С. В. Запечников

БЕЗОПАСНОСТЬ КАНАЛОВ ПЕРЕДАЧИ ДАННЫХ В ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЯХ

Введение

Традиционно основной сферой применения средств криптографической защиты информации были и остаются сети и системы защищенной связи. Современные информационно-телекоммуникационные системы нередко объединяют весьма значительное число абонентов, измеряемое десятками и сотнями тысяч, каждый из которых обладает некоторым количеством криптографических ключей. Нередко количество участников системы заранее не определено: одни из них могут добавляться в систему в процессе ее работы, другие — по разным причинам выбывать из нее. В таких системах вероятность утраты или компрометации ключей, по крайней мере, у части участников становится весьма высокой. Полный и объективный централизованный контроль за всеми пространственно распределенными абонентами сети связи и их ключами становится невозможен. В связи с этим выдвигается задача такого структурирования криптосистемы и такой организации работы с ключами, которая рационально сочетает надежность, криптографическую стойкость, управляемость и практичность системы для абонентов.

1. Особенности криптографической защиты виртуальных частных сетей

Основная мировая тенденция — ориентация на построение телекоммуникационных сетей на базе архитектуры TCP/IP. В связи с этим широкое развитие получили системы защищенной связи на основе открытых сетей связи общего пользования — *виртуальные частные сети* (VPN — Virtual private networks), реализуемые на базе средств шифрования и аутентификации на различных уровнях стандартизованной коммуникационной архитектуры TCP/IP. Виртуальная частная сеть (ВЧС) представляет собой совокупность защищенных двухточечных каналов связи, которые могут быть организованы либо между оконечными абонентами, либо между узлами сети, защищая весь тракт передачи данных или его часть. ВЧС — одни из наиболее востребованных средств защиты информации в современных сложных информационно-телекоммуникационных системах с большим числом участников. В принципе организация каналов и сетей защищенной связи возможна множеством различных способов и на различных уровнях архитектуры TCP/IP. Перечислим основные из них:

1) на уровне каналов (сетевого интерфейса) — средствами протокола L2TP (RFC 2661, 2888);

2) на уровне межсетевого взаимодействия — средствами рамочной модели безопасности (security framework) IPSec (RFC 2401), в частности средствами протоколов AH (RFC 2402) и

ESP (RFC 2403 – 2406), а также средствами пакетной трансляции, туннелирования трафика и (редко) трансляции сетевых адресов, что обычно выполняется межсетевыми экранами;

3) на транспортном уровне — средствами протоколов SSL, TLS (RFC 2246) и SOCKS v 5 (RFC 1928, 1961);

4) на прикладном уровне — средствами протоколов S/MIME, S-HTTP, PGP, SET, отчасти также средствами модели IPSec, из которой протокол IKE (RFC 2409) и методы распределения ключей ISAKMP (RFC 2408) и Oakley (RFC 2412) относятся к прикладному уровню.

Из всего многообразия перечисленных методов наиболее востребован на сегодняшний день способ организации ВЧС на основе протоколов модели IPSec. Он поддерживается большинством ведущих мировых производителей коммуникационного оборудования, таких как IBM, Cisco, Juniper, Nortel и др. Примером средств реализации ВЧС может служить серия продуктов eNetwork корпорации IBM. Семейство продуктов eNetwork включает в себя серверные компоненты: межсетевой экран IBM eNetwork Firewall for AIX, предназначенный для работы под управлением ОС AIX V4.3 и выше, средства ВЧС, встроенные в маршрутизаторы IBM Nways Router 2210/2216/3746, встроенные средства поддержки ВЧС в ОС OS/390 Server, а также клиентские компоненты IBM SecureWay VPN Client для различных ОС: AIX IPSec Client, Windows IPSec Client, OS/2 TCP/IP V4.1 и выше, Windows 95 Comms Suite. Реализация ВЧС на платформе eNetwork полностью соответствует архитектуре IPSec, но дополнена протоколом обновления ключей IPSP собственной разработки IBM. Вследствие этого продукты eNetwork совместимы с большим набором аппаратных и программных средств других фирм-производителей.

