ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 621.392

СРАВНЕНИЕ РАЗЛИЧНЫХ ТЕХНОЛОГИЙ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ ОГРАНИЧЕННЫХ ПОЛЬЗОВАТЕЛЕЙ В АСПЕКТЕ ОБЕСПЕЧЕНИЯ ИБ ОТ УГРОЗ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

В.А. Матвеев, руководитель научно-технического комплекса факультета ИУ, зав. каф. «Информационная безопасность» МГТУ им. Н.Э. Баумана, д.т.н., проф.
Р.А. Бельфер, доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, к.т.н., с.н.с.; a.belfer@yandex.ru

Ключевые слова: *информационная безопасность, сеть передачи данных, угроза, виртуальные частные сети (Virtual Private Routed Network, VPN), сети ограниченных пользователей, коммутируемый виртуальный канал, постоянный виртуальный канал, коммутация пакетов, центр коммутации пакетов.*

Введение. Настоящая работа посвящена исследованию метода сравнения технологий сетей передачи данных в плане обеспечения информационной безопасности (ИБ). Рассмотрению подлежат сети, в которых обычно предъявляются более высокие требования к информационной безопасности, чем в сетях связи общего пользования (ССОП). Речь идет о технологических сетях и сетях специального назначения (в соответствии с классификацией сетей связи, данной в ст. 12 ФЗ «О связи» [1]). Поскольку настоящая работа не относится непосредственно ни к одной из этих сетей, будем называть их, как предложено в [2], сетями ограниченных пользователей (ОгП).

Общие положения, касающиеся назначения этих сетей, также изложены в ФЗ «О связи». Особенностью многих сетей ОгП является использование в них отечественного оборудования. Задачам информационной безопасности сетей ОгП большое внимание уделяет Российская корпорация средств связи (РКСС) [3]. Обеспечением информационной безопасности таких сетей связи в энергетическом комплексе очень серьезно занимаются китайские ученые [4–6].

В сетях ОгП и ССОП некоторые характеристики качества обслуживания могут не совпадать. Эти характеристики в сетях ОгП задаются в требованиях заказчика и определяются конкретными функциями сети. В технологической сети ОгП такой характеристикой может быть, например, вероятность доставки сообщения управления определенной длины. Такая характеристика включает выполнение ограничений по задержке этих сообщений, отказы в установлении соединения и др. Защита от некоторых угроз ИБ в сети ОгП также является одним из факторов, определяющих вероятность доставки сообщения в пункт назначения.

Анализируемые угрозы несанкционированного доступа в сетях ОгП. Определим угрозы в сетях ОгП, анализ возможных механизмов защиты которых предстоит провести в настоящей работе, чтобы сравнить технологии сетей передачи данных в части обеспечения ИБ. Определим архитектуру ИБ сети, для которой решается данная задача. Для этого используем общие положения сетевой архитектуры безопасности, изложенные в Рекомендации Международного союза электросвязи ITU-T X.805 [7]. Согласно этому документу, ИБ сетей связи классифицируется по уровням безопасности и плоскостям безопасности. Уровни безопасности относятся к оборудованию сети связи, а плоскость безопасности – к функциям сети связи.

Определено три уровня безопасности: уровень безопасности инфраструктуры (Infrastructure Security), услуг (Services Security) и приложений (Applications Security). Уровень безопасности инфраструктуры относится к основным устройствам сети связи. Примерами таких устройств являются коммутаторы, каналы связи между ними.

Установлено три типа плоскости безопасности:

- плоскость безопасности по управлению сетью (Management Security Plane), к которой относится защита функций администрирования, эксплуатации и обслуживания сети (Operation Administration Maintenance&Provision, OAM&P);
- плоскость безопасности по управлению соединением (Control Security Plane): защита функций и передаваемой по сети информации, например по установлению и разъединению соединения (сигнальная информация), по маршрутизации сообщений;
- плоскость безопасности оконечного пользователя (End-User Security Plane): безопасность сети доступа и др.

Сочетание каждого уровня безопасности с каждой плоскостью безопасности представляет модуль (область) безопасности, в которой способы обеспечения ИБ применяются для противодействия угрозам. Таким образом, полная архитектура ИБ сети связи состоит из девяти модулей. В Рекомендации X.805 [7] определены восемь способов защиты. Очевидно, что полный анализ ИБ даже одного модуля безопасности потребует рассмотрения очень большого количества угроз. Поэтому в настоящей работе удовлетворимся анализом ограниченного типа угроз ИБ, относящихся к ограниченному числу модулей безопасности.

