влияние на мировое экономическое развитие // International Journal of Open Information Technologies. – 2017. – Vol. 5, No. 1. – С. 1-18.

6. *Меденников В.И.* Математическая модель формирования цифровых платформ управления экономикой страны // Цифровая экономика. – 2019. – № 1. – С. 25-35.

7. *Kulba V., Medennikov V., Butrova E.* Methodical Approaches to Agricultural Risk Estimate in Forecasting the Economic Effect of Applying Data of the Earth's Remote Sensing / IEEE Xplore Digital Library. Twelfth International Conference "Management of large-scale system development" (MLSD), 2019. – DOI: 10.1109/MLSD.2019.8911084.

8. *Губанов Д.А., Коргин Н.А., Новиков Д.А., Райков А.Н.* Сетевая экспертиза. – М.: Эгвес, 2010. – 168 с.

Иконников С.Е., Анисимова Е.А., Чебан А.Г.

Применение протоколов VPN-соединений для интеграции пользователей автоматизированных информационных систем

Аннотация: В работе рассматриваются ключевые аспекты протоколов IPSec и SSL, используемых для организации VPN-соединений. Оба протокола обеспечивают безопасный обмен данными через сети общего назначения. Также анализируются преимущества и недостатки каждого из типов протоколов

Ключевые слова: Secure Sockets Layer, Internet Protocol Security, VPN-сервер, протокол, информационная безопасность

В современных условиях распространена практика организации подключения удаленных пользователей автоматизированных информационных систем посредством VPN-соединения. При организации VPN-соединения на нижних уровнях модели OSI (Open Systems Interconnection) действуют собственные протоколы, позволяющие шифровать трафик и упаковывать информационные пакеты.

Secure Sockets Layer (SSL) и Internet Protocol Security (IPSec) являются протоколами, использующими для обеспечения безопасных подключений путем шифрования через виртуальную частную сеть (Virtual Private Network – VPN). Оба этих протокола обеспечивают конфиденциальность, различаются же они способом установления безопасного соединения между клиентским устройством и VPN-сервером. Протокол SSL кодирует данные на транспортном уровне и функционирует за счет шифрования трафика. VPN-соединения протокола IPSec зашифровывает и аутентифицирует данные на сетевом уровне и используется для защиты данных, отправленных через системы с идентифицируемыми IP-адресами.

VPN представляет собой технологию кодирования и конфигурации доступа к публичной сети, обеспечивающую частные сети связи. VPN настраиваема для пользователей и использует личный канал связи между ними. Применение данной технологии значительно снижает затраты пользователей по сравнению с обычной сетью. Протоколы PPTP, L2TP, IPSec, SSL и т.д. являются частью сетевых протоколов технологии VPN.

Механизм функционирования протокола IPSec заключается в организации системы сетевой безопасности, обеспечивающей защищенную связь между парой узлов. Данный протокол необходим для организации VPN-соединений между одним и другими шлюзами, обеспечивая защиту доступа, конфиденциальность, целостность, аутентификацию исходных данных и т.д.

Протокол SSL обеспечивает удаленное подключение к информации с помощью простого подхода, отличающегося от протокола IPSec. Любой компьютер, на котором установлен браузер, будет использовать протокол SSL. Но клиентская программа протокола IPSec должна быть установлена на всех пользователях автоматизированной информационной системы. Применение протокола IPSec является стандартным решением компании для управления удаленным доступом. Протокол SSL идеально подходит для удаленного доступа. По мере развития внедрения протокола SSL все больше организаций приступали к внедрению сетевой архитектуры протокола SSL. В данном исследовании рассматривались протоколы IPSec и SSL при

организации VPN-соединения с оценкой особенностей их применения, сложности и надежности.