В отечественных продуктах для организации ВЧС используются как протоколы IPSec, так и собственные протоколы для транспортировки защищенных пакетов через IP-сеть, обеспечивая совместимость на уровне протокола IP либо на уровне заголовков IP-пакетов. Среди известных отечественных средств реализации ВЧС можно выделить следующие продукты: широкополосный аппаратный IP-шифратор «Заслон» разработки ЗАО «Голлард», аппаратно-программный комплекс «Континент-К» разработки НИП «Информзащита», аппаратно-программный комплекс «ШИП» и программный комплекс «Игла-П» разработки МО ПНИЭИ, программный комплекс ViPNet и аппаратно-программный комплекс «Домен-К» разработки ОАО «ИнфоТеКС», программно-аппаратный комплекс «ФПСУ-IP» разработки ЗАО «Амикон», семейство продуктов для организации VPN «Застава» разработки Центра защиты информации ООО «Конфидент» (г. Санкт-Петербург), VPN-шлюз «Тропа-Джет» разработки ЗАО «Инфосистемы Джет», комплекс SmartNet разработки ЗАО «Лан Крипто», аппаратное средство криптографической защиты «Вектор» разработки СЦПС «Спектр» и Центра речевых технологий, криптомаршрутизатор КМ и многоуровневый криптомаршрутизатор DioNIS FW/KM разработки НИИ «Энергия» и ООО «Фактор-ТС». Этим перечнем далеко не исчерпываются все существующие отечественные продукты.

Дополнительные функциональные возможности ВЧС включают фильтрацию трафика, трансляцию сетевых адресов, обеспечение качества сервиса, поддержку протоколов канального уровня, поддержку удаленной аутентификации, дистанционное управление сетью.

Принципам построения ВЧС и способам их реализации посвящена обширная отечественная и зарубежная литература, из которой автор руководствовался в первую очередь фундаментальной трехтомной работой [1–3].

Развитием идеологии ВЧС стала идея построения виртуальных локальных сетей (VLAN – Virtual Local area networks) за счет логического разграничения фрагментов физической сети передачи данных и взаимной изоляции трафика в этих фрагментах путем шифрования и аутентификации IP-пакетов.

Основной практической целью применения ВЧС является организация системы защищенных каналов передачи данных между узлами компьютерной сети, обеспечивающих секретность и аутентичность передаваемой по ним информации вне зависимости от прикладных программ, которые используют эти каналы. Характерной особенностью ВЧС является использование только симметричных криптосхем для обеспечения секретности и аутентичности трафика, который, как правило, характеризуется большим объемом. Вместе с тем для распределения общих секретных ключей могут быть применены различные способы: от «ручной» передачи ключа под физической охраной до разнообразных протоколов распределения ключей (ПРК).

Далее в статье рассматриваются типовые технические решения по построению каналов ВЧС с точки зрения структуры их ключевых систем (КС) и влияния этой структуры на безопасность сети защищенной связи. Анализ намеренно проводится автором без привязки к конкретным аппаратным или программным средствам ВЧС, чтобы сохранить объективность и не создавать рекламу или «антирекламу» каким-либо отечественным или зарубежным продуктам. Однако, обладая соответствующей технической и эксплуатационной документацией, читатель довольно легко сможет применить изложенные в статье результаты для выявления сильных и слабых сторон множества средств организации ВЧС, представленных на российском рынке. Нередко в одном продукте сочетаются сразу несколько способов организации каналов ВЧС.

2. Каналы ВЧС с распределением общих секретных ключей «внешними» средствами

Самый простой способ организации ВЧС, состоящей из набора виртуальных защищенных каналов двусторонней связи, состоит в том, что каждому узлу сети выдается множество ключей парно-выборочной связи для взаимодействия со всеми другими узлами сети, т. е. используется модель полной ключевой матрицы. Пользуясь предложенным автором статьи способом модельного представления КС [4], структуру КС такой ВЧС можно представить графом, изображенным на рис. 1. Здесь и далее вершины графа соответствуют объектам ключевой системы (ОКС); ребра, изображенные пунктиром, показывают отношения параметрической зависимости между ОКС; ребра, изображенные тонкой линией, — отношения функциональной зависимости первого рода; ребра, изображенные жирной линией, — отношения функциональной зависимости второго рода.

Структура КС отличается хорошо выраженной регулярностью и характеризуется максимальной устойчивостью к компрометациям ключей. Поскольку узлов сети может быть очень много, для хранения ключей нередко требуется весьма значительный объем памяти. Кроме того, такой способ сильно затрудняет масштабирование ВЧС, так как введение каждого нового узла сети требует записи ключей парно-выборочной связи на все остальные узлы.

Узлы такой сети в отечественной терминологии чаще всего называются межсетевыми экранами (МЭ), в зарубежной терминологии — серверами ВЧС. Все ключи должны храниться в готовом виде на узлах ВЧС, а их распределение по узлам осуществляется какими-либо «внешними» по отношению к ним способами. Один возможный способ заключается в том, что персонал, обслуживающий ВЧС, отправляется в командировки и развозит ключи вручную. Другой способ — ключи предварительно устанавливаются в аппаратуру при получении ее от производителя и рассылаются вместе с самой аппаратурой при монтаже сети для заказчика. Третий способ — для инсталляции ключей используются каналы защищенной связи между удаленными администраторами и узлами ВЧС (несмотря на то что такой способ нередко «официально» запрещен или не документирован, на практике администраторы ВЧС все равно широко используют его).

