УДК 004.01

# ПРОГРАММНЫЕ ПРОДУКТЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ

***© 2018 Д. А. Жайворонок, А. С. Лукьянов***

*Воронежский институт МВД России (г. Воронеж, Россия)*

*В данной статье рассматриваются вопросы, повышения уровня безопасности протоколов Интернета, увеличению числа механизмов защиты в Интернете и повышению предоставляемого ими уровня безопасности. Также указываются ключевые области применения механизмов защиты, отмечена необходимость защиты сетевой архитектуры от неавторизованного мониторинга и управления сетевым трафиком, а также необходимость защиты сквозного трафика путем аутентификации и шифрования.*

*Ключевые слова: спецификация IPSec, защищенное соединение, удаленный доступ, защищенный протокол Интернета, IP-протокол, локальными сетями, трафик.*

Сегодня спецификация IPSec (Secure Internet Protocol – защищенный протокол Интернета) существует в виде набора стандартов [3] Интернета.

Спецификация IPSec позволяет обезопасить взаимодействие в локальной сети, а также при передаче данных через частные и общественные глобальные сети, и Интернет.

Ниже приводятся некоторые примеры применения IPSec.

Защищенное соединение с филиалом через Интернет. Компания может развернуть безопасную виртуальную частную сеть в Интернете или в другой общественной глобальной сети. В результате коммерческая фирма получает возможность использовать Интернет для большей части своих нужд, сократив использование частных сетей и, таким образом, снизив финансовые затраты и накладные расходы на сетевое администрирование.

Защищенный удаленный доступ через Интернет. Конечный пользователь, чья система оборудована защищенными IP-протоколами, может установить соединение с местным поставщиком услуг Интернета и получить защищенный доступ к сети компании. Это позволяет снизить транспортные расходы сотрудников.

Установка соединений с партнерами через экстранет или интранет. Защищенный протокол может использоваться для установки защищенного соединения с другими организациями, для гарантирования аутентификации и конфиденциальности, для обмена ключами.

Повышение уровня безопасности в электронной коммерции [1]. Несмотря на то, что некоторые веб-приложения и программы для электронной коммерции оснащены встроенными протоколами защиты, использование защищенного протокола позволяет повысить уровень безопасности. IPSec гарантирует, что для всего назначенного сетевым администратором трафика применяется шифрование и аутентификация. Для этого к уровню безопасности, предоставляемому приложением, добавляется дополнительный уровень безопасности.

Основная особенность спецификации IPSec, обеспечивающая поддержку всех этих приложений, заключается в том, что она позволяет шифровать и аутентифицировать весь трафик на уровне протокола IP. Таким образом, могут быть защищены все распределенные приложения, включая удаленную регистрацию, модель клиент-сервер, электронную почту, передачу файлов, веб-доступ и т. д.

На рисунке 1 показан типичный пример использования, защищенного протокола. Организация управляет локальными сетями в удаленных друг от друга филиалах. В каждой сети поддерживается незащищенный IP-трафик.

Для внешнего трафика, проходящего через частные или общественные глобальные сети, используется защищенный прото-

Жайворонок Денис Александрович – Воронежский институт МВД России, доцент кафедры инфокоммутационных систем и технологий, к. т. н., доцент, e-mail: d.zh007@bk.ru.

Лукьянов Александр Сергеевич – Воронежский институт МВД России, старший преподаватель кафедры инфокоммутационных систем и технологий, к. т. н., e-mail: las92@yandex.ru.

кол. Этот протокол работает в таких сетевых устройствах, как маршрутизатор и брандмауэр, соединяющих локальную сеть с внешним миром [3].

