УДК 004.056.55

ЗАЩИТА КАНАЛА ПЕРЕДАЧИ ДАННЫХ НА БАЗЕ ТЕХНОЛОГИИ VPN В СИСТЕМАХ ЭКОЛОГИЧЕСКОГО МОНИТОРИНГА

Н.Л. Корепанова, М.А. Лебедева

Севастопольский государственный университет
г. Севастополь, ул. Университетская, 33
E-mail: nat270702@gmail.com

Рассмотрены средства защиты каналов передачи данных в автоматизированных системах экологического мониторинга на базе технологии виртуальных частных сетей. Обеспечение конфиденциальности и целостности передаваемых данных основано на использовании стойких симметричных шифров и криптографических хеш-функций в сочетании с механизмами аутентификации и туннелирования. Указаны подходы к выбору криптографических алгоритмов, применяемых в виртуальных частных сетях. Выполнен анализ ресурсоемкости программной реализации некоторых криптографических алгоритмов, определены направления повышения производительности защищенного канала.

Ключевые слова: виртуальная частная сеть, туннелирование, криптография; блочные шифры; хэш-функции.

Поступила в редакцию: 29.05.2018.

Введение. Мониторинг и контроль состояния окружающей среды является важнейшей задачей современного общества. В соответствии с «Концепцией совершенствования системы мониторинга загрязнения окружающей среды с учетом конкретизации задач федерального, регионального и локального уровней на 2017–2025 годы», принятой в 2017 г., предусмотрено дальнейшее развитие систем мониторинговых наблюдений, которое невозможно без использования современных информационных технологий.

Применение информационных технологий в сфере экологического контроля и мониторинга предполагает разработку автоматизированных систем, основными функциями которых является измерение параметров окружающей среды (вода, воздух, почва), накопление и обработка информации, анализ данных и принятие решений о состоянии природных ресурсов.

Технология защиты каналов передачи данных. Как правило, системы экологического мониторинга включают датчики для измерения конкретных параметров окружающей среды или измерительные станции мониторинга, удаленный сервер с программным и аппаратным обеспечением и базой данных и средства передачи измерительной и управляющей информации по каналам связи. Использование в качестве коммутационного канала сети Internet позволяет организовать эффективный и надежный обмен данными между измерительными пунктами и центром обработки результатов измерений. К достоинствам такого канала относится также быстродействие и невысокая стоимость. Однако протоколы передачи информации по глобальной сети не обеспечивают защищенности данных.

Эффективным средством защиты передаваемой по сети информации, гарантии ее конфиденциальности и целостности является технология виртуальных частных сетей (VPN), которая заключается в создании защищенного канала поверх внешней сети, как правило, осуществляющей пакетную передачу данных: X.25, FR, ATM, IP (Internet). Наиболее популярны технологии VPN, рассчитанные на использование в среде Internet. Особенности инфраструктуры систем экологического контроля, объединяющих обрабатывающий сервер, удаленные посты контроля и локальные сети, требуют надежного канала связи для обмена данными. Технология виртуальной частной чети позволяет изолировать информацию, циркулирующую в системе мониторинга, от других потоков общедоступной сети путем применения

криптографических алгоритмов и методов идентификации и аутентификации в сочетании с механизмом туннелирования [1].

Туннелирование предполагает скрытие адресов отправителя и получателя и другой информации передаваемого пакета путем его инкапсуляции в пакет другого протокола и выполняется с целью защиты передаваемых данных и согласования разных транспортных протоколов. Для создания туннелей при построении VPN используют протоколы канального (PPTP, L2TP, MPLS), сетевого (IPSec, AH, ESP, IKE) и сеансового уровней (SSL, TLS).

Протоколы туннелирования имеют разные характеристики и выполняют различные задачи, поэтому на практике обычно применяют их комбинацию. Создание безопасного туннеля включает аутентификацию пользователя, шифрование данных пакета, вычисление хэш-функции и объединение с зашифрованными данными, инкапсуляцию полученного пакета в другой пакет. Эти функции выполняют VPN-агенты. Технически виртуальные частные сети строятся на базе брандмауэров, маршрутизаторов, аппаратного и программного обеспечения, сетевой операционной системы, что определяется особенностями реализации VPN-агентов в конкретной виртуальной частной сети.

Существуют российские и зарубежные программные и аппаратные решения, использующие различные протоколы и позволяющие создавать безопасные и быстродействующие каналы связи. К ним относятся аппаратно-программный комплекс Криптон-IP, решения ViPNet Custom российской компании «Инфотекс», «Микротест» на базе сертифицированных VPN-продуктов компании «Инфотекс», решение компании Cisco Systems и другие VPN сервисы.