В последнем случае общие секретные ключи для защиты канала удаленного администрирования вырабатываются с помощью какого-либо протокола распределения ключей: Диффи — Хеллмана, SSL, TLS и др. (систематичный обзор этих протоколов можно найти в учебном пособии [5]). На рис. 2 для примера показана структура КС канала, в котором используется широко известный

протокол распределения ключей STS, предложенный в работе [6]. Этот протокол основан на вычислительно сложной задаче Диффи — Хеллмана, но дополнительно использует симметричную схему шифрования и две схемы электронной цифровой подписи вида $S_X(m)=(H(m))^{d_X} \bmod n_X$, $X=\{A,B\}$, $H(m)<n_X$ (на эту роль подходят схемы RSA и Рабина). Протокол обеспечивает аутентификацию его участников, аутентификацию общего секретного ключа и совершенную опережающую безопасность. Похожий протокол рекомендован в международном стандарте ISO/IEC 9798-3.

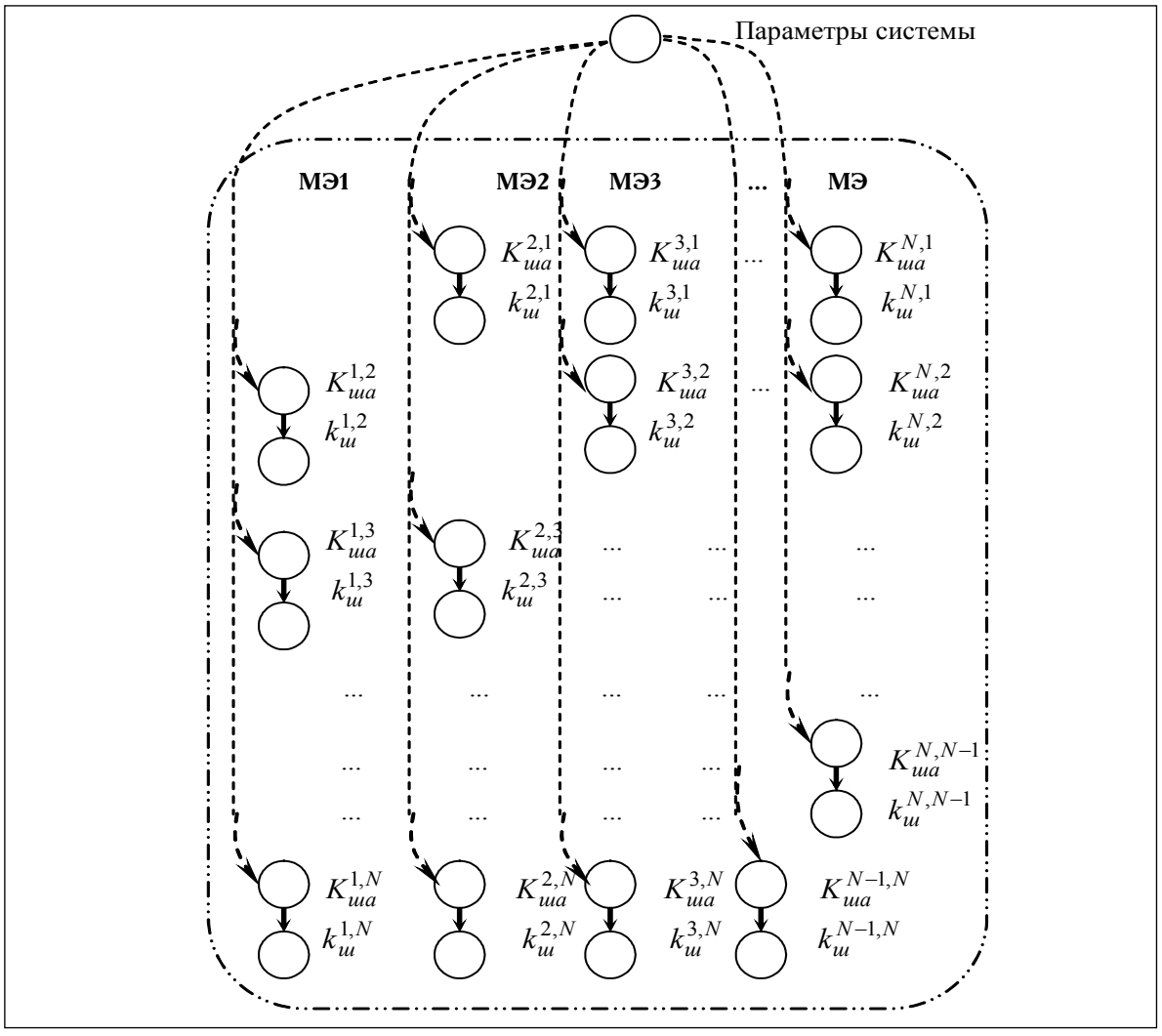


Рис. 1. Структура КС типового технического решения ВЧС с каналами, в которых общие секретные ключи распределяются «внешними» по отношению к ним средствами