Рассмотрению подлежит архитектура сетевой безопасности, включающая два модуля: 1) плоскость безопасности по управлению соединением и уровень безопасности инфраструктуры, 2) плоскость безопасности оконечного пользователя и уровень безопасности инфраструктуры. Анализу подлежат угрозы с высоким значением характеристики риска ИБ – последствием при ее реализации [8]. Рассматриваются потенциальные угрозы злоумышленника с целью несанкционированного доступа к адресной или информационной части пакета сообщения и последствия реализации таких угроз: формирование нелегитимного сообщения и передача его по раскрытому злоумышленником адресу конечного пункта, перехват сообщения с целью его уничтожения, изменение информационной части сообщения. Для некоторых сетей

возможность несанкционированного изучения структуры потока по адресам проходящих сообщений также является угрозой информационной безопасности, которая называется «анализ трафика» [9].

Основным механизмом защиты от рассматриваемых угроз несанкционированного доступа в сети коммутации пакетов (КП) является шифрование.

Технологии сетей ОгП, подлежащие сравнению по показателю обеспечения ИБ. Рассмотрим некоторые возможные технологии сетей связи, на которых могут быть построены сети связи ОгП. Покажем на примере этих сетей, каким образом могут решаться задачи защиты от указанных выше угроз несанкционированного доступа в сеть. В настоящей работе такому анализу подлежат следующие технологии сетей ОгП:

1) сети КП, построенные на основе таблицы маршрутизации только физических адресов;

2) сети КП на основе логических адресов без установления и с установлением виртуальных частных сетей. При построении таких отечественных сетей могут быть использованы (частично) принципы работы стандартизированных сетей X.25, Frame Relay [10]:

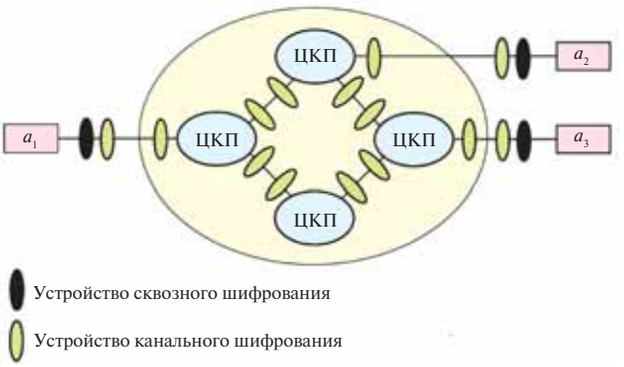
- сети, построенные на базе коммутируемых виртуальных каналов (КВК, SVC);
- сети, построенные на базе постоянных виртуальных каналов (ПВК, PVC);
- сети, построенные на базе комбинированных (коммутируемых и постоянных) виртуальных каналов (КПВК). Такие сети называются перепрограммируемыми (soft PVC).

Канальное и сквозное шифрование. На примере сети КП, построенной на основе таблицы маршрутизации физических адресов, покажем угрозы несанкционированного доступа в сеть и принцип организации защиты с помощью шифрования. На рисунке приведен пример структуры сети передачи данных с коммутацией пакетов с четырьмя центрами коммутации пакетов (ЦКП). К трем из этих ЦКП подключены оконечные устройства a_1, a_2, a_3.

Для такой сети возможны два основных варианта шифрования: адресной части пакета (канальное) между смежными устройствами сети и информационной части пакета (сквозное) между оконечными устройствами. Защиту от формирования нелегитимных сообщений и их передачу по полученному злоумышленником адресу конечного пункта обеспечивает шифрование адресной части сообщения (канальное шифрование). Защита от перехвата сообщений с целью его уничтожения или от изменения его информационной части основана на шифровании информационной части сообщения (сквозное шифрование).

При канальном шифровании каждый уязвимый к угрозе канал на сетевом уровне оборудуется устройствами аутентификации сообщений и шифрования на обоих концах канала. Таким образом, весь поток данных в канале оказывается защищенным. Недостатком только канального шифрования является то, что каждый раз, проходя через коммутатор пакетов, сообщение должно расшифровываться, чтобы коммутатор прочитал адрес в заголовке пакета и направил пакет в нужном направлении.

