УДК 681.3.06 (0.43)

О.Г. Король

Харьковский национальный экономический университет, Харьков

ПРОТОКОЛЫ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Анализируются требования, предъявляемые к современным телекоммуникационным системам и сетям, в частности, анализируются требования, предъявляемые к показателям качества передачи данных в инфокоммуникационных системах специального назначения (на примере телекоммуникационной сети национальной системы массовых электронных платежей). Рассматриваются протоколы сетевой безопасности наиболее распространенных телекоммуникационных IP-сетей, исследуются особенности обеспечения целостности, аутентичности и конфиденциальности передачи пакетов данных.

Ключевые слова: *телекоммуникационные системы, протоколы сетевой безопасности, целостность, аутентичность, конфиденциальность.*

Введение

Постановка проблемы. Современные телекоммуникационные системы и сети характеризуются быстрым ростом числа пользователей и потребителей информации, расширением спектра предоставляемых телекоммуникационных услуг, прежде всего, обеспечением доступа к различным мультимедийным сервисам и технологиям, поддержке удаленных пользователей, обслуживанию субъектов автоматизированного информационного взаимодействия и т.д. Эти тенденции обуславливают резкое повышение объемов обрабатываемых и передаваемых данных и, как следствие, ужесточение вероятностно-временных требований, предъявляемых к основным компонентам телекоммуникационных систем и сетей на всех этапах информационного обмена данными [1, 5, 9 – 11].

Важнейшим показателем эффективности современных телекоммуникационных систем и сетей является их безопасность, под которой будем понимать способность к обеспечению целостности, аутентичности и конфиденциальности обрабатываемых и передаваемых данных [1, 3, 5, 12]. От степени реализации этих характеристик непосредственно зависит уровень защищенности от современных угроз сетевой безопасности и, в конечном счете, качество предоставляемых телекоммуникационных услуг [1, 3, 5, 12].

Целью статьи является анализ требований, предъявляемых к современным телекоммуникационным системам и сетям, исследование протоколов сетевой безопасности телекоммуникационных IP-сетей, а также особенности обеспечения целостности, аутентичности и конфиденциальности передачи пакетов данных.

Основной материал

Анализ требований, предъявляемых к современным телекоммуникационным системам и сетям. Мировые тенденции в развитии телекоммуникационной отрасли определяют построение современных систем и сетей связи в виде мультисервисных телекоммуникационных сетей с обеспечением заданного уровня качества обслуживания (Quality of Service, QoS) [1, 3, 4, 12].

Обобщенная схема построения мультисервисной телекоммуникационной сети представлена на рис. 1.

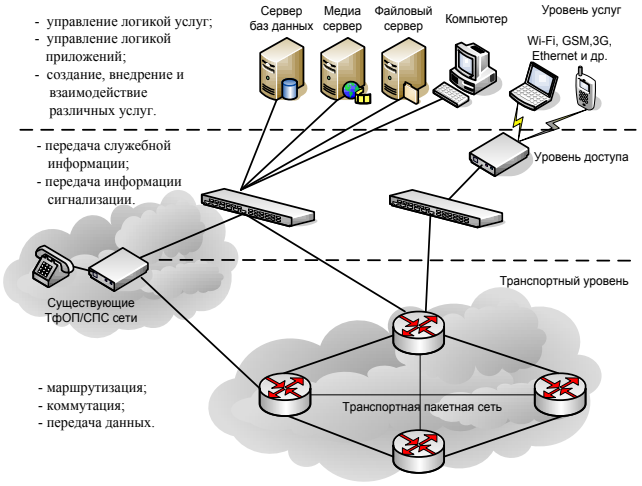

Рис. 1. Обобщенная схема построения мультисервисной телекоммуникационной сети

В соответствии с рекомендациями Е.430, Е.800, Х.134 и др. международного союза электросвязи под качеством обслуживания (QoS) понимается обобщенный (интегральный) полезный эффект, который определяется степенью удовлетворения пользователя, как от полученной услуги, так и от самой системы обслуживания [4, 9]. Общая схема характеристик и показателей, относящихся к качеству обслуживания и эффективности функционирования телекоммуникационной сети (ТКС) в соответствии с международными рекомендациями (ITU-T, ETSI, TL 9000, Е.800), представлена на рис. 2 [4, 9].

