УДК 004.056.52
DOI 10.33764/2618-981X-2022-6-15-20

Выбор технологии VPN в условиях блокировок ресурсов в сети Интернет

О. А. Герлиц[1]*, *Г. В. Попков*[2]
[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
[2] Сибирский государственный университет телекоммуникаций и информатики, г. Новосибирск, Российская Федерация
* e-mail: dvornikovaOlga21@gmail.com

Аннотация. В данной статье рассматривается актуальная на данный момент проблема выбора программных продуктов в условиях блокировок ресурсов сети Интернет. Большое количество иностранных компаний временно прекратило сотрудничество с российскими клиентами. Лишь немногие сделали это «мягко» для пользователей своих ресурсов: с рассылкой предупреждений и предоставлением возможности переноса базы данных на другие площадки или вывода денег с ранее купленных подписок на обслуживание программных обеспечений. Острым остается вопрос: какие сложности возникли у российского бизнеса? И какие альтернативы выбора технологий VPN в условиях блокировок ресурсов в сети интернет? Целью представленной работы заключается в проведении анализа программных продуктов, а именно корпоративного VPN. На основании проведенного анализа составлены рекомендации для выбора систем удаленного доступа.

Ключевые слова: VPN, корпоративная сеть, информационная безопасность, шифрование, защищенный канал

Development of a project to create a protected corporate network using VPN technologies

O. A. Gerlits[1]*, *G. V. Popkov*[2]
[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
[2] Siberian State University of Telecommunications and Informatics, Novosibirsk, Russian Federation
*e-mail: dvornikovaOlga21@gmail.com

Abstract. This article discusses the currently relevant problem of choosing software products in the conditions of blocking Internet resources. A large number of foreign companies have temporarily ceased cooperation with Russian clients. Only a few have done this “softly” for users of their resources: with the distribution of warnings and the possibility of transferring the database to other sites or withdrawing money from previously purchased software maintenance subscriptions. The question remains acute: what difficulties have arisen for Russian business? And what are the alternatives to choosing VPN technologies in the face of blocking resources on the Internet? The purpose of the presented work is to analyze software products, namely corporate VPN. Based on the analysis carried out, recommendations were made for choosing remote access systems.

Keywords: VPN, corporate network, information security, encryption, secure channel

Введение

Удаленная работа сотрудников уже далеко не новое явление и практикуется большим количеством компаний, особенно из сферы Information Technology (IT). Однако происходящие обстоятельства заставляют компании из самых разных об-

ластей деятельности задуматься об оперативном переходе сотрудников на удаленную работу и продолжать деятельность в изменившихся условиях [1].

Переход на отечественное программное обеспечение (ПО) является одним из актуальных вопросов на текущий момент, так как многие зарубежные IT-лидеры ходят с российского рынка. Для отечественных разработчиков это шанс занять выгодные позиции и предложить продукт не только госучреждениям, но и коммерческим компаниям. Данную проблематику освещают многие новостные источники и предоставляют статистику об охватах внедрения российского софта. Также в рамках данной статьи были использованы данные предоставленные компаниями SearchInform и PositiveTechnologies, являющимися лидерами в сфере рынка информационной безопасности, что подтверждает актуальность выбранной темы.

Целью данной работы является проведение анализа характеристик продуктов, используемых для удаленного подключения сотрудников и разработка рекомендаций по выбору системы удаленного доступа.

Материалы

Для проведения анализа распространенного на рынке ПО, используемого для подключения сотрудников к корпоративной сети, рассмотрены технологии корпоративного VPN. За основу выбора программного обеспечения использован Реестр программного обеспечения [2]. А именно предоставлен обзор: ViPNet Coordinator от ИнфоТеКС, продуктов российской компании «С-Терра СиЭсПи», AnyConnect Secure Mobility Client американской компании Cisco, продуктов для организации удаленного доступа от компании «Код безопасности».

Сравнительный анализ перечисленных программных продуктов производили по таким критериям, как универсальность применения, безопасность VPN, производительность, простота использования и качество поддержки пользователей, цена.

Выбор VPN технологий в условиях блокировки

Для полноценной удаленной работы необходимо обеспечить, прежде всего, безопасный доступ к используемым корпоративным информационным системам и данным, а также безопасность самих корпоративных данных, покидающих защищенный периметр организации [3].

