УДК 004.056.5

И. А. Назаренко[1], Д. И. Сачков[1]

[1] Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация

МЕТОДИКА ВЫБОРА ПРОТОКОЛА VPN ДЛЯ ЗАЩИТЫ КОММЕРЧЕСКОЙ ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ ПО КАНАЛУ СВЯЗИ С УДАЛЁННЫМ ОФИСОМ

Аннотация. *В статье проанализированы основные протоколы VPN и их актуальность в наше время. Рассмотрены, используемые в данных протоколах, инструменты обеспечения безопасности информации. Предложена методика выбора протокола VPN для организаций малого и среднего бизнеса с целью защиты коммерческой информации, передаваемой по каналу связи с удалённым офисом.*

Ключевые слова: *виртуальная частная сеть, сеть, каналы связи, шифрование.*

I. A. Nazarenko[1], D. I. Sachkov[1]

[1] Irkutsk State Transport University, Irkutsk, the Russian Federation

THE METHODOLOGY OF CHOOSING A VPN PROTOCOL FOR PROTECTING COMMERCIAL INFORMATION TRANSMITTED OVER A COMMUNICATION CHANNEL WITH A REMOTE OFFICE

Abstract. *The article analyzes the main VPN protocols and their relevance in our time. The information security tools used in these protocols are considered. A methodology for choosing a VPN protocol for small and medium-sized businesses is proposed in order to protect commercial information transmitted over a communication channel with a remote office.*

Keywords: *virtual private network, network, communication channels, encryption.*

Введение

В последнее время переход на частичный или полный удалённый формат работы стал всё более частым явлением. В связи с этим обеспечение конфиденциальности, целостности и доступности информации, передаваемой по дистанционным каналам связи, стало более актуальной проблемой [1-2]. Одним из методов решения данной проблемы является технология виртуальных частных сетей (Virtual Private Network - VPN), позволяющая создавать каналы связи между домашними и рабочими компьютерами, а также соединять локальные сети нескольких офисов одной организации. VPN, как ясно из названия, является виртуальной сетью, выступающей в качестве зашифрованного канала связи [3-5]. Безопасность данного канала обеспечивается шифрованием передаваемых через него данных и определяется используемыми протоколами шифрования, хеширования, согласования секретного ключа и др. инструментами. Отслеживать новые технологии и проверять актуальность используемых средств защиты важно для обеспечения безопасности информации [6, 7]. Как определить какой протокол VPN следует выбрать организации, чтобы создать защищённый канал связи для передачи информации? Для решения этого вопроса автором статьи была разработана методика выбора протокола VPN для защиты коммерческой информации (информации, составляющей коммерческую тайну), передаваемой по каналу связи с удалённым офисом.

Протоколы VPN

Чтобы понять, какие протоколы подходят организации, для начала рассмотрим основные протоколы VPN:

PPTP (англ. Point-to-Point Tunneling Protocol) – один из старейших протоколов разработанный компанией Microsoft. Использует протокол шифрования (MPPE), который реализует алгоритм RSA [8].

SSTP (англ. Secure Socket Tunneling Protocol) – протокол разработанный компанией Microsoft. Соединение проходит с помощью HTTPS по 443 порту, протоколом шифрования выступает SSL, а для аутентификации на сетевых узлах используются SSL и PPP [9].

L2TP/IPsec (англ. Layer 2 Tunnelling Protocol, IP Security) – протокол является объединением двух технологий – L2TP и IPsec. L2TP отвечает за туннелирования данных, а IPsec отвечает за шифрование данных и аутентификацию пользователя. В данном случае используются алгоритмы шифрования 3DES или AES и алгоритмы хеширования MD5 или SHA [10].

IKEv2/IPsec (англ. Internet Key Exchange Version 2) – так же включает в себя два протокола – IPsec и IKEv2, что отвечает за туннелирование. Используемые инструменты безопасности: алгоритмы шифрования – 3DES или AES, алгоритм хеширования – SHA и протокол согласования секретного ключа – Диффи-Хеллмана [11].

OpenVPN – относительно новый протокол VPN с открытым исходным кодом. Безопасность обеспечивается инструментами из криптографической библиотеки OpenSSL, что предоставляет возможность гибкой настройки используемого инструментария: алгоритмов шифрования, хеширования и сертификатов ЭЦП (электронной цифровой подписи) [12].

WireGuard – новый протокол с открытым исходным кодом, использующий множество различных инструментов для обеспечения безопасности передаваемых данных: протокол согласования ключей – Noise protocol framework в связке с криптографической эллиптической кривой – Curve25519, потоковый шифр ChaCha20 в связке с кодом аутентификации сообщения – Poly1305, алгоритм хеширования – BLAKE2, хэш-функцию – SipHash24 и функцию получения ключа – HKDF [13].