При сквозном шифровании процесс шифрования выполняется на уровне выше сетевого только на двух конечных станциях. Исходные данные шифруются в оконечном устройстве источника сообщений. Затем данные в шифрованном виде передаются без изменений через всю сеть получателю. Адресат использует тот же ключ, что и отправитель, дешифруя полученные данные. Недостаток только сквозного шифрования состоит в незащищенности адресной части. Как показано на рисунке, для защиты от вышеуказанных угроз несанкционированного доступа используются оба вида шифрования.



Структура сети передачи данных с коммутацией пакетов

Защита от несанкционированного доступа в сети ОгП на основе физических адресов. В связи с высокими требованиями к ИБ в сетях ОгП часто основой механизма защиты является рекомендация ITU-T X.509 [11], в соответствии с которой используется один или несколько уровней удостоверяющих центров (центров сертификации), создающих цепочку сертификатов. Примером реализации этого метода является обеспечение шифрования в сети связи общего пользования ISDN в соответствии с рекомендациями ITU-T и ETSI [12, 13]. Такая защита для сетей ОгП может быть построена на этих алгоритмах с использованием отечественных ГОСТов шифрования и аутентификации.

Представим в общем виде последовательность работы механизмов обеспечения шифрования при сквозном и канальном шифровании.

Для установленного соединения должна быть предусмотрена взаимная аутентификация между взаимодействующими конечными пунктами (при сквозном шифровании), между смежными ЦКП (при канальном шифровании), между ЦКП и подключенным к нему конечным пунктом (при канальном шифровании). Одновременно с процедурой аутентификации выполняется функция по созданию общего секретного ключа шифрования. В зависимости от конкретных требований заказчика к показателям качества обслуживания определенной сети ОгП функции аутентификации и установления общего ключа шифрования могут производиться периодически, т.е. не при каждом установлении соединения.

При реализации рассматриваемого механизма аутентификации с использованием сертификатов канальное шифрование адресной части (обычно небольшой длины) в определенных условиях можно производить также с помощью ключей асимметричной криптографии. Такими условиями являются небольшая длина адресной части, конкретные требования заказчика к характеристике задержки сообщения управления в сети ОгП и др. При использовании криптографии с открытым ключом для обеспечения ИБ может быть создана структура данных, аналогичная используемой в протоколе защиты электронной почты PGP, – связка ключей [10]. Смена пар используемых ключей усиливает защиту от угроз несанкционированного доступа.

Для защиты от указанных выше угроз несанкционированного доступа шифрование адресной части заголовка сообщений и информационной части сообщения необходимо проводить как на этапе создания соединения, так и в процессе обмена сообщениями по установленному соединению.

Защита от несанкционированного доступа в сети ОгП на основе логических адресов. Защиту от несанкционированного доступа в сети КП на основе логических адресов рассмотрим на примере сети передачи данных, не использующей выделенный канал сигнализации.

Исследуем особенности уязвимости от анализируемых угроз и защиты в сети ОгП на основе логических адресов в двух случаях: без использования виртуальных частных сетей (VPN) и с использованием VPN.

Защита от несанкционированного доступа в сети без использования виртуальных частных сетей. Рассмотрению подлежат сети ОгП, пользователями которых являются различные системы (технологические, спецсистемы). При этом для пользователей этих систем не созданы виртуальные частные сети. Защита информационной части сообщений (сквозное шифрование) в такой сети ОгП не отличается от защиты в сети КП на основе физических адресов.

При установлении соединения между оконечными устройствами с помощью виртуального канала КВК, ПВК или КПВК в зависимости от конкретных требований заказчика в некоторых сетях ОгП может отсутствовать необходимость в шифровании адресной части сообщения. При этом надо учесть, что отсутствие шифрования адресной части на этапе передачи сообщений не защищает от угрозы нелегитимного повтора сообщения. Знание злоумышленником логического адреса в любом месте установленного соединения позволяет реализовать такую угрозу при отсутствии защиты от нее (например, с помощью счетчика сообщений). Риск ИБ при реализации угрозы повтора небольшой, поскольку в этом случае характеристика риска, выраженная вероятностью угрозы [8], невысока в сравнении с вероятностью реализации других анализируемых угроз несанкционированного доступа.