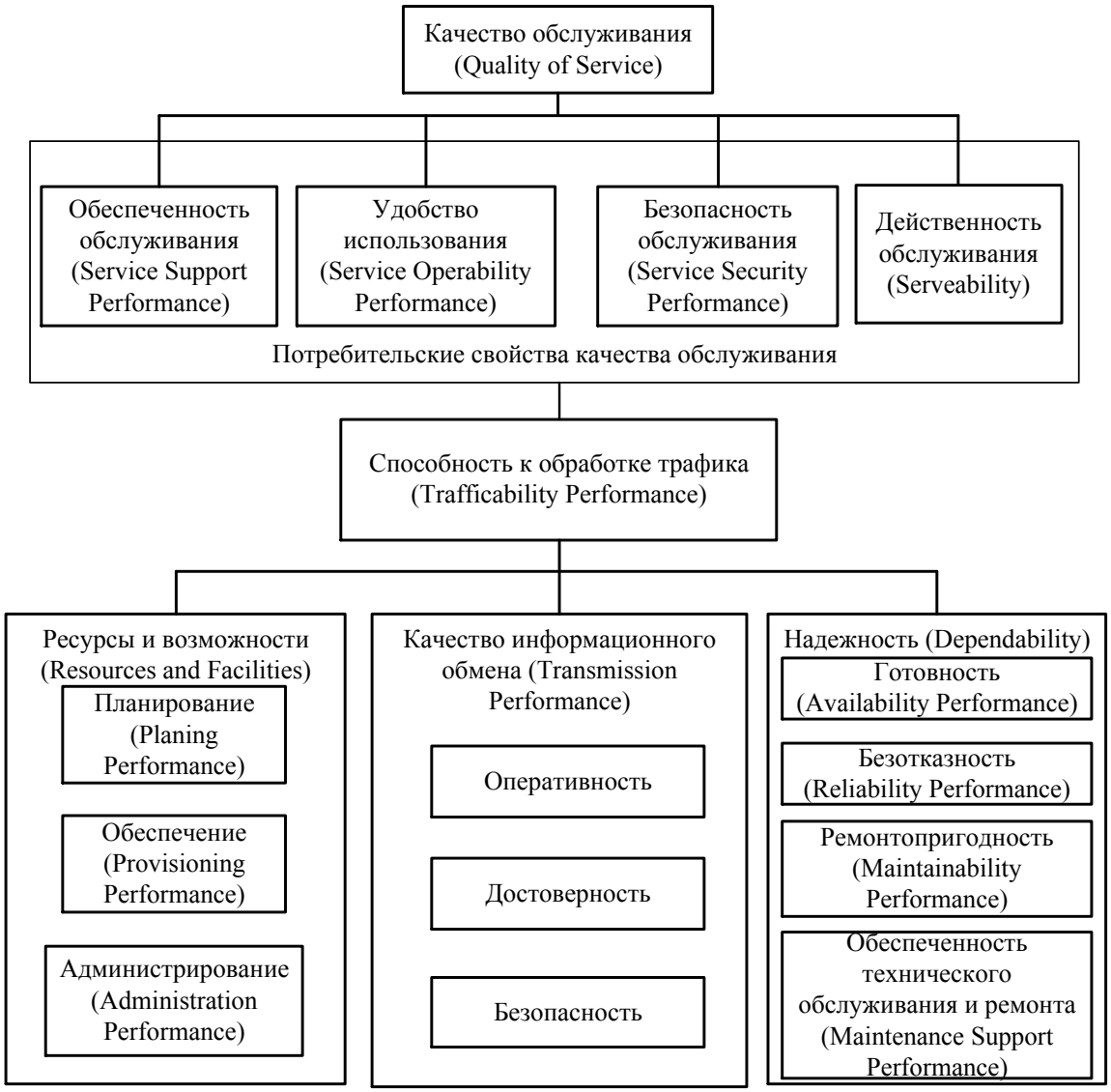

Рис. 2. Общая схема характеристик и показателей качества обслуживания и эффективности функционирования телекоммуникационной сети

Таким образом, качество обслуживания характеризуется четырьмя потребительскими свойствами услуг [1, 5, 9 – 11]: обеспеченностью (Service Support Performance), удобством использования (Service Operability Performance), действенностью (Serveability) и безопасностью обслуживания (Service Security Performance). Реализация перечисленных свойств зависит, в основном, от способности сети «обрабатывать трафиковые нагрузки» (Trafficability Performance). Качество такой обработки зависит от ресурсных возможностей телекоммуникационных сетей, задействованных оператором (Resources and Facilities), надежности каналов связи и сетевого оборудования (Dependability), а так же качества информационного обмена (Transmission Performance), характеризующихся оперативностью, достоверностью и безопасностью передачи данных по каналам телекоммуникационных систем и сетей.