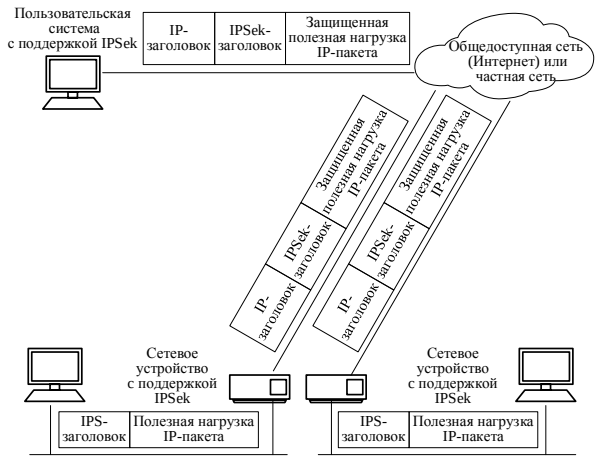


Рисунок 1. Пример использования защищенного протокола.

Поддерживающее защищенный протокол сетевое устройство, как правило, шифрует и сжимает весь исходящий трафик и дешифрирует, и распаковывает весь входящий трафик. Эти операции являются прозрачными для рабочих станций и серверов локальной сети. Защищенная передача данных также может предоставляться индивидуальным пользователям, соединяющимся с глобальной сетью по телефонной линии.

Ниже перечислены достоинства спецификации IPSec.

Когда защищенный протокол реализуется на брандмауэре или маршрутизаторе, он обеспечивает высокий уровень безопасности всего трафика, пересекающего границы сети. Трафик в пределах компании или рабочей группы не требует накладных расходов на поддержание безопасности.

Защищенный протокол, реализованный на брандмауэре, устойчив к попыткам его обойти, если весь входящий трафик должен использовать протокол IP, а брандмауэр представляет собой единственную точку входа из Интернета в корпоративную сеть.

Защищенный протокол функционирует под транспортным уровнем (TCP, UDP), поэтому он прозрачен для приложений. Нет необходимости изменять программное обеспечение на пользовательской системе или на сервере, если защищенный протокол реализован на брандмауэре или маршрутизаторе. Даже если защищенный протокол реализован на оконечных системах, программное обеспечение более высоких уровней стека протоколов, включая прикладной, не затрагивается.

Работа защищенного протокола может быть прозрачной для конечных пользователей. Нет необходимости переобучать пользователей.

Защищенный протокол при необходимости может обеспечивать безопасность отдельных пользователей. Это может пригодиться в плане предоставления безопасного доступа удаленным сотрудникам или развертывания внутри организации защищенной виртуальной подсети для наиболее важных с точки зрения безопасности приложений.

Спецификация IPSec предоставляет три основные функции: отдельную функцию аутентификации, известную как функция AH (Authentication Header – заголовок аутентификации), комбинированную функцию аутентификации/шифрования, называемую функцией ESP (Encapsulating Security Payload – инкапсулированная защищенная полезная нагрузка), и функцию обмена ключами. Для виртуальных частных сетей, как правило, желательны аутентификация и шифрование, так как одинаково важно гарантировать, во-первых, что неавторизованные пользователи не проникают в виртуальную частную сеть, и, во-вторых, что злоумышленники в Интернете не смогут читать сообщения, посланные по виртуальной частной сети. Поскольку желательно, чтобы были выполнены обе функции, в большинстве реализаций, как правило, применяется функция ESP, а не AH. Функция обмена ключами позволяет обмениваться ключами вручную, а также автоматически.

Текущая спецификация IPSec требует поддержки стандарта шифрования данных (DES), но также могут использоваться другие алгоритмы шифрования. В связи с серьезными сомнениями по поводу надежности алгоритма DES весьма

вероятно, что широкое применение получат другие алгоритмы, такие как тройной алгоритм DES. Для аутентификации требуется относительно новая схема, известная как HMAC.

