	Удаление передаваемых сообщений	Внш	П, Т	Ц, Д	Пр, Сл	1.1
1.3	Переупорядочивание сообщений	Внш	П, Т	Ц, Д	Пр, Сл	1.1
1.4	Дублирование сообщений	Внш	П, Т	Ц	Пр	1.1
1.5	Вставка сообщений	Внш	П, Т	Ц	Пр	1.1
1.6	Навязывание ложного маршрута	Внш	П, Т	Ц, Д	Пр	1.1
1.7	Подмена адреса источника передаваемой информации	Внш	П, Т	Ц	Пр	1.6
1.8	Модификация сообщений	Внш	П, Т	Ц	Пр	1.1

Продолжение табл. 2.

Угроза		Характеристика вида угроз				Возможные зависимости (см. номер угрозы)
Номер	Вид	ПИУ	ТОУ	НУ	ХПУ	
2. При обработке и хранении информации						
2.1	Несанкционированное получение полномочий в системе	Внш, Внт	Т	К	Пр	1.6, 2.2, 2.3, 2.5
2.2	Подбор ключевой информации и информации аутентификации	Внш	Т	К	Пр	
2.3	Чтение, изменение, уничтожение значений параметров конфигурации элементов системы	Внш, Внт	Т	К, Ц, Д	Пр, Сл	2.1, 2.2
2.4	Обмен информацией между абонентами без применения средств защиты	Внт	П, Т	К	Пр, Сл	2.3
2.5	Передача информации пользователям, не имеющим к ней доступа	Внт	П, Т	К	Пр, Сл	2.3
2.6	Отказ источника/ получателя информации от передачи/получения информации	Внт	П, Т	Д, Ц	Пр, Сл	
2.7	Перерасход ресурсов общего пользования	Внш, Внт	П, Т	Д	Пр	

Примечание: ПИУ — принадлежность источника угрозы; ТОУ — тип объекта угрозы; НУ — направленность угрозы; ХПУ — характер происхождения угрозы угрозы; Внш и Внт — соответственно внешняя и внутренняя угроза; П, Т, К, Ц, и Д — угроза информации соответственно: пользовательской, технологической, ее конфиденциальности, целостности и доступности; Пр — преднамеренная угроза; Сл — случайная угроза.

Действия нарушителя, осуществляемые им в непосредственном контакте с ЗМС, рассматриваются как атака (реализация сценария воздействия). При этом нарушитель может применять и пассивное, и активное воздействие на элементы ЗМС. Под *пассивным* понимается воздействие, которое не оказывает непосредственного влияния на работу элементов ЗМС, но может привести к нарушению безопасности обрабатываемой в ней информации. Пример пассивного воздействия на ЗМС — «прослушивание» канала связи в сети (анализ сетевого тра-

фика). Под *активным* понимается воздействие, нарушающее безопасность циркулирующей в ней информации и оказывающее непосредственное влияние на работу элементов ЗМС.

Примерами такого воздействия могут служить изменение конфигурации элементов ЗМС, искажение, уничтожение информации.

Таким образом, основными задачами подсистемы управления безопасностью ЗМС являются [5]:

— своевременное выявление потенциальных угроз ресурсам ЗМС (мониторинг угроз);

— выработка соответствующих политик безопасности;

— выработка соответствующих воздействий на элементы ЗМС с целью предотвратить деструктивные попытки со стороны потенциального нарушителя;

— ведение журнала всех событий в ЗМС в части НСД;

— управление ключевой информацией;

— обеспечение целостности информации;

— поддержание высокой степени доверия к системе обеспечения информационной безопасности и т.д.

Формально задача управления безопасностью 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 (состояние каналов); $\mathbf{G}$ — состояние сетевых информационных фондов и информационных фондов телематических услуг; $\mathbf{R}$ — требуемые телекоммуникационные ресурсы.

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

$$\hat{\mathbf{S}}\langle \hat{\mathbf{A}},\hat{\mathbf{Z}},\hat{\mathbf{G}},\hat{\mathbf{R}} \rangle = \mathbf{S}\langle \mathbf{A},\mathbf{Z},\mathbf{G},\mathbf{R} \rangle \oplus \theta\left(\bar{\mathbf{U}}\right), \qquad (1)$$

где $\theta\left(\bar{\mathbf{U}}\right)$ — некоторая функция от вектора $\bar{\mathbf{U}}$, изменяющая состояние ЗМС; $\oplus$ — действие этой функции на $\mathbf{S}\langle \mathbf{A},\mathbf{Z},\mathbf{G},\mathbf{R} \rangle$ (не обязательно аддитивное).