Взаимодействующие конечные пункты КВК могут стать известны злоумышленнику в результате получения их открытых физических адресов, перехваченных во время установления соединения. Это открывает злоумышленнику путь к установлению нелегитимного соединения с конечным пунктом, хотя вероятность такой угрозы может быть незначительна при выполнении аутентификации конечных пунктов с помощью сертификатов. Отсутствие шифрования адресной части в случае КВК на этапе передачи сообщений не защищает также от угроз «анализ трафика», уничтожения сообщения известного злоумышленнику соединения. Отсутствие необходимости использовать физические адреса при установлении ПВК позволяет избежать этих угроз ИБ. В случае установления КПВК такие угрозы могут быть реализованы с очень малой вероятностью, так как злоумышленнику могут быть известны физические адреса не взаимодействующих конечных пунктов, а ЦКП, к которым они подключены.

Защита от несанкционированного доступа в сети с использованием виртуальных частных сетей. Рассмотрению подлежат сети ОгП, пользователями которых являются несколько разных систем. При этом для пользователей каждой системы созданы виртуальные частные сети, что в некоторых сетях ОгП может привести к снижению требований к защите от рассматриваемых угроз несанкционированного доступа.

Защита информационной части сообщения (сквозное шифрование) в этой сети может отличаться от защиты в сети КП на основе физических адресов. Виртуальные частные сети позволяют снизить требования к механизму аутентификации и созданию общего ключа шифрования, да и к самому механизму шифрования. Это вызвано тем, что виртуальная частная сеть обеспечивает изолированность взаимодействующих пользователей одной системы (технологической или спецсистемы). Поэтому в некоторых сетях ОгП аутентификация и создание общего ключа шифрования могут быть реализованы на другом механизме (без использования сертификатов). Виртуальные частные сети при отсутствии шифрования адресной части сообщений позволяют снизить вероятность реализации злоумышленником отмеченных выше угроз в случае отсутствия VPN.

Сравнительный анализ защищенности от угроз несанкционированного доступа в сетях ОгП. Настоящий раздел посвящен сравнительному анализу защищенности приведенных ниже семи технологий сетей ОгП от рассмотренных угроз несанкционированного доступа. Для этого используем математический аппарат, предложенный для сравнения механизмов защиты от угроз ИБ авторами международного проекта, финансируемого Европейской комиссией по сетям связи (материалы проекта опубликованы в открытой печати [14]).

В настоящей работе этот математический аппарат используется в рамках решения поставленной задачи – сравнения различных технологий сетей ОгП в аспекте обеспечения ИБ от анализируемых угроз несанкционированного доступа. Для иллюстрации предлагаемого метода приводится пример.

Сравнение производится по показателю R:

$$R = \frac{\sum_{i=1}^{N} 5\, k_i x_i}{\sum_{i=1}^{N} k_i}.$$

Здесь под k_i понимается степень важности требования заказчика по характеристике i. Чем больше k_i, тем важнее i-е требование ($k_i = 1, 2, 3$). Выбор характеристик k_i зависит от функций конкретной сети ОгП и определяется на этапе согласования технических требований. Для рассматриваемого примера сравнительного анализа защищенности от угроз несанкционированного доступа сетей ОгП примем следующие требования важности защиты от угроз несанкционированного доступа k_i: k_1 – защита от формирования нелегитимных сообщений и передача их по полученному злоумышленником адресу конечного пункта; k_2 – защита от перехвата сообщений с целью его уничтожения; k_3 – защита от изменения информационной части сообщений.

Значение x_i показывает степень выполнения этого требования. В указанном отчете $x_i = 0$ – требование совсем не выполняется, $x_i = 1$ – выполняется частично, $x_i = 2$ – требование полностью удовлетворено. При выбранных в формуле возможных k_i, x_i и коэффициенте 5 диапазон R может принимать значения между 0 и 10. Значения k_i, x_i определяем методом экспертных оценок.