Для обеспечения защищенной связи в автоматизированных информационных системах (АИС), объединяющих удаленные компьютеры и локальные сети, можно использовать продукты разных производителей. В этом случае средства защиты являются надстройкой над уже существующей системой. Однако такой подход не позволяет обеспечивать комплексную защиту информации. Кроме того, возникают сложности при сопряжении различных подсистем. Поэтому более перспективным является комплексный подход к разработке АИС. В этом случае подсистема защиты должна разрабатываться на этапе проектирования архитектуры системы. Подсистема защиты автоматизированной системы включает модули криптографической защиты, идентификации и аутентификации пользователей системы, фильтрации и экранирования сетевых потоков данных, средства туннелирования. При оценке качества реализации VPN необходимо учитывать безопасность передаваемой информации, быстродействие и надежность канала передачи данных

Криптографическая защита. Основную функцию обеспечения информационной безопасности канала связи выполняют модули криптографической защиты. Криптографическая защита в технологии VPN включает шифрование данных для защиты от несанкционированного доступа и вычисление хэш-функции для обеспечения целостности данных. Основным требованием к криптографическим алгоритмам является стойкость к криптоанализу. В существующих реализациях VPN используют такие алгоритмы шифрования, как 3DES. AES, RC4, RC6, ГОСТ 28147-89, которые относятся к блочным шифрам с длиной ключа 128-256 бит, что позволяют добиться высокой криптостойкости защиты. Для хеширования данных, как правило, используют алгоритмы MD5 и SHA.

При проектировании систем экологического мониторинга необходимо учитывать то обстоятельство, что такие системы могут входить в состав государственной системы управления природоохранной деятельностью. В этом случае в соответствии с законодательством Российской Федерации допускается использование средств криптографической защиты, сертифицированных ФСБ. При этом обязательными для применения являются следующие алгоритмы:

− ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры»;

− ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая

защита информации. Функция хеширования»;

− ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

ГОСТ Р 34.12-2015 содержит описание двух блочных шифра, получивших названия «Магма» и «Кузнечик». В отличие от нового шифра «Кузнечик» шифр «Магма» – это алгоритм ГОСТ 28147–89 с фиксированной таблицей замен. В редакции 1989 года набор подстановок наряду с ключом являлся секретной информацией, что создавало трудности при взаимодействии различных реализаций алгоритма. По основным параметрам криптостойкости ни из алгоритмов не обладает особым преимуществом перед другим.

Хэш-функция «Стрибог», описанная в ГОСТ Р 34.11-2012, создающая на выходе хеш-код размером 256 или 512 бит, отличается стойкостью к коллизиям, использованием хорошо изученных преобразований и высоким быстродействием. Параметры алгоритмов приведены в табл. 1.

Таблица 1. Параметры криптографических алгоритмов

Параметр	«Кузнечик»	«Магма»	«Стрибог»
Длина блока	128 бит	64 бит	512 бит
Длина ключа	256 бит	256 бит	–
Число раундов	10	32	12
Архитектура	Подстановочно-перестановочная сеть (LSX-шифр)	Сбалансированная сеть Фейстеля	Итерационная схема Меркля-Дамгарда
Описание ключа	Сеть Фейстеля как ключевое расписание	32-битные части секретного ключа в качестве раундовых ключей	–

Функции шифрования и хеширования в виртуальных частных сетях выполняют VPN-агенты. Для обеспечения высокой производительности VPN целесообразно использование низкоресурсной или легковесной криптографии, основная цель которой – минимизация ресурсов для реализации алгоритмов шифрования с сохранением их криптостойкости и быстродействия. Для таких алгоритмов должны выполняться ограничения: в случае аппаратной реализации – на площадь микросхемы, потребление энергии, время исполнения, для программной реализации – на размер кода, процессорные операции, размер памяти,

Ресурсная эффективность программной реализации характеризуется трудоемкостью алгоритма, определяющую используемые ресурсы процессора, и требуемым объемом памяти. Приближенная оценка ресурсов алгоритма [2]

$$\psi = c_1 \cdot F(n) + c_2 \cdot M + c_3 \cdot S, \qquad (1)$$

где F – трудоемкость алгоритма; M – число процессорных операций; n – вход алгоритма в битах; S – ресурс памяти; c_i – веса ресурсов, зависит от конкретной реализации.

Рассмотрим ресурсоемкость криптографических алгоритмов шифрования и вычисления хеш-функции при обработке одного блока данных.