Обозначения: МЭ — межсетевой экран, $K_{ша}^{X,Y}$ — долговременные парно-выборочные ключи шифрования ключей и аутентификации пары МЭ X и Y, $k_ш^{X,Y}$ — сеансовые парно-выборочные ключи для шифрования IP-пакетов, передаваемых от МЭ X к МЭ Y, N — общее количество МЭ в ВЧС.

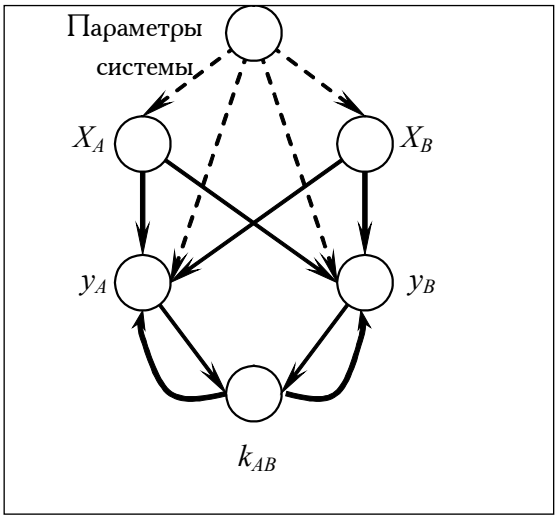


Рис. 2. Структура КС виртуального канала, в котором для распределения общих секретных ключей используется протокол STS

Обозначения: X_A – ОКС «Долговременные ключи A», X_B – ОКС «Долговременные ключи B», y_A – ОКС «Разовые ключи A», y_B – ОКС «Разовые ключи B», k_{AB} – ОКС «Общий секретный ключ A и B».

3. Каналы ВЧС типа «клиент – сервер»

Удобным для практики является решение, представляющее собой своеобразный компромисс между моделью полной ключевой матрицы и другим крайним случаем, когда всем узлам ВЧС мог бы быть выдан один общий секретный ключ. МЭ – это чаще всего специализированные аппаратно-программные комплексы, достаточно хорошо защищенные и находящиеся под контролем администраторов. МЭ получают секретные ключи, называемые системными или первичными (обозначим их K_S), предназначенные для обслуживания группы «приписанных» к ним клиентов. Группу клиентов в разных случаях может обслуживать либо только один МЭ, либо ограниченное множество МЭ (на которых установлены соответствующие ключи), либо все МЭ сети. На компьютерах клиентов, которые чаще всего хуже защищены и не находятся под непосредственным контролем администраторов безопасности, устанавливаются собственные мастер-ключи клиентов $k_{кл.}$, которые служат для организации защищенных виртуальных каналов между клиентом и обслуживающим его МЭ. При взаимодействии с МЭ клиентам запрещено «видеть» ключ K_S. Чтобы МЭ и клиент могли взаимодействовать, ключ $k_{кл.}$ вычисляется МЭ из серийного номера устройства клиента $n_{кл.}$ (возможные варианты – из номера лицензии на ПО, из MAC-адреса сетевой карты, из других уникально идентифицирующих его данных) при помощи некоторой (как правило, секретной или не разглашаемой разработчиком средств ВЧС) операции вида $f(K_S, n_{кл}) \rightarrow k_{кл}$, где f – некоторая однонаправленная функция (с точки зрения криптографии желательно, чтобы это была псевдослучайная функция). Следовательно, каждый МЭ, получив $n_{кл.}$, может использовать системный ключ для восстановления $k_{кл.}$. Затем оба устройства могут использовать $k_{кл.}$ в качестве общего секретного ключа для выработки сеансовых ключей шифрования и (или) аутентификации сообщений. На рис. 3 показана примерная структура КС такого канала.