Далее, был проведён анализ защищённости протоколов VPN, на основании информации о используемых в них инструментах (протоколах шифрования, хеширования, согласования секретного ключа и эллиптических кривых), обеспечивающих безопасность информации.

Так, PPTP не безопасен в использовании из-за различных серьёзных уязвимостей (например, проблемы с аутентификацией, шифрованием) [14]. SSTP может обеспечить безопасную передачу данных, хоть используемые инструменты защиты довольно стары и при сравнении проигрывают более современным аналогам. Так же он имеет закрытый код, что делает невозможным его улучшение.

Протоколы L2TP/IPsec и IKEv2/IPsec являются жизнеспособными вариантами построения VPN, хотя у этих протоколов закрытый исходный код, однако они поддерживают современные и надёжные методы шифрования данных и могут быть реализованы на различных платформах и операционных системах.

OpenVPN и WireGuard используют наиболее современные методы защиты информации, обладают большой гибкостью настройки этих методов защиты и имеют открытый исходный код который возможно изменять и дорабатывать. Однако для качественной доработки исходного кода требуются квалифицированные специалисты и значительные ресурсы, что могут позволить себе далеко не все компании и это может ограничить возможный перечень компаний, которые смогут реализовать эти возможности. К тому же протокол WireGuard не является полностью завершённым продуктом и в настоящее время он находится в стадии интенсивной разработки, однако проблем с безопасностью выявлено не было.

Методика выбора протокола VPN для защиты

Чтобы определиться с выбором протокола VPN, подходящего организации, следует опираться на имеющуюся информацию об организации: на важность обрабатываемой организацией информации, составляющей коммерческую тайну, её размер и количество эконо-

мических ресурсов. Пусть размер организации и количество экономических ресурсов не являются линейно зависимыми параметрами, однако они весьма коррелирующие.

Для проведения оценки автором предлагается двухфакторная модель, критериями которой выступают размер организации и значимость передаваемой по сети информации.

Первым фактором выступает размер организации. Согласно Постановлению Правительства РФ № 265, организации делятся по размеру на 3 основных категории, приведённые в таблице 1: микропредприятия, малые предприятия и средние предприятия [15].

Таблица 1: Классификация организации по размеру

Размер	Доход
Микропредприятие	Менее 120 млн. рублей в год
Малое предприятие	От 120 млн. до 800 млн. рублей в год
Среднее предприятие	От 800 млн. до 2 млрд. рублей в год

Вторым фактором выступает значимость коммерческой информации, которая будет передаваться по каналам связи. Для определения значимости авторами предложена классификация сведений, составляющих коммерческую тайну, содержащая три уровня: информация ограниченного доступа, конфиденциальная информация и строго конфиденциальная информация, показанные в таблице 2.

Таблица 2: Классификация организации по уровню значимости обрабатываемой информации

Уровень значимости коммерческой информации		
Информация ограниченного доступа	Конфиденциальная информация	Строго конфиденциальная информация

К информации ограниченного доступа относится внутренняя информация организации, потеря которой может нанести незначительный репутационный или материальный ущерб компании.

К конфиденциальной информации относится внутренняя информация организации, её потеря несёт за собой значительный репутационный или материальный ущерб, который может оказать негативное влияние на функционирование компании.

К строго конфиденциальной информации относится внутренняя информация организации. Её потеря нанесёт огромный репутационный или материальный ущерб компании, который может оказать сильное негативное влияние на функционирование компании или даже привести к её закрытию.

В некоторых случаях организация может работать с информацией нескольких уровней. В таком случае уровень определяется как самый высокий из обрабатываемых. После получения двух предыдущих показателей (из таблиц 1 и 2), определяем необходимый уровень защищённости протокола VPN, согласно предложенной автором классификации, изображённой в таблице 3.

Таблица 3: Определение уровня защищённости VPN

Определение необходимого уровня защищённости протокола VPN.	Уровень значимости коммерческой информации		
	Информация ограниченного доступа	Конфиденциальная информация	Строго конфиденциальная информация

Размер организации	Среднее предприятие	У2	У1	У1
	Малое предприятие	У2	У2	У1
	Микропредприятие	У3	У2	У2

После определения уровня защищённости (из таблицы 3), организация получает информацию о подходящих ей протоколах VPN, определяемых по полученному уровню:

У3 – низкий уровень защищённости, ценность передаваемой информации невелика и использование продвинутых средств защиты нецелесообразно. К данному уровню относится протокол – SSTP.