В соответствии с рекомендациями МСЭ I.350 определены три основные функции, реализуемые телекоммуникационной сетью, установлены конкретные характеристики каждой из указанных функций [5, 11]. В табл. 1 представлены основные показатели качества передачи данных в телекоммуникационных сетях в соответствии с функциями, реализуемыми операторами телекоммуникационных услуг.

На основе данных, полученных в результате исследования Европейским исследовательским центром в области телекоммуникаций (RACE – Research on Advanced Communication), определены допустимые значения требований к основным показателям качества обслуживания в ТКС [1, 11, 12].

В табл. 2 представлены допустимые значения требований к основным показателям качества при передаче различных видов данных.

Таблица 2

Допустимые значения требований к основным показателям качества передачи различных видов данных

Телекоммуникационные услуги	$T_д$,мс	J ,мс	$P_{иск}$	$P_{н.ц.}$	$P_{нав}$	$T_б$,лет	$P_с$	$P_к$
Телефония	400-500	10	10^{-7}	$< 2^{-l_{кц}}$	$< 2^{-l_a}$	$> T_{б_д}$	$< 2^{-l_ш}$	$< 2^{-l_{кш}}$
IP-телефония	400-500	10	10^{-7}	$< 2^{-l_{кц}}$	$< 2^{-l_a}$	$> T_{б_д}$	$< 2^{-l_ш}$	$< 2^{-l_{кш}}$
Высокоскоростная передача массивов данных	1000	20	10^{-7}	$< 2^{-l_{кц}}$	$< 2^{-l_a}$	$> T_{б_д}$	$< 2^{-l_ш}$	$< 2^{-l_{кш}}$
Краткосрочный обмен данными (БД, дистанционное обучение и т.д.)	1000	40	10^{-7}	$< 2^{-l_{кц}}$	$< 2^{-l_a}$	$> T_{б_д}$	$< 2^{-l_ш}$	$< 2^{-l_{кш}}$
Информационный поиск	1000	40	10^{-7}	$< 2^{-l_{кц}}$	$< 2^{-l_a}$	$> T_{б_д}$	$< 2^{-l_ш}$	$< 2^{-l_{кш}}$
Потоковое видео по запросу	500	10	10^{-6}	$< 2^{-l_{кц}}$	$< 2^{-l_a}$	$> T_{б_д}$	$< 2^{-l_ш}$	$< 2^{-l_{кш}}$
Цифровое телевидение	500	10	10^{-6}	$< 2^{-l_{кц}}$	$< 2^{-l_a}$	$> T_{б_д}$	$< 2^{-l_ш}$	$< 2^{-l_{кш}}$
Видеоконференцсвязь, видеонаблюдение	500	10	10^{-6}	$< 2^{-l_{кц}}$	$< 2^{-l_a}$	$> T_{б_д}$	$< 2^{-l_ш}$	$< 2^{-l_{кш}}$
Дистанционное управление обработкой	1000	20	10^{-5}	$< 2^{-l_{кц}}$	$< 2^{-l_a}$	$> T_{б_д}$	$< 2^{-l_ш}$	$< 2^{-l_{кш}}$
Передача служебной информации	500	10	10^{-6}	$< 2^{-l_{кц}}$	$< 2^{-l_a}$	$> T_{б_д}$	$< 2^{-l_ш}$	$< 2^{-l_{кш}}$

Проведенный анализ [6, 8] показал, что быстрый рост числа пользователей и потребителей информации, расширение спектра предоставляемых телекоммуникационных услуг, прежде всего, обеспечение доступа к различным мультимедийным сервисам и технологиям, резко возросшие в последнее десятилетие объемы обрабатываемых и передаваемых данных, приводит к ужесточению вероятностно-временных требований, предъявляемых к основным компонентам телекоммуникационных систем и сетей на всех этапах информационного обмена данными. Это относится, в первую очередь, к показателям безопасности передачи данных.

Таким образом, актуальность создания телекоммуникационных систем и сетей с защищенными каналами передачи данных в последние годы резко возросла.

Возросли и требования к показателям безопасности передачи данных в телекоммуникационных системах и сетях, особенно в сетях специального назначения, в которых отказ в обслуживании или выход конкретных параметров качества за установленные пределы может привести к катастрофическим последствиям в финансовом секторе, промышленности, энергетическом комплексе и пр.

В качестве примера такой системы можно привести создаваемую в Украине национальную систему массовых электронных платежей (НСМЭП), упрощенная структурная схема которой приведена на рис. 3, а [6, 8]. На рис. 3, б приведена структурная схема главного (регионального) процессингового центра, на рис. 3, в – в упрощенном виде структурная схема телекоммуникационной системы банка.