Несомненным достоинством такого подхода является сокращение общего количества ключей в ВЧС и строго упорядоченная система доступа клиентов к ВЧС, недостатком – тот факт, что весь трафик клиента неизбежно расшифровывается на обслуживающем его МЭ и

далее шифруется на других ключах для передачи по виртуальным каналам «МЭ – МЭ» или «МЭ – другой клиент», поэтому МЭ должны пользоваться безусловным доверием со стороны клиента. Некоторые средства организации ВЧС допускают, чтобы виртуальный канал между МЭ и клиентом «прозрачно» проходил через другие МЭ, однако при этом часть функций для клиента может быть ограничена.

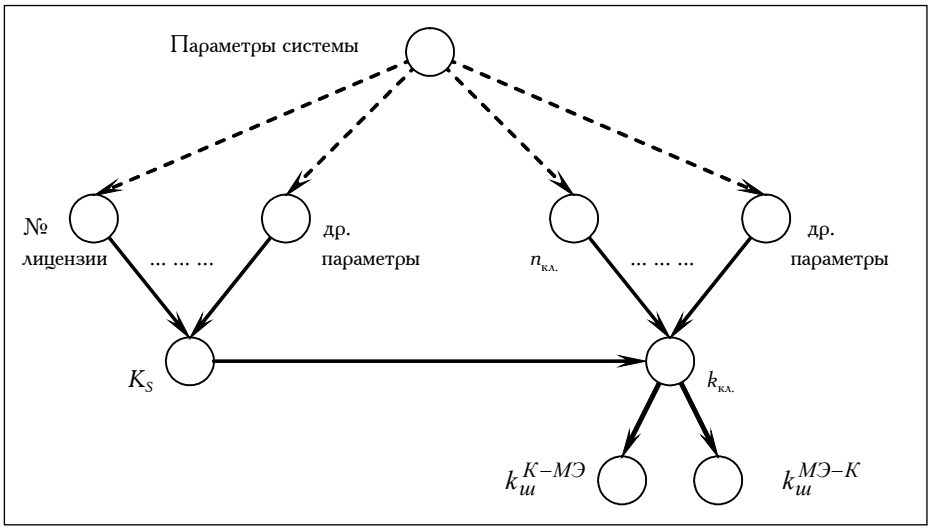


Рис. 3. Структура КС виртуального канала типа «клиент – сервер», в котором общие секретные ключи вырабатываются узлами сети

Обозначения: МЭ – межсетевой экран, K_S – системный (или первичный) ключ МЭ, $k_{кл.}$ – мастер-ключ клиента, $K_{ш}^{К-МЭ}$ и $K_{ш}^{МЭ-К}$ – сеансовые ключи парной связи МЭ и их клиентов.

4. Каналы ВЧС с распределением общих секретных ключей системными средствами

Альтернативный способ организации ВЧС состоит в том, что каждая пара узлов сети (независимо от их роли серверов или клиентов) имеет ключи парно-выборочной связи, которые генерируются и периодически обновляются путем выполнения протоколов распределения ключей. Таким образом, протокол взаимодействия каждой пары узлов ВЧС включает «рабочие» фазы, когда канал используется для передачи пользовательской информации, и «служебные» фазы, когда канал используется для взаимной аутентификации сторон, обновления ключей, согласования параметров «рабочей» фазы и пр. Поскольку «служебная» фаза занимает относительно небольшую долю времени функционирования канала или вообще может выполняться параллельно с «рабочей» фазой по отдельному виртуальному каналу, эффективность такого способа довольно высока. Ярким примером реализации этой идеологии могут служить ВЧС на основе архитектурной модели IPSec.

Структура КС для одного виртуального канала ВЧС на базе модели IPSec, выраженная в терминах модели [4], показана на рис. 4. Относительно приведенной здесь структуры КС необходимо сделать несколько комментариев.