Функция ESP поддерживает два режима работы: транспортный и туннельный. Транспортный режим, в первую очередь, обеспечивает защиту протоколов верхнего уровня. То есть защита транспортного режима распространяется на полезную нагрузку IP-пакета (рис. 2, а). Как правило, транспортный режим используется для сквозной передачи данных между хостами

(например, клиентом и сервером или двумя рабочими станциями) [4]. В транспортном режиме функция ESP зашифровывает и, по желанию, аутентифицирует полезную нагрузку IP-пакета, но не IP-заголовок (рис. 2, б). Такая конфигурация полезна для относительно небольших сетей, в которых каждый хост и каждый сервер поддерживают спецификацию IPSec. Однако для развитой виртуальной частной сети значительно более эффективным является туннельный режим (рис. 2, в.)

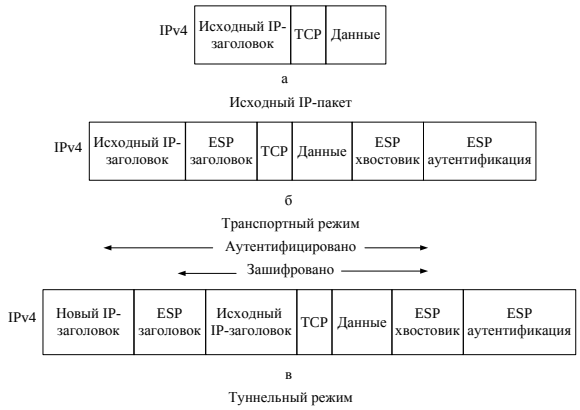


Рисунок 2. Сфера применения функции ESP.

Туннельный режим обеспечивает защиту всего IP-пакета. После того как к IP-пакету добавлены ESP-ноля, весь пакет трактуется как полезная нагрузка нового «выходного» IP-пакета с новым IP-заголовком. Оригинальный внутренний пакет целиком путешествует через «туннель» от одной точки IP-сети к другой. Встречающиеся ему на пути маршрутизаторы не могут исследовать внутренний IP-заголовок. Поскольку оригинальный пакет инкапсулирован, у нового большего пакета могут быть совершенно другие адреса отправителя и получателя. Туннельный режим используется, когда один или оба конца соединения представляют собой защищенный шлюз, например, брандмауэр или маршрутизатор, на котором реализован защищенный протокол. В туннельном режиме несколько хостов в сетях, защищенных брандмауэрами, могут устанавливать защищенные соединения друг с другом, даже если на хостах и не реализован защищенный протокол. Незащищенные пакеты, генерируемые такими хостами, туннелируются через внешние сети при помощи программного обеспечения IPSec в брандмауэрах или защищенных маршрутизаторах, располагающихся на границе локальной сети.

## ЛИТЕРАТУРА

1. Нестеров С. В. Основы информационной безопасности / С. В. Нестеров // Лань. – Москва, 2016. – 324 с.

2. Олифер В. А. Компьютерные сети. Принципы, технологии протоколы / В. А. Олифер // Питер. – Санкт-Петербург, 2016. – 412 с.

3. Родичев Ю. С. Нормативная база и стандарты в области информационной безопасности / Ю. С. Родичев // Питер. – Санкт-Петербург, 2017. – 256 с.

4. Столлингс В. Передача данных / В Столлингс // Питер. — Санкт-Петербург, 2015. – 750 с.

## SOFTWARE PROVIDERS FOR SECURITY OF VIRTUAL PRIVATE NETWORKS

***© 2018 D. A. Zhaivoronok, A. S. Lukiyanov***

*Voronezh institute of the Interior of Russia (Voronezh, Russia)*

*This article examines the issues, increasing the level of security of Internet protocols, increasing the number of security mechanisms on the Internet and increasing the level of security provided by them. Key areas of application of protection mechanisms are also indicated the need to protect the network architecture from unauthorized monitoring and management of network traffic, as well as the need to protect end-to-end traffic through authentication and encryption.*

*Key words: IPSec specification, secure connection, remote access, secure Internet protocol, IP-protocol, local networks, traffic.*