Таким образом, современные автоматизированные банковские системы (рис. 3, в) представляют собой большие территориально распределенные мультисервисные телекоммуникационные сети специального назначения, использующие высокопроизводительные вычислительные комплексы и сложные механизмы комплексной защиты информационных технологий.

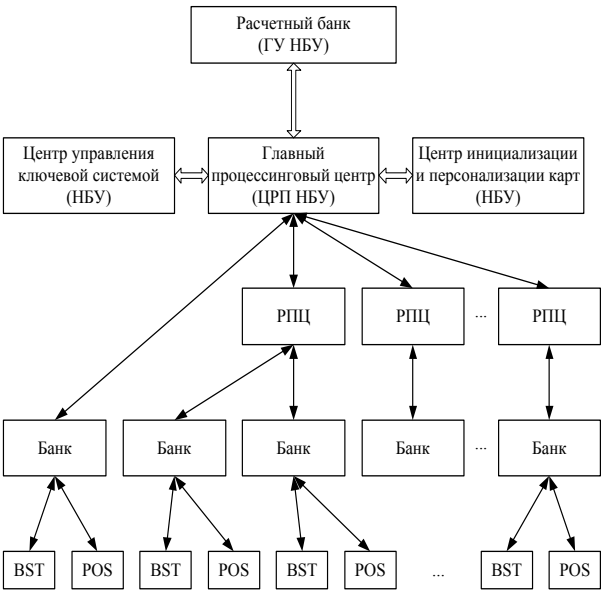

Рис. 3, а. Упрощенная структурная схема НСМЭП

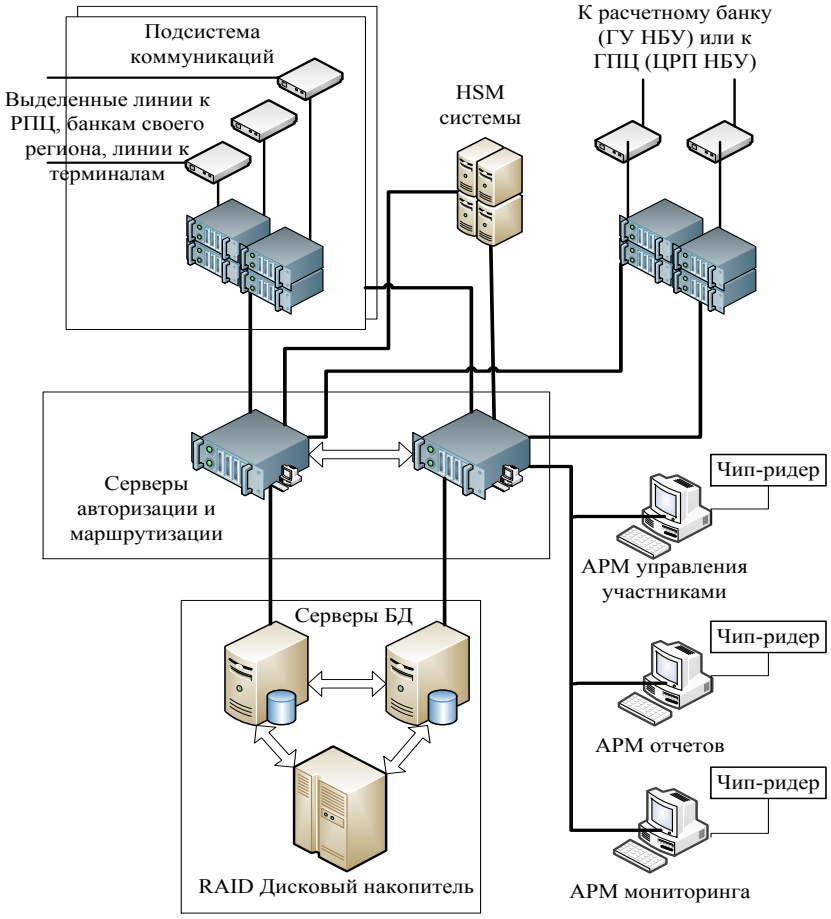

Рис. 3, б. Структурная схема главного (регионального) процессингового центра

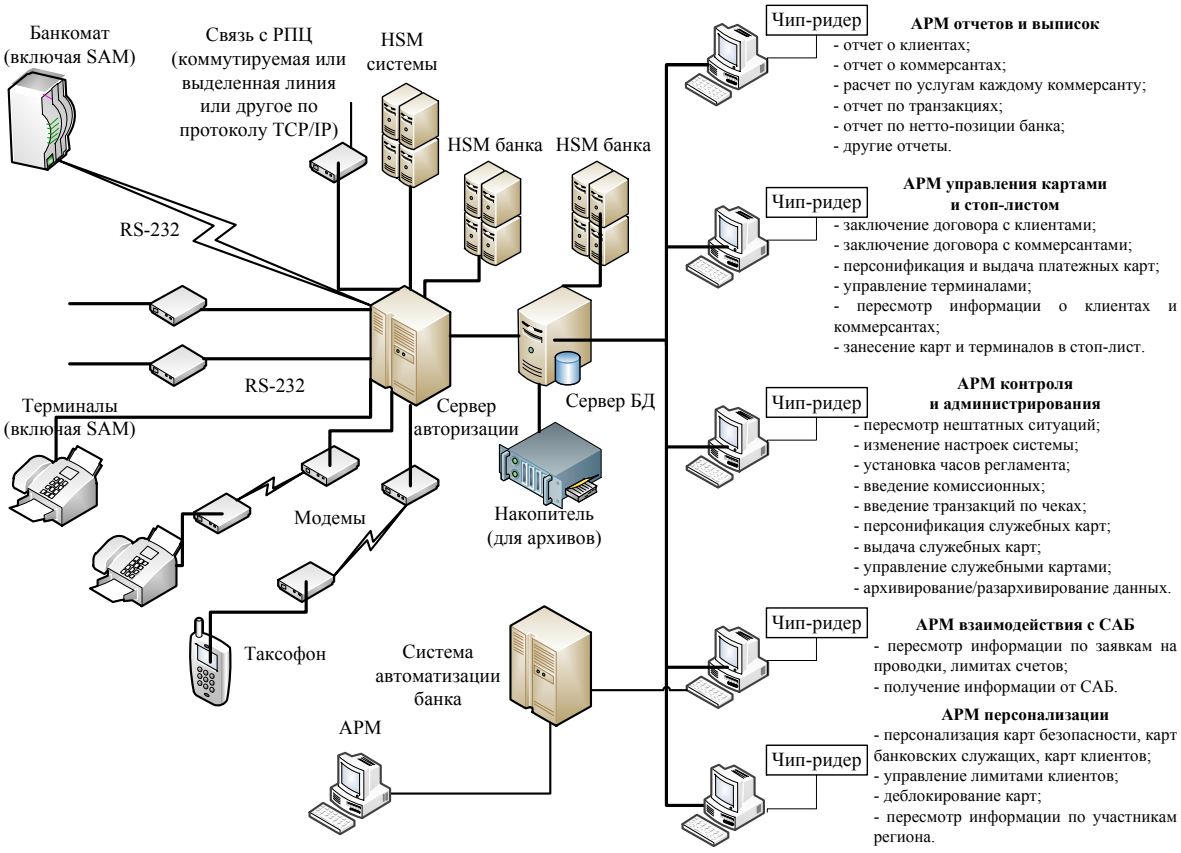

Рис. 3, в. Структурная схема телекоммуникационной системы банка

Проведенный анализ [4, 6, 8] показал, что современные автоматизированные банковские системы, используя последние достижения в развитии электронных коммуникаций и IT-технологий, успешно расширяют спектр предоставляемых банковских услуг, в том числе по обслуживанию субъектов автоматизированного информационного взаимодействия, предоставлению услуг оплаты через сети банкоматов, поддержке автоматизированных комплексов банковской системы постоянно возрастают.

Результаты проведенного анализа основных вероятностно-временных требований к частным показателям оперативности, достоверности и безопасности (целостности, аутентичности и конфиденциальности) применяемым в автоматизированных банковских системах информационным технологиям сведены в табл. 3.

Анализ данных табл. 3 показывает, что вероятностно-временные требования к применяемым информационным технологиям в автоматизированных банковских системах существенно возросли. В первую очередь это относится к применяемым механизмам обеспечения целостности, аутентичности и конфиденциальности передаваемых пакетов данных.

Перспективные методы и механизмы безопасности должны обеспечивать решение возложенных на них задач в чрезвычайных условиях резко возросших объемов обрабатываемых и передаваемых данных, расширения спектра угроз информационной безопасности на всех этапах жизненного цикла телекоммуникационных систем и сетей, стремительного развития средств удаленных пользователей, продаже товаров через интернет-магазины и т.д.

Как следствие выявленных тенденций, возрастают предъявляемые требования к показателям качества передачи данных в телекоммуникационных системах и сетях вычислительной техники, совершенствованию математических методов и вычислительных алгоритмов криптографического анализа [1– 4, 7, 10, 12].