Для решения поставленной задачи сравнительного анализа защищенности от угроз несанкционированного доступа сетей ОгП с помощью приведенного выражения примем следующие обозначения семи рассматриваемых технологий сетей передачи данных:

Результаты расчета показателя защищенности в зависимости от требований важности защиты k_i и степени их выполнения x_i для семи технологий сетей передачи данных ОгП

k_i	x_i для технологий сетей						
	1	2	3	4	5	6	7
$k_1 = 3$	2	1	1	1	2	2	1
$k_2 = 2$	1	0	1	0	0	1	2
$k_3 = 3$	2	0	1	1	1	1	1
Показатель защищенности R	8,75	1,9	5	3,75	5,6	6,9	6,25

- технология 1 – сеть КП на основе физических адресов (ФА);
- технология 2 – сеть КП на основе логических адресов (ЛА) и коммутируемых виртуальных каналов (КВК) (без VPN);
- технология 3 – сеть КП на основе ЛА и постоянных виртуальных каналов (ПВК) (без VPN);
- технология 4 – сеть VPN КП на основе ЛА и комбинированных постоянных виртуальных каналов (КПВК);
- технология 5 – сеть VPN КП на основе ЛА и КВК;
- технология 6 – сеть VPN КП на основе ЛА и ПВК;
- технология 7 – сеть КП на основе ЛА и КПВК.

В таблице приведены результаты расчета для семи технологий сетей передачи данных ОгП. Значения требований важности защиты k_i и степени выполнения этих требований x_i для каждой рассматриваемой технологии зависят от используемых в них механизмов защиты от рассматриваемых угроз несанкционированного доступа, частоты смены ключа шифрования и др.

Значения x_i зависят от конкретной реализации. Приведенные в таблице результаты расчета показывают, что в данном примере технология 1 по сравнению с другими анализируемыми технологиями в большей степени (значение R максимальное) выполняет требования защищенности от угроз несанкционированного доступа в сети ОгП.

Следует подчеркнуть, что этот пример приведен только для иллюстрации использования предлагаемого метода сравнительного анализа защищенности от угроз ИБ сетей передачи данных ограниченных пользователей.

Заключение. Настоящая работа может быть использована для сравнительного анализа защищенности от угроз несанкционированного доступа проектируемых и действующих сетей передачи данных ограниченных пользователей.

ЛИТЕРАТУРА

1. Федеральный закон Российской Федерации «О связи» № 126-ФЗ от 07.07.2003 (редакция от 23.02.2011).
2. **Москвитин В.Д.** От взаимосвязанной сети связи к Единой сети электросвязи России // Вестник связи. – 2003. – № 8.
3. **Бадалов А.Ю.** Концепция доверенного оборудования как отражение воли рынка //Электросвязь. – 2011. – № 8.
4. **Hui-sheng Gao, Jing-xue Ran, Yi-qun Sun.** Risk Evaluation of Communication Network of Electric Power Based on Restriction Coefficient //Wireless Communications, Networking and Mobile Computing, 2007 (WiCom 2007. International Conference). – P. 3127–3134.
5. **Hui-sheng Gao (and others).** Risk Evaluation of Communication Network of Electric Power Using logarithm Least, 7th World Congress on Intelligent Control and Automation, 2008, Chongqing, China. – P. 5801–5806.
6. **Hui-Sheng Gao, Jing-xue Ran, Yi-qun Sun.** Risk Evaluation of Communication Network of Electric Power Based on Improved FAHP, Fuzzy Systems and Knowledge Discovery, Fourth International Conference //FSKD 2007. – V. 3. – P. 653–659.
7. ITU-T Recommendation X.805. Security architecture for System providing end-to-end communication, 2003.
8. ITU-T Recommendation E.408. Telecommunication Network Security Requirement, 2004.
9. **Таненбаум Э., Уэзеролл Д.** Компьютерные сети, 5-е изд. – СПб.: Питер, 2012.
10. **Бельфер Р.А.** Сети и системы связи (технологии, безопасность). Учеб. пособие по дисциплине «Сети и системы связи»: электронное учеб. издание. – М.: ФГБОУ ВПО МГТУ им. Н.Э. Баумана, 2012.
11. ITU-T Recommendation X.509. Information technology – Open Systems Interconnection. The Directory: Authentication framework (1993 edition – version 2, 1997 edition version 3).
12. ITU-T Recommendation H.234. Encryption key management and authentication system for audio-visual services, 1998.
13. ETSI ETS 300 841. Telecommunications Security; Integrated Services digital Network (ISDN); Encryption Key management system for audio-visual services, 1998.
14. **Sead Muftic (and others).** Security Architecture for Open Distributed Systems. – John Wiley & Sons, Wiley Series in Communications & Distributed Systems, 1994. – P. 281.

Получено 03.06.13