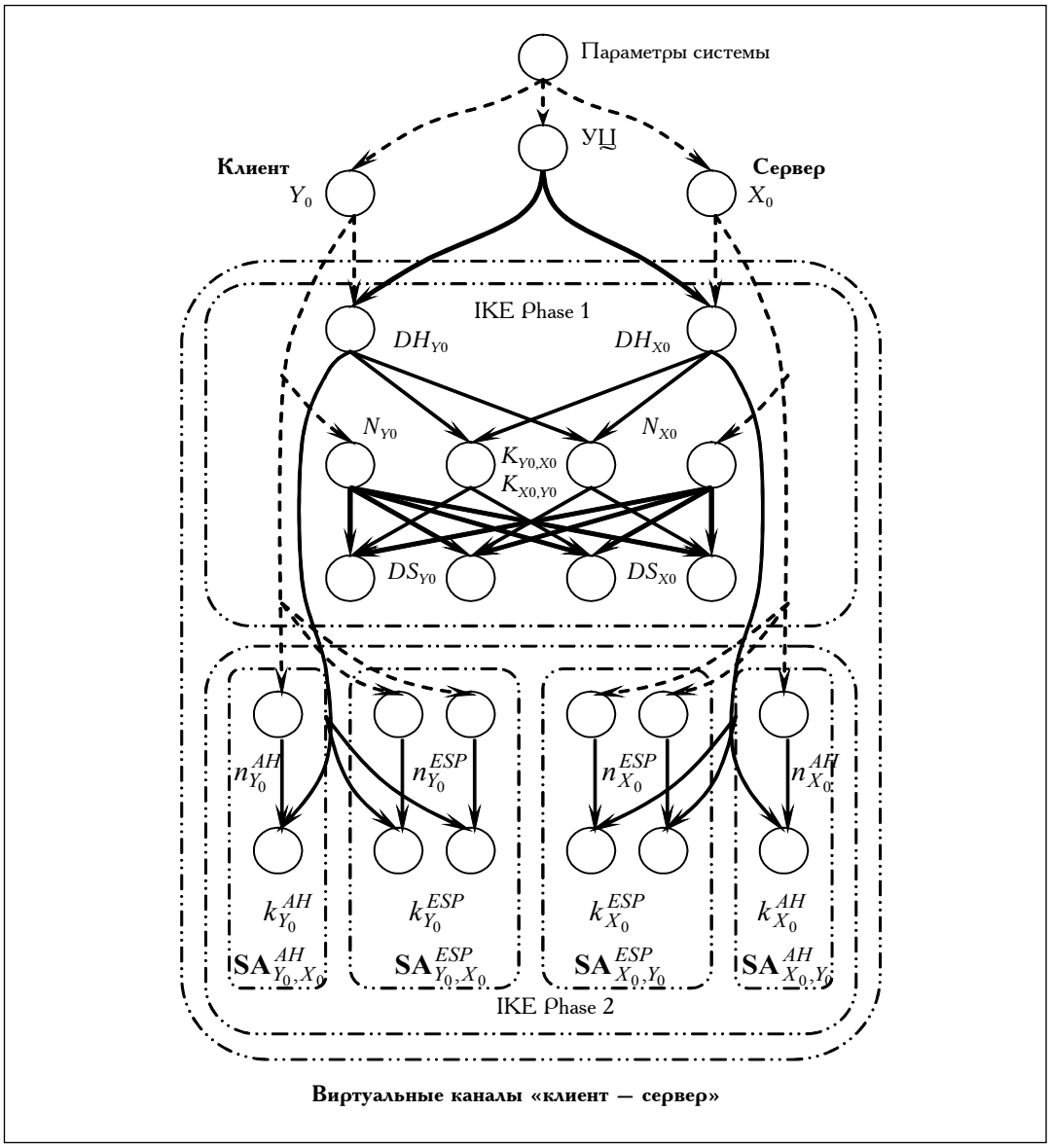


Рис. 4. Структура КС виртуального канала, в котором для распределения общих секретных ключей используются протоколы, рекомендованные моделью IPSec

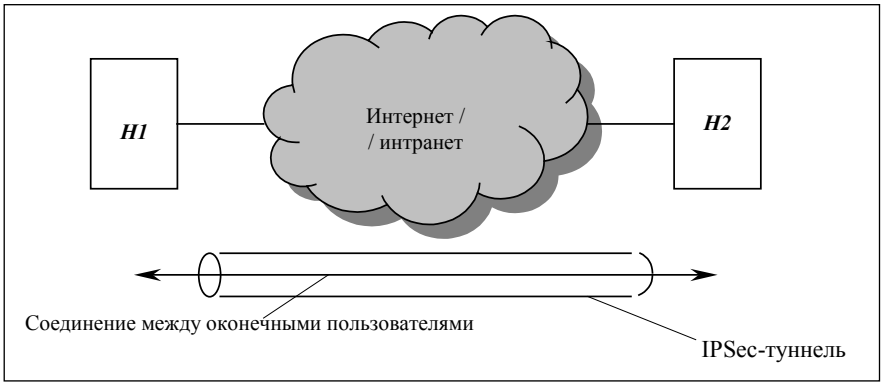
Обозначения: X_0 — сервер ВЧС (межсетевые экраны), Y_0 — клиент ВЧС, DH_{Xi}, DH_{Yj} — пары ключей Диффи — Хеллмана серверов и клиентов, $K_{Xi,Yj}$, $K_{Yj,Xi}$ — общие секретные ключи парно-выборочной связи, вырабатываемые в результате выполнения протокола IKE Phase 1, N_{Xi}, N_{Yj} — случайные величины, вырабатываемые в протоколе IKE Phase 1 и используемые в качестве ключа цифровой подписи, DS_{Xi}, DS_{Yj} — цифровые подписи, используемые для аутентификации общих секретных ключей в протоколе IKE Phase 1, n_{Xi}^{AH}, n_{Yi}^{AH}, n_{Xi}^{ESP}, n_{Yi}^{ESP} — случайные величины, используемые для генерации секретных ключей «защищенных ассоциаций» AH и ESP соответственно, k_{Xi}^{AH}, k_{Yi}^{AH}— секретные ключи шифрования «защищенных ассоциаций» AH, $k_{X_i}^{ESP}$,$k_{Y_j}^{ESP}$ — секретные ключи шифрования и аутентификации сообщений «защищенных ассоциаций» ESP.