В алгоритме «Магма» шифрование осуществляется за 32 раунда [3]. На каждом раунде используется относительно простая функция преобразования, состоящая из операции комбинирования входной половины 64-битного блока (ветви сети Фейстеля) с раундовым ключом – сложения их по модулю 2^{32}, подстановки, выполняемой независимо в восьми 4-битовых группах, битового сдвига результата подстановки, сложения по модулю 2 полученного результата с правой ветвью и обмена ветвей. 512-битная таблица замен представляет собой восемь узлов, содержащих 16 4-битовых элементов Входной ключ интерпретируется, как массив из 8 элементов по 32 бита. Для раундов с 1 по 8, с 9 по 16 и с 17 по 24 используются ключи из массива – с 1 по 8 соответственно. Для раундов с 25 по 32 эти ключи используются в обратном порядке.

Количество элементарных шагов алгоритма в шифре «Магма» при преобразовании одного блока: $M = 32 \cdot (1 + 8 + 1 + 1 + 1) = 394$. Ресурс памяти $S \approx 2 \cdot 32 + 512 + 32 + 32 + 32 =$ 672 бита.

Шифрование в алгоритме «Кузнечик» основано на последовательном применении десяти однотипных раундов, каждый из которых содержит три преобразования: побитовое сложение по модулю 2 128-битного блока и раундового ключом, преобразование блоком подстановок и линейное преобразование. Таблица подстановки используется для замены 16 8-битных частей блока. Линейное преобразование реализуется с помощью сдвигового регистра, работа которого состоит из 16 тактов. В алгоритме «Кузнечик» первые два раундовых ключа получаются разбиением входного ключа пополам. Затем, для выработки очередной пары раундовых ключей используется 8 итераций сети Фейстеля, где в качестве раундовых ключей используется результат подстановки и линейного преобразования алгоритма.

Количество элементарных шагов при обработки блока шифром «Кузнечик» составляет: $M = 2 \cdot (1 + 16 + 16) + 8 \cdot (4 \cdot (1 + 16 + 16 + 1 + 1) + 1 + 16 + 16) = 1450$. Ресурс памяти $S \approx 128 + 128 + 512 + 128 + 128 + 64 =$938 бит.

Алгоритм «Стрибог» обрабатывает блоки размером 512 бит, которые поступают на вход функции сжатия вместе с вычисленным на предыдущем шаге значением хэш-кода и номером блока [4]. При необходимости блок дополняется до нужного размера последовательностью 00…1. Алгоритм сжатия состоит из 12 шагов. На каждом шаге выполняются линейное преобразование, заключающееся в умножении блока на фиксированную матрицу байтов размерностью 64x64, перестановка байтов в соответствии с 64-элементной таблицей перестановок, замена каждого байта на основании таблицы замен размерностью 64 байта и сложение по модулю 2 полученного результата с раундовым ключом. Ключ на каждой итерации получают из ключа предыдущего раунда и описанной в алгоритме константы путем выполнения линейного преобразования, перестановок и подстановок.

Количество элементарных шагов алгоритма в алгоритме «Стрибог»: $M = 1 + 12 \cdot (1 + 64 + 64 + 64 * 16) + 1 + 1 = 13839$. Оценка ресурса памяти $S \approx 512 + 512 + 512 + 512 = 2048$ бит.

В криптографических алгоритмах трудоемкость зависит от объема входных данных n. В качестве оценок трудоемкости для алгоритмов «Магма», «Кузнечик» и «Стрибог» соответственно рассмотрим функции:

$$F_{\text{М}} = \frac{n}{64}\ F_K = \frac{n}{128}\ F_C = \frac{n}{512}.$$

Технология VPN предполагает пакетную передачу данных, поэтому в качестве параметра n выбрана длина пакета.

Зависимость трудоемкости от размера пакета для рассмотренных криптографических алгоритмов приведена на рис. 1.