Протокол SSL (Secure Sockets Layer) представляет собой набор интернет-протоколов, которые используются для аутентификации личности и передачи данных между Web-браузерами и сервером. В протоколах прикладного уровня используется протокол SSL. Он обеспечивает защиту передачи данных. Протокол SSL состоит из двух уровней: SSL Handshake, SSL Log, SSL Change Cipher Specific Protocol и SSL Warn. Протокол SSL Script основан на доверенном транспортном протоколе (таком как TCP), который обеспечивает поддержку протокола более высокого уровня для кодирования, сжатия, шифрования данных, а также других базовых функций. Протокол SSL Handshake основан на протоколе SSL login, который используется при текущей передаче данных прежде, чем все стороны свяжутся для проверки личности, консультаций, обмена ключами и алгоритмами шифрования. VPN-соединение по протоколу SSL позволяет удаленным пользователям получить доступ при наличии соединения с Интернетом. Одним из ключевых достоинств протокола SSL заключается в простоте настройки и использовании, также данный вид соединения не требует специального программного обеспечения, установленного на стороне клиента.

Преимуществами VPN-соединения по протоколу SSL являются: масштабируемость, отсутствие необходимости устанавливать дополнительное программное обеспечение, наличие возможности получения доступа при наличии соединения с глобальной сетью Интернет.

Недостатки VPN-соединения по протоколу SSL заключаются в том, что данное соединение может не работать со старыми и/или неподдерживаемыми устройствами, имеется зависимость от качества сетевой инфраструктуры, а также уязвимость для атаки «человек посередине».

Протоколы IPSec защищают соединения на сетевом уровне, шифруют и аутентифицируют данные, которыми обмениваются устройства, подключенные к сети VPN. Протокол IPSec предлагает два типа механизмов защиты контактов: ESP (Encapsulation Security Payload) и AH (Authentication Head). Система ESP обеспечивает конфиденциальность и достоверность информации; механизм AH

защищает целостность. Эти системы позволяют избежать атаки, предотвращающей повторное воспроизведение. Протокол IKE (включен в протокол IPSec) был введен для подтверждения автоматизированных параметров для обеспечения конфиденциальности. Согласованные параметры безопасности включают алгоритмы шифрования и аутентификации, кодирование ключей и ключи аутентификации. ESP предоставляет два режима инкапсуляции для IP-пакетов: режим передачи и туннельный режим. Исходный IP-адрес остается неизменным в режиме передачи, шифруются только данные транспортного уровня. В туннельном режиме новый IP-адрес подключается ко всему пакету IP-данных.

На рисунке 1 представлен пример настройки VPN-соединения по протоколу IPSec.