Анализ современных коммуникационных протоколов телекоммуникационных сетей

В зависимости от задач, на решение которых ориентирован тот или иной протокол, он может быть отнесен к одной из множества категорий. На пример:

Транспортные протоколы регламентируют порядок передачи данных между сетевыми устройствами. Эти протоколы образуют "каркас" телекоммуникационной сети, реализуя транспортный механизм. К данной категории можно отнести протоколы: IP, TCP, IPX, SPX, X.25.

Протоколы аутентификации позволяют организовать процесс аутентификации пользователей и устройств, участвующих в сетевом взаимодействии. К этой категории относятся протоколы Kerberos, RADIUS.

Протоколы маршрутизации используются для реализации межсетевого взаимодействия устройств, получивших название маршрутизаторов. Протоколы маршрутизации используются маршрутизаторами для построения подобных таблиц (протоколы RIP, OSPF, IS-IS, BOP).

Таблица 3

Основные вероятностно-временные требования
к некоторым информационным технологиям в автоматизированных банковских системах

Обеспечиваемая услуга или предоставляемый сервис	Показатели эффективности						
	$T_д$, мс	$P_{иск}$	$T_б$, лет	$P_с$	$P_к$	$P_{н.ц.}$	$P_{нав}$
Передача финансовых электронных документов между банками и их подразделениями	500	10^{-6}	200	10^{-10}	10^{-10}	10^{-25}	10^{-25}
Поддержка транзакций при выполнении расчетов	400-500	10^{-9}	200	10^{-10}	10^{-10}	10^{-30}	10^{-30}
Поддержка работы удаленных банкоматов	400-500	10^{-9}	200	10^{-10}	10^{-10}	10^{-30}	10^{-30}
Объединение локальных сетей банков, функционирование вычислительных сетей банка	500	10^{-7}	-	-	-	10^{-25}	10^{-25}
Доступ к финансовым информационным службам	1000	10^{-5}	-	-	-	10^{-25}	10^{-25}

Протоколы обеспечения безопасности передачи данных. К этой группе относятся протоколы туннелирования и протоколы шифрования данных: например, SSL, PPTP, L2TP, IPSec.

Вспомогательные протоколы. Эта группа протоколов реализует вспомогательные сетевые сервисы – DHCP, HTTP, FTP.

Коммуникационные протоколы современных телекоммуникационных систем и сетей реализуются как в программном, так и в аппаратном виде.

Наиболее компромиссным вариантом реализации функций безопасности в телекоммуникационных системах и сетях являются протоколы сетевой безопасности IPSec, функционирующие на сетевом уровне [1, 12]. С одной стороны, они прозрачны для приложений, а с другой – могут работать практически во всех сетях, так как основаны на широко распространенном протоколе IP [1, 12].

Протоколы сетевой безопасности IPSec (Internet Protocol Security (IPSec) – это согласованный набор

открытых стандартов, имеющий на сегодняшний день конкретную спецификацию, который, в то же время, может быть дополнен новыми протоколами, алгоритмами и функциями сетевой безопасности [1, 12].

Основное назначение протоколов IPSec – обеспечение безопасной передачи данных по IP-сетям. Их применение обеспечивает [1, 12]:

целостность, т.е. способность телекоммуникационной сети обеспечивать передачу данных без искажения, потери или дублирования;

аутентичность, т.е. способность телекоммуникационной сети обеспечивать передачу данных с возможностью доказательства их подлинности (т.е. того, что данные переданы именно тем отправителем, за кого он себя выдает);

конфиденциальность, т.е. способность телекоммуникационной сети обеспечивать передачу данных в форме, предотвращающей их несанкционированный просмотр.

Основными компонентами IPsec являются:

RFC2402 «IP Authentication Header» (AH), предназначенный для контроля целостности и аутентичности пакетов данных в IP-сетях;

RFC2406 «IP Encapsulation Security Payload» (ESP), предназначенный для обеспечения конфиденциальности, контроля целостности и аутентичности пакетов данных в IP-сетях;

RFC2408 «Internet Security Association and Key Management Protocol» (ISAKMP), предназначенный для обеспечения согласования параметров, создания, изменения, уничтожения контекстов защищенных соединений (Security Association, SA) и управления ключами в IP-сетях;

RFC2409 «The Internet Key Exchange» (IKE), являющийся дальнейшим развитием и адаптацией ISAKMP, предназначенный для работы с протоколами IPsec.

Ядро IPSec составляют три протокола (рис. 4): протокол аутентификации (Authentication Header, AH), протокол шифрования (Encapsulation Security Payload, ESP) и протокол обмена ключами (Internet Key Exchange, IKE). Функции по поддержанию защищенного канала распределяются между этими протоколами следующим образом:

протокол AH обеспечивает целостность и аутентичность данных;

протокол ESP шифрует передаваемые данные, гарантируя конфиденциальность, но он может также поддерживать аутентификацию и целостность данных;

протокол IKE решает вспомогательную задачу автоматического предоставления секретных ключей, необходимых для работы протоколов аутентификации и шифрования данных.