Во-первых, структура КС показана в предположении, что виртуальный канал соединяет клиента Y_0 и сервер X_0. Для случаев, когда виртуальный канал соединяет два сервера X_i и X_j или двух клиентов Y_i и Y_j, она будет аналогична показанной на этом рисунке.

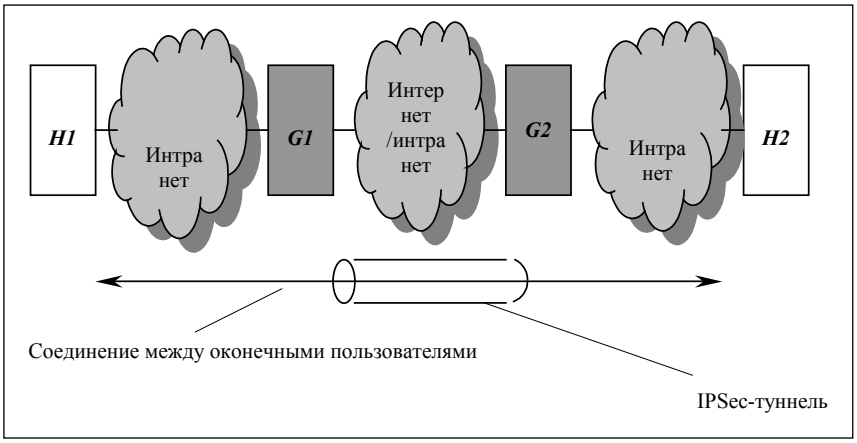
Во-вторых, предполагается, что для распределения начальных секретных ключей и обновления ключей используется режим IKE Phase 1 с выработкой общего секретного ключа по протоколу Диффи – Хеллмана и аутентификацией посредством цифровой подписи. В результате этого образуются защищенные ассоциации (SA – Security Association) для управления ключами обработки данных. Для распределения секретных ключей обработки данных используется режим IKE Phase 2. Каждая SA предназначена для защиты односторонней передачи данных. Для удостоверения пар ключей, участвующих в выполнении протокола Диффи – Хеллмана, используются сертификаты, для чего в сети внешними средствами должна поддерживаться инфраструктура открытых ключей. (Альтернативным способом транспортировки общего секретного ключа может служить протокол TLS.)

Безопасность такой КС можно усилить, применив к ключам шифрования и аутентификации SA схему эволюции ключей, обеспечивающую совершенную опережающую безопасность.

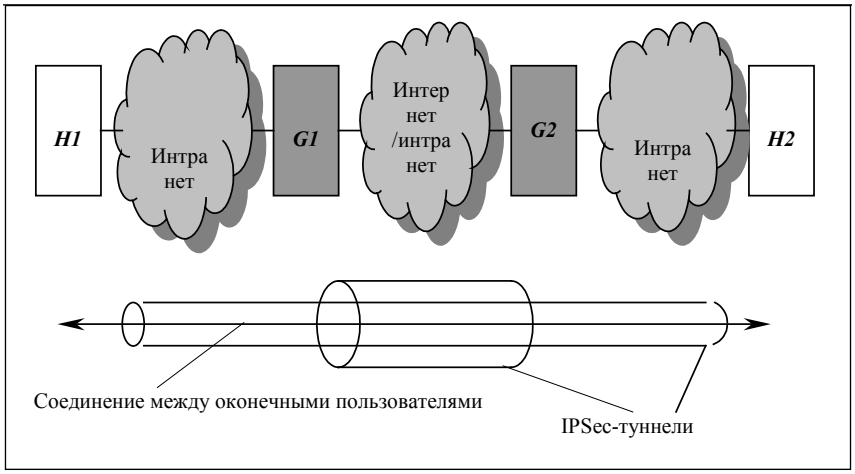
Архитектурой IPSec предусмотрена поддержка ручных и автоматизированных способов образования виртуальных каналов — туннелей — и различных режимов передачи данных: только с шифрованием, только с обеспечением аутентичности, с шифрованием и последующей генерацией кода аутентификации сообщений, с генерацией кода аутентификации сообщений и последующим шифрованием, без защиты открытого текста. Все это создает богатые функциональные возможности и позволяет конфигурировать виртуальные каналы самыми различными способами (Рис. 5), в том числе создавать «вложенные» друг в друга виртуальные каналы, «цепочки» каналов между узлами сети, «сквозные» каналы между оконечными пользователями.