Требуется сформировать вектор управления $\bar{\mathbf{V}}$, такой, чтобы выполнялось условие

$$\bar{\Delta} = \left\| \hat{\mathbf{S}} - \mathbf{S} \right\| \to \min . \qquad (2)$$

При этом $\bar{\Delta} = \varphi\left(\bar{\mathbf{V}}, t\right)$, $t \le t_{\text{треб}}$, т.е. необходимо минимизировать рассогласование состояния ЗМС за период времени не больше заданного $t_{\text{треб}}$, который взаимосвязан с периодом времени актуальности защищаемой информации. Таким образом, условие (2) должно выполняться при следующих ограничениях:

$$\begin{cases} \mathbf{B} \Rightarrow \max \\ \mathbf{R} \ge \mathbf{R}_{\text{òð}} \\ \mathbf{F(G)} = \mathbf{F(G}_{\text{òð}}\mathbf{)} \\ \mathbf{F(I)} = \mathbf{F(I}_{\text{èñõ}}\mathbf{)} \\ \mathbf{W} \Rightarrow \max \\ t \le t_{\text{òð}} \end{cases}, \qquad (3)$$

где **B** — состояние сетевой безопасности, **W** — степень доверия к информационной безопасности, **F(G)** — целостность сетевых информационных фондов и информационных фондов телематических услуг, **F(I)** — целостность передаваемой информации.

Отметим, что данная задача относится к классу задач выпуклого программирования [6].

Для ЗМС СН определены следующие функции (сервисы) безопасности:

1) аутентификация (обеспечивает аутентификацию партнеров по общению и аутентификацию 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 соединения и без него (криптографическая защита данных на физическом, канальном, сетевом, транспортном и прикладном уровне);

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

5) безотказность, или защита от отказа источника или получателя сообщений (основана на использовании криптографических протоколов, цель которых состоит в обретении надежных гарантий отправки/прочтения сообщений для их получателя/источника).

В табл. 3 указаны уровни эталонной модели взаимодействия открытых систем (ЭМВОС), на которых могут быть реализованы указанные функции безопасности. Отметим, что прикладные процессы в принципе могут взять на себя поддержку всех защитных сервисов.

Таблица 3. **Распределение функций безопасности ЗМС по уровням ЭМВОС**

Функция безопасности	Уровень						
	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							+

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

Для реализации функций безопасности могут использоваться следующие механизмы защиты информации и их комбинации [7]: шифрование; электронная цифровая подпись; управление доступом; кон-

троль целостности данных; аутентификация; дополнение трафика; управление маршрутизацией; нотаризация.

Механизм нотаризации служит для заверки таких коммуникационных характеристик, как целостность, время, личности отправителя и получателей. Заверение обеспечивается надежной третьей стороной, которая обладает достаточной информацией, чтобы ее заверениям можно было доверять. Обычно нотаризация опирается на механизм электронной подписи.

В табл. 4 сведены основные функции и механизмы безопасности ЗМС СН. Данная таблица показывает, какие механизмы или их комбинации могут использоваться для реализации той или иной функции.

Таблица 4. **Взаимосвязь функций и механизмов безопасности ЗМС СН**

Функция безопасности	Механизм безопасности							
	Шифрование	Электронная подпись	Управление доступом	Целостность	Аутентификация	Дополнение трафика	Управление маршрутизацией	Нотаризация
Аутентификация партнеров	+	+			+			
Аутентификация источника	+	+						
Управление доступом			+					
Конфиденциальность	+						+	
Избирательная конфиденциальность	+							
Конфиденциальность трафика	+					+	+	
Целостность соединения	+			+				
Целостность вне соединения	+	+		+				
Безотказность		+		+				+

4. Заключение. Эффективная реализация перечисленных функций безопасности возможна только на основе применении сбалансированной комбинации автоматизированного и автоматического управления безопасностью ЗМС СН.

Для реализации указанных принципов, которые позволят обеспечить комплексное и эффективное управление безопасностью, необходима разработка соответствующих моделей и методов построения и функционирования ЗМС СН.

Литература

1. *Гребешков А. Ю.* Стандарты и технологии управления сетями связи. М.: Эко-Трендз, 2003. 288 с.
2. ГОСТ Р 50922—96. Защита информации. Основные термины и определения. М.: Изд-во стандартов, 1996.
3. Руководящий документ Гостехкомиссии России. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. М.: Военное изд-во, 1992. 12 с.
4. *Коняев И., Беляев А.* Информационная безопасность предприятия. СПб.: БХВ-Петербург, 2003. 752 с.
5. ГОСТ Р ИСО/МЭК 15408-1—2002, 15408-2—2002, 15408-3—2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 1–3. М.: Изд. Госстандарта России.
6. *Босс В.* Лекции по математике. Т. 7. Оптимизация: Учебное пособие / Изд. 2-е, стереотипное. М: КомКнига, 2007. 216 с.
7. *Соколов А., Степанюк О.* Защита от компьютерного терроризма. Справочное пособие. СПб.: БХВ-Петербург Арлит, 2002. 496 с.

Агеев Сергей Александрович — канд. техн. наук, доцент; доцент кафедры информационных систем Санкт-Петербургского государственного университета информационных технологий, точной механики и оптики. Область научных интересов: проектирование телекоммуникационных систем. Число научных публикаций — 75. serg123_61@mail.ru; ВАС, Тихорецкий проспект, 3, Санкт-Петербург, 194064, РФ; р.т. +7(812)247-9842, факс +7(812)247-9442

Ageev Sergey Aleksandrovich — PhD in Technical, associate professor; associate professor of the branch of the information system of St. Petersburg State University of Information Technologies, Mechanics and Optics. Research interests: design of telecommunication systems. The number of publications — 75. serg123_61@mail.ru; MASC, Tihoretsky Prospekt, 3, St. Petersburg, 194064, Russia; office phone +7(812)247-9842, fax +7(812)247-9842.