Для формирования кодов контроля целостности и аутентичности пакетов данных (integrity check value, ICV) используются специальные механизмы безопасности информации: коды обнаружения манипуляций (MDC – Manipulation Detection Code), коды аутентификации сообщений (MAC – Message Authentication Code). Их формирование основано на использовании хеширующих функций, позволяющих для данных в общем случае произвольной длины формировать хеш-код (хеш-значение) строго заданной длины. Указанные механизмы применяются по умолчанию в целях обеспечения целостности и аутентичности пакетов данных во всех реализаций сетей IPv6.

Рис. 4. Основные компоненты протокола сетевой безопасности IPSec

При этом для формирования ICV в протоколе AH предусмотрены обязательные алгоритмы (для обеспечения совместимости программных продуктов различных производителей), такие, например, как HMAC-MD5-96 (описанный в стандарте RFC 2403), HMAC-SHA-1-96 (описанный в стандарте RFC 2404). Кроме того, предусмотрены некоторые другие (дополнительные) алгоритмы для формирования ICV, например, DES-MAC, HMAC-ГОСТ Р 34.11-94, HMAC-ГОСТ Р 34.11-2001.

Протокол ESP реализует: шифрование данных IP-пакетов для обеспечения конфиденциальности информации; дополнительно (аналогично протоколу AH) аутентификацию источника каждого пакета, целостность данных каждого пакета, защиту от повторной передачи пакетов. Для обеспечения конфиденциальности данных IP-пакетов предусмотрено использование криптографических алгоритмов шифрования, среди которых предусмотрены обязательные алгоритмы (для обеспечения совместимости программных продуктов различных производителей), такие, например, как DES-CBC (описанный в стандарте RFC 2405), NULL (описанный в стандарте RFC 2410). Кроме того, предусмотрены некоторые

другие (дополнительные) алгоритмы шифрования, например, CAST-128, IDEA, 3DES (описанные в стандарте RFC 2451), а также национальный стандарт шифрования США AES-128, 192, 256 (FIPS-197) и отечественный стандарт ГОСТ-28147-89. Протоколы ESP и AH могут использоваться как в туннельном, так и в транспортном режиме, как самостоятельно, так и в комбинации.

Таким образом, проведенный анализ современных протоколов сетевой безопасности, применяемых в IP-сетях для обеспечения целостности, аутентичности и конфиденциальности передачи данных, позволяет сделать следующие выводы:

применение механизмов защиты информации на верхних уровнях (уровня прикладного процесса, уровня представлений или сеансового уровня) модели OSI позволяет эффективно реализовать функции безопасности конкретных сетевых служб. В то же время наблюдается зависимость реализации сетевых служб и конкретных приложений от версии протокола сетевой безопасности. Снижение уровня (по спецификации модели OSI) повышает универсальность применяемых средств защиты для любых приложений и протоколов прикладного уровня, однако возникает зависимость протокола защиты от конкретной сетевой технологии;

компромиссным вариантом являются протоколы сетевой безопасности IPSec, функционирующие на сетевом уровне. С одной стороны, они «прозрачны» для приложений, а с другой – могут работать практически во всех сетях, так как основаны на широко распространенном протоколе IP.

Для контроля целостности и аутентичности пакетов данных в протоколах IPSec применяются специальные механизмы защиты. Их применение позволяет, за счет внесения в передаваемые данные специально сформированной избыточности (MDC, MAC) эффективно решать задачи защиты пакетов данных от случайного и злонамеренного изменения. Формирование кодов контроля целостности и аутентичности пакетов данных основано на использовании ключевых (MAC) и бесключевых (MDC) хеширующих функций. Указанные механизмы применяются по умолчанию в протоколах IPSec в целях обеспечения целостности и аутентичности пакетов данных во всех реализаций сетей IPv6.

Выводы

Проведенный анализ показал, что современные телекоммуникационные системы и сети постоянно расширяют спектр предоставляемых услуг доступа к различным мультимедийным сервисам и технологиям, поддержке удаленных пользователей и т.д. В то же время быстрый рост объемов обрабатываемых данных приводит к ужесточению вероятностно-временных требований, предъявляемых к основным компонентам телекоммуникационных систем и сетей на всех этапах информационного обмена данными. Одним из наиболее эффективных подходов к построению механизмов контроля целостности и аутентичности информации является ключевое и бесключевое хеширование данных. Практическое использование соответствующих механизмов безопасности позволяет без привлечения дополнительных средств обеспечивать требуемые показатели целостности и аутентичности обрабатываемых и передаваемых данных.