У2 – средний уровень защищённости, передаваемые сведенья весьма ценны и необходимо использовать продвинутые средства защиты, чтобы избежать бóльших затрат ресурсов из-за последствий утечки. К данному уровню относятся протоколы – L2TP/IPsec и IKEv2/IPsec.

У1 – высокий уровень защищённости, передаваемая информация имеет огромную значимость для компании в случае её утечек последствия для организации будут катастрофическими, средства защиты информации должны быть современными и иметь возможность дальнейшего улучшения. К данному уровню относятся протоколы – OpenVPN и WireGuard.

Заключение

В данной статье рассмотрены протоколы VPN и предложена авторская методика, позволяющая организациям малого и среднего бизнеса выбрать подходящий им протокол, для обеспечения безопасности информации, передаваемой по удалённым каналам связи. Выбор протокола производится на основании двух критериев: размера организации и значимости, передаваемой по сети конфиденциальной информации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Нуриев С.А., Карцан И.Н. Обеспечение безопасности конфиденциальной информации компании при удаленном доступе сотрудника // Современные инновации, системы и технологии. – 2023. – № 3 (2). – С. 234-242.
2. Гамзин Д.М., Тибалов Н.П., Поначугин А.В. Актуальность использования vpn-сервисов в россии в условиях мировой нестабильности // Международный научно-исследовательский журнал. – 2023. – № 2 (128). – С. 1-5.
3. Кондрущенков О.М., Лекарь Л.А. Защищенная территориально распределенная мультисервисная система связи для обеспечения управления в реальном масштабе времени // Информационная безопасность социотехнических систем. – 2017. – № 1 (1). – С. 53-58.
4. Кондрущенков О.М., Лекарь Л.А. Построение защищенного ведомственного портала // Информационная безопасность социотехнических систем. – 2017. – № 3 (1). – С. 32-37.
5. Олифер. В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. Юбилейное издание / ISBN 978-5-4461-1426-9 // СПб.: Питер, 2020. – С. 584.
6. Ahmed M., Mahmood A.N., Islam M.R. A survey of anomaly detection techniques in financial domain. Future Generation Computer Systems – 2016. – №55. – С. 278-288.
7. Mishra P., Phillip E.S., Varadharajan V., Tupakula U. Intrusion detection techniques in cloud environment: Journal of Network and Computer Applications. – 2017. – №77. – С. 18-47.
8. First Net Security. Available at: https://www.firstnetsecurity.com/library/ms/understanding_pptp.pdf (Accessed: 17.02.2024).
9. Интернет Контроль Сервер - межсетевой экран ИКС для защиты корпоративной сети [Электронный ресурс] – Режим доступа: https://xserver.a-real.ru/blog/useful/secure-socket-tunneling-protocol/ (дата обращения: 17.02.2024).
10. CLI Book 3: Cisco ASA Series VPN CLI Configuration Guide, 9.6 - L2TP over IPsec [Cisco ASA 5500-X Series Firewalls] - Cisco. Available at:

https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/configuration/vpn/asa-96-vpn-config/vpn-l2tp-ipsec.html (Accessed: 17.02.2024).

11. Cisco 1000 Series Connected Grid Routers Security Software Configuration Guide – Configuring IKEv2 and IPSec - Cisco. Available at: https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/cgr1000/1_0/software/configuration/guide/security/security_Book/sec_ipsec_cgr1000.html (Accessed: 18.02.2024).

12. Reference Manual For OpenVPN 2.4 | OpenVPN. Available at: https://openvpn.net/community-resources/reference-manual-for-openvpn-2-4/ (Accessed: 18.02.2024).

13. WireGuard: fast, modern, secure VPN tunnel. Available at: https://www.wireguard.com (Accessed: 18.02.2024).

14. Bruce S., Mudge. Cryptanalysis of Microsoft's Point-to-Point Tunneling Protocol (PPTP) / DOI:10.1145/288090.288119 // CCS '98: Proceedings of the 5th ACM conference on Computer and communications security. – 1998. – P. 132-141.

15. Постановление Правительства Российской Федерации от 4 апреля 2016 г. N 265 г. Москва "О предельных значениях дохода, полученного от осуществления предпринимательской деятельности, для каждой категории субъектов малого и среднего предпринимательства" - Российская газета – Федеральный выпуск: №76(6944) [Электронный ресурс] – Режим доступа: https://rg.ru/documents/2016/04/11/dohody-biznesa-dok.html (дата обращения: 6.04.2024).