Саенко Игорь Борисович — д-р техн.наук, проф.; в. н. с. лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации РАН (СПИИРАН). Область научных интересов: автоматизированные информационные системы, информационная безопасность, обработка и передача данных по каналам связи, теория моделирования и математическая статистика, теория информации. Число научных публикаций — 220. ibsaen@mail.ru; СПИИРАН, 14-я линия В.О., 39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328-2642, факс +7(812)328-4450.

Saenko Igor Borisovich — Ph.D., Doctor of Technical Sciences, professor; leading research scientist of laboratory of computer network security of Saint-Petersburg Institute for Information and Automation of RAS (SPIIRAS). Research interests: automated information systems, information security, processing and transfer of data on data links, theory of modeling and mathematical statistics, information theory. The number of publications — 220. ibsaen@mail.ru; SPIIRAS, 14th line, 39, St. Petersburg, 199178, Russia; office phone +7(812) 328-2642, fax +7(812)328-4450.

Рекомендовано лабораторией проблем компьютерной безопасности, заведующий лабораторией д-р техн. наук, проф. И.В. Котенко.
Статья поступила в редакцию 10.12.2010.

РЕФЕРАТ

Агеев С.А., Саенко И.Б. **Управление безопасностью защищенных мультисервисных сетей специального назначения.**

В статье рассматриваются концептуальные вопросы управления безопасностью защищенных мультисервисных сетей специального назначения (ЗМС СН).

ЗМС СН является территориально распределенной гетерогенной телекоммуникационной системой, предоставляющей пользователям набор телематических услуг с заданным качеством. По своей структуре она является единой сетью, объединяющей элементы на общих для них системных, функциональных и технических принципах функционирования и управления.

Для эффективного решения возложенных на нее задач ЗМС СН имеет автоматизированную систему управления связью (АСУС), основные функциональные задачи которой состоят в управлении конфигурацией, устранением неисправностей, качеством передачи информации, защитой информации и использованием ресурса. При построении АСУС предлагается использовать концепцию *TMN*.

Декомпозиция задачи защиты информации в ЗМС СН позволила выделить направления и этапы ее решения. Важнейшим начальным этапом является выявление угроз безопасности. Приведенная в статье классификация этих угроз позволила уточнить функции АСУС по управлению безопасностью ЗМС и сформулировать формальную постановку задачи управления безопасностью ЗМС. Исходными данными задачи являются состояние сетевых элементов, топология сети, состояние сетевых информационных фондов, требуемые телекоммуникационные ресурсы. Требуется найти такой вектор управления, при котором отклонение состояния ЗМС от требуемого было бы минимальным при ограничениях на ресурсы, целостность информационных фондов и время рассогласования состояния.

Определены основные сервисы безопасности ЗМС СН, включающие аутентификацию, управление доступом, конфиденциальность и целостность потока данных, целостность соединений и безотказность. Приведено распределение этих сервисов по уровням ЭМВОС.

Приведены механизмы защиты информации и их комбинации, которые могут использоваться для реализации сервисов безопасности: шифрование, управление доступом, контроль целостности трафика, аутентификации, управления маршрутизацией, нотаризация. Показано, какие механизмы могут использоваться для реализации тех или иных сервисов безопасности ЗМС СН.

SUMMARY

Ageev S.A., Saenko I.B. **Network key formation protocol on open communication channels with errors.**

The article deals with conceptual issues of safety management of protected multi-service networks for special purposes (PMN SP).

PMN SP is a geographically distributed heterogeneous telecommunication system that provides users with a set of telematic services with the specified quality. In its structure, it is a single network that combines the elements on their common systemic, functional and technical principles of operation and management. To effectively address its tasks PMN SP has an automated communication control system (ACCS), the main functional problem which consists in managing the configuration, troubleshooting, quality of communication, information protection and resource use. In the construction of ACCS we are encouraged to use the concept of TMN.

Decomposition of the task of information security in PMN SP made possible to identify trends and stages of the solution. The most important initial step is to identify security threats. The classification of security threats, made in the article, helped to clarify the function of ACCS on PMN security management and formulate a formal statement of the problem of PMN safety management. The initial data of this problem are the status of network elements, network topology, network state information collections required by telecommunication resources. We want to find a vector control, in which the deviation from the desired state of PMN would be minimal under the constraints on resources, the integrity of information assets and mismatch condition time.

The basic security services of PMN SP include authentication, access control, confidentiality and integrity of the data flow, seal integrity and reliability. The distribution of these services by levels of OSI model is shown.

The article shows the mechanisms for the protection of information and combinations thereof, which may be used to implement security services: encryption, access control, integrity control traffic, authentication, routing control, and notarization. It shows what mechanisms can be used for the implementation of these security services of PMN SP.