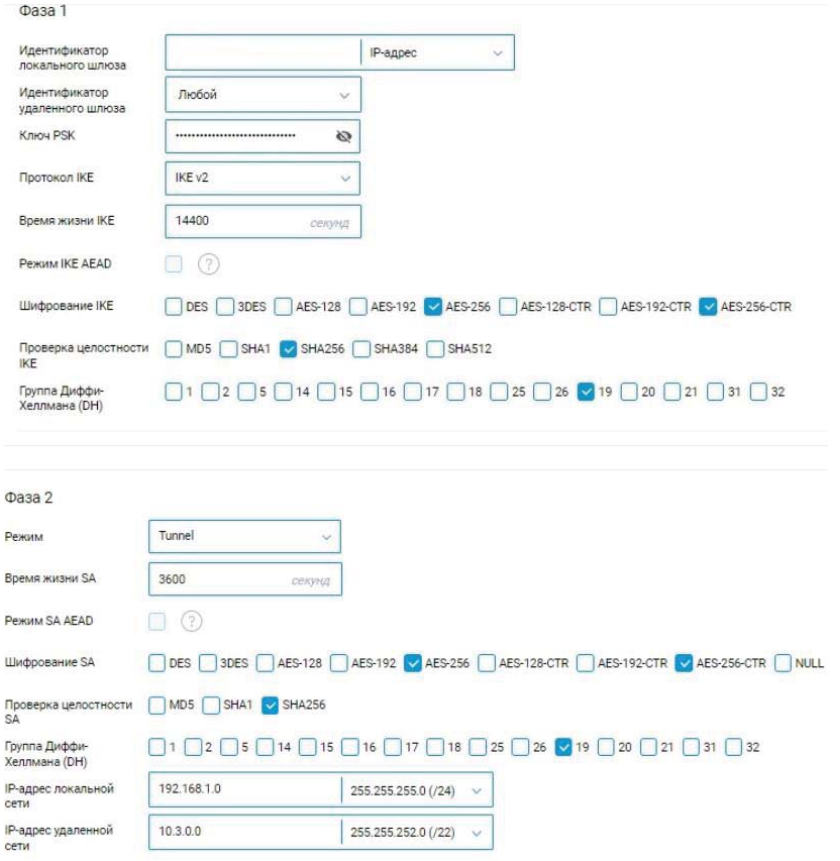

Рисунок 1 – Настройка IPSec подключения

Согласно последним стандартам шифрования используется шифр AES-256. Существует российский аналог данного шифра – шифр «Кузнечик». Скорость работы шифра AES выше, чем у шифра «Кузнечик», но это полностью зависит от производительности микропроцессора. Если говорить о криптостойкости, то атака «человек по середине» встретит большее сопротивление с шифром AES, чем с шифром «Кузнечик». Тем не менее на практике используются оба шифра.

Относительно группы Диффи-Хеллмана рекомендуется применять группу 19, 20, если алгоритм шифрования или аутентификации со 128-битным ключом; с 256-битным – 21 группа.

Достоинствами VPN-соединения по протоколу IPSec являются: организация доступа к остальным устройствам в сети, обеспечение безопасности высокого уровня за счет надежной аутентификации по цифровым сертификатам, предварительно совместно используемых ключей или других методов.

Недостатком VPN-соединения по протоколу IPSec является требования по наличию дополнительного или более производительного оборудования программного обеспечения, что значительно увеличивает эксплуатационные расходы организации.

По результатам проведенного исследования были сделаны следующие выводы.

Протокол SSL действует на прикладном уровне и доступен через Web-браузер и/или любое устройство, подключенное к Интернету. Данный протокол хорошо интегрируется с облачными приложениями. При использовании этого протокола конечными узлами являются устройства с Web-браузером. Длина ключа составляет от 40 до 128 бит.

Протокол IPSec действует на сетевом уровне, при его использовании необходимо установить дополнительное программное обеспечение. Конечными точками являются только одобренные и настроенные устройства, устанавливаемые с программ пользователя. Данный протокол лучше работает с локальными системами, запущенными во внутренней инфраструктуре организации. Длина ключа составляет от 56 до 256 бит.

VPN-соединение по протоколу IPSec предназначено для таких пользователей информационной системы, для которых предъявляются высокие требования к безопасности и у которых имеется сложная сетевая инфраструктура. VPN-соединение по протоколу SSL используется более массово за счет безопасного удаленного доступа к отдельным пользователям и/или устройствам без наличия дополнительных требований.

Литература:
1. SSL VPN, 2024. – URL: https://www.cisco.com (дата обращения 17.09.2024).
2. Network Security Docs – IPSec VPN, 2024. – URL: https://docs.paloaltonetworks.com (дата обращения 15.09.2024).
3. *Соболев М.А.* Сравнительный анализ российского стандарта шифрования по ГОСТ Р 34.12–2015 и американского стандарта шифрования AES // Политехнический молодежный журнал. – 2022. – № 04(69). – DOI: 10.18698/2541-8009-2022-04-785.

Макшаков С.В.

Система поддержки принятия решений в задачах технического переоснащения в железнодорожной отрасли

Аннотация: Описание функционала и программной архитектуры системы поддержки принятия решений в задачах технического переоснащения в подразделениях ОАО «РЖД». Назначение системы – автоматизация процессов формирования, мониторинга и контроля выполнения программы технического переоснащения. Цель создания системы – повышение эффективности, точности планирования и реализации проектов по техническому переоснащению. Демонстрируется архитектурный подход и анализируются основные технологии, используемые при построении системы.

Ключевые слова: система поддержки принятия решений, техническое переоснащение, архитектура программного обеспечения, веб-приложение, АО «ВНИИЖТ», ОАО «РЖД»

В работе представлена автоматизированная информационно-аналитическая система, разработанная АО «ВНИИЖТ» для реализации технического переоснащения в холдинге ОАО «РЖД».

1. Описание проблематики и постановка вопросов

Программа технического переоснащения в железнодорожной отрасли решает проблемы обеспечения экономической и