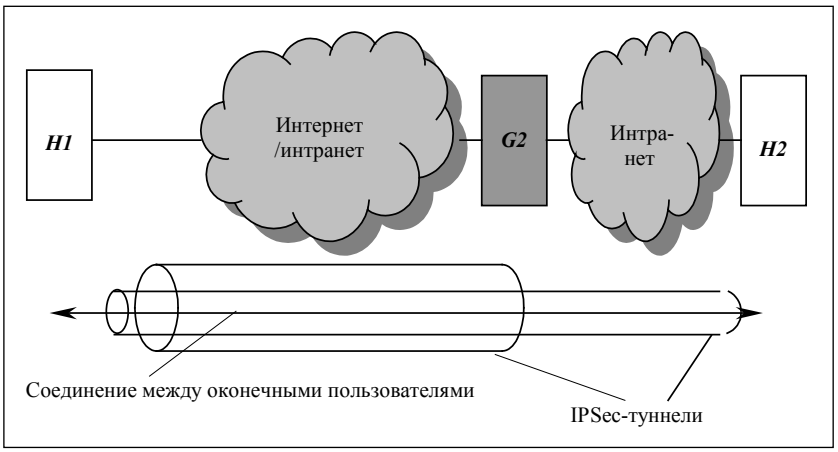
а) обеспечение безопасности соединений между оконечными пользователями;



б) базовый режим поддержки ВЧС;



в) обеспечение безопасности соединений между оконечными пользователямис поддержкой ВЧС;



г) защита удаленного доступа

Рис. 5. Конфигурации виртуальных каналов, построенных в соответствии со спецификацией IPSec

Анализ КС ВЧС с каналами, построенными в соответствии со спецификациями архитектуры IPSec, позволяет отметить следующие характерные ее особенности:

- единая КС, образованная за счет формирования среды ВЧС, позволяет строить защищенные виртуальные каналы в произвольных комбинациях между клиентами и серверами ВЧС, в том числе каналы любой степени «вложенности» друг в друга;
- КС обеспечивает аутентичное распределение парно-выборочных ключей между любой парой участников ВЧС: как серверов, так и клиентов;
- стойкость КС к компрометациям ключей обеспечивается за счет того, что все пути в графе, обозначающие направления компрометации парно-выборочных ключей SA, разделены.

Заключение

На основе предложенной в работе классификации типовых методов организации защищенных каналов ВЧС выявлены и проанализированы характерные особенности структуры их ключевых систем, отмечены их преимущества и недостатки, выявлены факторы, влияющие на безопасность сети защищенной связи. Полученные результаты представляют интерес для проектировщиков

ВЧС и системных аналитиков, осуществляющих поиск эффективных решений задач, связанных с построением или интеграцией защищенных информационно-телекоммуникационных систем, и выбор рациональных практических решений.

СПИСОК ЛИТЕРАТУРЫ:

1. A comprehensive guide to Virtual private networks, Volume I: IBM Firewall, Server and Client solutions: ITSO Redbook No. SG24–5201–00 [электронный ресурс] / M. Murhammer [и др.]. – IBM, 1998. – 250 рр. – URL: http://www.redbooks.ibm.com.
2. A comprehensive guide to Virtual private networks, Volume II: IBM Nways Router solutions: ITSO Redbook No. SG24–5234–01 [электронный ресурс] / M. Murhammer [и др.]. – IBM, 1999. – 642 рр. – URL: http://www.redbooks.ibm.com.
3. A comprehensive guide to Virtual private networks, Volume III: Cross-platform key and policy management: ITSO Redbook No. SG24–5309–00 [электронный ресурс] / M. Murhammer [и др.]. – IBM, 1999. – 686 рр. – URL: http://www.redbooks.ibm.com.
4. *Запечников С. В.* Модельное представление ключевых систем средств криптографической защиты информации // Безопасность информационных технологий. 2008. № 4. С. 84–92.
5. *Запечников С. В.* Криптографические протоколы и их применение в финансовой и коммерческой деятельности: учеб. пособие для вузов. М.: Горячая линия – Телеком, 2007. – 320 с.
6. *Diffie W., van Oorschot P. C., Wiener M. J.* Authentication and authenticated key exchanges // Designs, Codes and Cryptography. 1992. №. 2. P. 107–125.