REFERENCES

1. Nuriev S.A., Kartsan I.N. Obespechenie bezopasnosti konfidencial'noj informacii kompanii pri udalennom dostupe sotrudnika [Ensuring the security of confidential company information during remote access of an employee] // Sovremennye innovacii, sistemy i tekhnologii [Modern Innovations, Systems and Technologies], 2023, No. 3 (2), pp. 234—242.

2. Gamzin D.M., Tibalov N.P., Ponachugin A.V. Aktual'nost' ispol'zovaniya vpn-servisov v rossii v usloviyah mirovoj nestabil'nosti [The relevance of using vpn-services in russia in the face of global instability] / DOI:https://doi.org/10.23670/IRJ.2023.128.25 // Mezhdunarodnyj nauchno-issledovatel'skij zhurnal [International Research Journal], 2023, No. 2 (128), pp. 1—5.

3. Kondrushchenkov O.M., Lekar L.A. Zashhishhennaja territorial'no-raspredelennaja mul'tiservisnaja sistema svjazi dlja obespechenija upravlenija v real'nom masshtabe vremeni [Secure territorial distributed multi service communication system for real-time ensuring management] // Informacionnaya bezopasnost' sociotekhnicheskih sistem [Information security of socio-technical systems], 2017, No. 1 (1), pp. 53—58

4. Kondrushchenkov O. M., Lekar L. A. Postroenie zashhishhennogo vedomstvennogo portala [Building a secure departmental portal] // Informacionnaya bezopasnost' sociotekhnicheskih sistem [Information security of socio-technical systems], 2017, No. 3 (1), pp. 32—37.

5. Olifer V.G., Olifer N.A. Computer networks. Principles, technologies, protocols. Anniversary edition / ISBN 978-5-4461-1426-9 // St. Petersburg, 2020, p. 584.

6. Ahmed M., Mahmood A.N., Islam M.R. A survey of anomaly detection techniques in financial domain. Future Generation Computer Systems – 2016. – №55. – С. 278—288.

7. Mishra P., Phillip E.S., Varadharajan V., Tupakula U. Intrusion detection techniques in cloud environment: Journal of Network and Computer Applications, 2017, No.77, pp. 18—47.

8. First Net Security. Available at: https://www.firstnetsecurity.com/library/ms/understanding_pptp.pdf (Accessed: 17.02.2024).

9. Internet Control Server - ICS firewall to protect the corporate network. Available at: https://xserver.a-real.ru/blog/useful/secure-socket-tunneling-protocol/ (Accessed: 17.02.2024).

10. CLI Book 3: Cisco ASA Series VPN CLI Configuration Guide, 9.6 - L2TP over IPsec [Cisco ASA 5500-X Series Firewalls] - Cisco. Available at: https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/configuration/vpn/asa-96-vpn-config/vpn-l2tp-ipsec.html (Accessed: 17.02.2024).

11. Cisco 1000 Series Connected Grid Routers Security Software Configuration Guide – Configuring IKEv2 and IPSec - Cisco. Available at: https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/cgr1000/1_0/software/configuration/guide/security/security_Book/sec_ipsec_cgr1000.html (Accessed: 18.02.2024).

12. Reference Manual For OpenVPN 2.4 | OpenVPN. Available at: https://openvpn.net/community-resources/reference-manual-for-openvpn-2-4/ (Accessed: 18.02.2024).

13. WireGuard: fast, modern, secure VPN tunnel. Available at: https://www.wireguard.com (Accessed: 18.02.2024).

14. Bruce S., Mudge. Cryptanalysis of Microsoft's Point-to-Point Tunneling Protocol (PPTP) / DOI:10.1145/288090.288119 // CCS '98: Proceedings of the 5th ACM conference on Computer and communications security, 1998, pp. 132—141.

15. Resolution of the Government of the Russian Federation dated April 4, 2016 No. 265, Moscow "On the maximum values of income received from entrepreneurial activity for each category of small and medium-sized businesses" – Rossiyskaya Gazeta Federal Issue: No.76(6944) Available at: https://rg.ru/documents/2016/04/11/dohody-biznesa-dok.html (Accessed: 04.6.2024).

Информация об авторах

Назаренко Иван Александрович – магистрант, студент кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: 89994206594@yandex.ru

Сачков Дмитрий Иванович – к. э. н., проректор по цифровым технологиям, Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: sachkov_di@irgups.ru

Information about the authors

Nazarenko Ivan Aleksandrovich - graduate student, student of the Department «Information Systems and Information Protection», Irkutsk State University of Communications, Irkutsk, e-mail: 89994206594@yandex.ru

Sachkov Dmitry Ivanovich – Ph.D. in Economics, Vice-Rector for Digital Technologies, Irkutsk State Transport University, e-mail: sachkov_di@irgups.ru