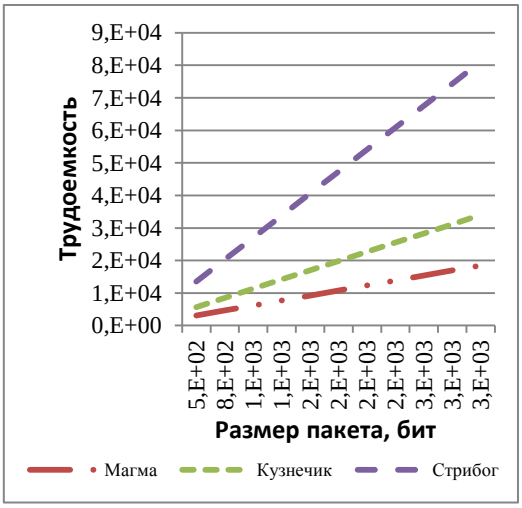

Рис. 1. Зависимость трудоемкости от размера пакета

Наименее ресурсоемким является алгоритм «Магма», однако для всех алгоритмов имеется возможность минимизации ресурсов, которая состоит в применении параллельных вычислений, ключевых расписаний, использовании графических процессоров, переходе к аппаратной реализации алгоритмов.

Производительность VPN. Трудоемкость криптографического алгоритма определяет время выполнения операций шифрования и хеширования

$$t_{krypt} = F(n) \cdot t_{op}, \qquad (2)$$

где t_{ov} – среднее время реализации шага алгоритма, зависит от особенностей задачи, типа процессора и количества обрабатываемых блоков.

На производительность VPN влияют также реализация механизмов аутентификации и туннелирования Защищенное соединение устанавливается между VPN-агентами после выполнения проверки их подлинности. Аутентификации на основе IP-адресов агентов не защищает от подмены адреса злоумышленником. Аутентификация на основе пароля предполагает передачу аутентифицирующей информации по сети в незащищенном (протокол PAP) или зашифрованном (CHAP) виде, использование смарт-карт (EAP). Более надежной является взаимная аутентификация VPN-агентов на основе симметричной или асимметричной криптографии и использование сертификатов, которая защищает от активных и пассивных атак в сети Internret.

Туннелирование или инкапсуляция заключается в добавлении к исходному пакету дополнительного заголовка, содержащего данные о маршруте, хэш и другую служебную информацию, данные пакета вместе с заголовком при этом шифруются. Длина заголовка составляет не менее 20 байт, размер пакета и время передачи при этом увеличивается. На приемном конце VPN-агент удаляет эту информацию, расшифровывает данные пакета и вычисляет хеш-код для проверки целостности. Процедура туннелирования оказывает большее влияние на производительность по сравнению с аутентификацией, которая сводится к нескольким обменам данными между агентами.

Заключение. Виртуальные частные сети позволяют решить задачу защиты информации от несанкционированного доступа и изменения в процессе ее передачи по открытой сети за счет криптографических методов и характеризуются эффективностью защиты и невысокой стоимостью. Однако производительность канала передачи данных при использовании данной технологии падает, поэтому необходимо использовать низкоресурсную криптографию, стремиться к уменьшению туннельных задержек. Алгоритмы шифрования, вычисления хэш-функции, электронной цифровой подписи должны обладать криптографической стойкостью. Необходимо предусматривать смену криптографических ключей через определенные периоды времени, при использовании симметричной криптографии обеспечивать распределение секретных ключей между VPN-агентами. В целом, преимущества данной технологии, делают целесообразным ее использование в системах экологического мониторинга.

СПИСОК ЛИТЕРАТУРЫ

1. *Браун С.* Виртуальные частные сети VPN. М.: Лори, 2001. 503 с.
2. *Ульянов М.В.* Ресурсно-эффективные компьютерные алгоритмы. Разработка и анализ. М.: Наука, 2007. 376 с.
3. *ГОСТ* Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры; введ. 2016-01-01. М.: Стандартинформ, 2016. 16 с.
4. *ГОСТ* Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хеширования; введ. 2013-01-01. М.: Стандартинформ, 2013. 24 с.
5. *Шаньгин В.Ф.* Защита информации в компьютерных системах и сетях. М.: «ДМК», 2012. 592 с.

PROTECTION OF DATA TRANSMISSION CHANNEL ON THE BASIS OF VPN TECHNOLOGIES IN SYSTEMS FOR ENVIRONMENTAL MONITORING

N.L. Korepanova, M.A. Lebedeva

Sevastopol State University, Russian Federation, Sevastopol, Universitetskaya St., 33

The means of protection of data transmission channels in automated systems of ecological monitoring based on virtual private networks technology are considered. Ensuring the confidentiality and integrity of the transmitted data is based on the use of persistent symmetric ciphers and cryptographic hash functions in combination with authentication and tunneling mechanisms. The approaches to the choice of cryptographic algorithms used in virtual private networks are indicated. The analysis of the resource intensity of the software implementation of some cryptographic algorithms is carried out, directions for increasing the performance of the protected channel are determined.

Keywords: virtual private network, tunneling, cryptography; block ciphers; hash functions.