Список литературы

1. Столлингс В. Криптография и защита сетей: принципы и практика: пер. с англ. / В. Столлингс. – 2-е изд. – М.: Издательский дом «Вильямс», 2001. — 672 с.

2. Романец Ю.В. Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин; Под ред. В.Ф. Шаньгина. – 2-е изд., перераб. и доп. – М.: Радио и связь, 2001. – 376 с.

3. Артеменко Д.А. Механизм обеспечения финансовой безопасности банковской деятельности: дис. канд. экон. наук: 08.00.10 / Артеменко Д.А. – Ростов н/Д, 1999. – 190 с.

4. Чмора А.Л. Современная прикладная криптография / А. Л. Чмора. – М., 2002. – 508 с.

5. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 2.5-004-99.– [Чинний від 1999-28-04]. – К.: Держспоживстандарт України 1999. – 53 с.

6. Евсеев С.П. Защита информации в интернет-платежных системах / С.П. Евсеев, О.Г. Король, А.С. Жученко // Восточно-европейский журнал передовых технологий. – 2008. – 5/2(35). – С. 34-38.

7. Евсеев С.П. Исследование методов обеспечения аутентичности и целостности данных на основе односторонних хеш-функций / С.П. Евсеев, О.Г. Король // Науково-технічний журнал «Захист інформації». Спецвипуск (40). – 2008. – С. 50-55.

8. Кузнецов А.А. Исследования криптографических средств защиты информации в платежных системах банков Украины // А.А. Кузнецов, С.П. Евсеев, О.Г. Король // Науково-технічний журнал «Захист інформації». – 2009. – №1 (42). – С. 31-39.

9. Евсеев С.П. Анализ эффективности передачи данных в компьютерных системах с с пользованием интегрированных механизмов обеспечения надежности и безопасности / С.П. Евсеев, Д.В. Сумцов, Б.П. Томашевский, О.Г. Король // Восточно-европейский журнал передовых технологий. – 2010. – 2/2(44). – С. 45-50.

10. Король О.Г. Оцінка ризику реалізації загроз безпеки у внутрішньоплатіжних банківських системах / О.Г. Король // Системи управління навігації та зв'язку. – К.: ДП «ЦНДІ НІУ», 2010. – Вип. 3(15). – С. 154-159.

11. Евсеев С.П. Механизмы и протоколы защиты информации в компьютерных сетях и системах / С.П. Евсеев, А.В. Дорохов, О.Г. Король // Научный журнал Министерства обороны республики Сербия. Военно-технический весник, Белград, 2011. – Вып.4. – С. 15-39.

12. Смірнов О.А. Технології і стандарти комп'ютерних мереж: Навчальний посібник / О.А. Смірнов, С.П. Євсеєв, В.Ю. Жукарев, В.Є. Сорокін, О.Г. Король, Є.В. Мелешко. – Кіровоград: Вид. КНТУ, 2011. – 456 с.

Поступила в редколлегию 1.07.2012

Рецензент: д-р техн. наук, проф. А.А. Кузнецов, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

АНАЛІЗ СТАНУ ПРОТОКОЛІВ БЕЗПЕКИ СУЧАСНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

О.Г. Король

Аналізуються вимоги, пропоновані до сучасних телекомунікаційних систем і мереж, зокрема аналізуються вимоги, пропоновані до показників якості передачі даних в інфокомунікаційних системах спеціального призначення (на прикладі телекомунікаційної мережі національної системи масових електронних платежів). Розглядаються протоколи мережної безпеки найпоширеніших телекомунікаційних Ір-мереж, досліджуються особливості забезпечення цілісності, автентичності й конфіденційності передачі пакетів даних.

Ключові слова: *телекомунікаційні системи, протоколи мережної безпеки, цілісність, автентичність, конфіденційність.*

ANALYSIS OF THE CONDITION PROTOCOL TO SAFETY OF THE MODERN TELECOMMUNICATION NETWORKS

O.G. Korol

The requirements are analyzed to modern telecommunication systems and networks, especially requirements to factor quality data communication in telecommunication system of the special purpose (on example of the telecommunication network of the national system of the mass electronic payments). They Are Considered protocols to network safety telecommunication IP-networks, are researched particularities of the provision to wholeness, authenticity and confidentiality of the transmission package data.

Keywords: *telecommunication systems, protocols to network safety, wholeness, authenticity, confidentiality.*