Однако большое количество иностранных компаний временно прекратило сотрудничество с российскими клиентами. Лишь немногие сделали это «мягко» для пользователей: с рассылкой предупреждений и предоставлением возможности перенести базы данных на другие площадки или вывести деньги [4]. Острым остается вопрос: какие сложности возникли у российского бизнеса? И каковы альтернативы выбора технологий VPN в условиях блокировок ресурсов в сети интернет?

VPN представляет собой экономичный и безопасный способ быстро подключить удаленных пользователей к офисной сети. VPN повышает уровень защиты информации пользователя или компании за счет шифрования данных. Бо-

лее мощный алгоритм шифрования способен обеспечить высокую степень защиты внутренних корпоративных документов, информации пользователей, переписки сотрудников, торговых секторов и т.п. Важное замечание: VPN лучше использовать в качестве дополнительного инструмента защиты, а не единственного. Что определяет выбор технологий VPN: его функциональные возможности, цена или же наличие сертификатов [5]?

Когда VPN используется по назначению и использует современные криптографические протоколы, то может эффективно шифровать трафик между удаленными сотрудниками или командами и внутренней сетью их компании. Кроме того, виртуальные частные сети дешевле и проще в управлении, чем устаревшие решения, такие как покупка защищенной «выделенной линии» у интернет-провайдера или ручное добавление в «белый список» отдельных IP-адресов, принадлежащих удаленным работникам.

Однако у VPN также есть ограничения. Некоторые из них приведены ниже:

– угрозы безопасности [6];

– штрафы за задержку для каждого отдельного запроса между сотрудниками и сетью;

– сложности облака и гибридного облака [7];

– затраты на установку;

– время управления.

В настоящее время многие нормативно-правовые акты регулируют вопросы защиты информации, передаваемой по незащищенным каналам связи, рекомендуют или обязывают использовать при удаленном доступе сертифицированные ФСБ России средства криптографической защиты информации.

В текущих реалиях многие компании столкнулись с проблемами оборудования и ПО. С рынка ушли Acronis, Cisco Systems Inc, Citrix, Hewlett Packard Enterprise, IBM, Intel, Veeam, VMWare и ряд других компаний, имеющих важную роль в IT-сфере. Услугами компаний пользовались крупнейшие российские частные и государственные корпорации. Почти треть зарубежных компаний, связанных с сферой информационной безопасности, работающих в России, уже ушли из России или собираются покинуть страну, забрав с собой сотрудников. Запрет на обновление ПО или блокировка лицензий также могут замедлить работу систем безопасности, повысить уязвимость бизнеса и затруднить удаленный доступ сотрудников к их рабочим местам. Также запрет на валютные операции усложняет процесс оплаты товаров и услуг компаниям, которые продолжают сотрудничать с Россией. Купить нужное ПО или оборудование в теории можно, но пользователи сталкиваются с проблемами оплаты [8]. Не стоит забывать и о резко выросших ценах на иностранную продукцию, в связи с чем бюджет на обновление инфраструктуры придется увеличивать минимум в два раза.

Пути решения описанных выше проблем имеются. Так, у организаций остается возможность отобрать отечественные программные продукты, услуги и сервисы под свои нужды, например, такие как КриптоПро CSP, ViPNet Client, vGate R2, MaxPatrol SIEM, SecretNet Studio, Kaspersky Endpoint Security, R-Vision SGRC и другие.

Направление на импортозамещение – это поэтапный отказ от иностранных технологий и товаров. Данный курс был объявлен уже в 2014 году. В плане указа описаны экономические меры обеспечения технологического самоуправления и безопасности объектов критической информационной инфраструктуры. Также отмечалось, что отечественные организации должны перейти на российское ПО по завершению срока действия прав на владение софта и при наличии отечественных аналогов [9]. На текущий момент, вместо плановых коэффициентов доли отечественного софта наблюдается в государственных структурах на уровне 90 %, а в государственных компаниях— 70 % к 2024 году, на конец 2021 отражена лишь на 30-35 %.

Российская компания «Код безопасности» предоставляет различные продукты для организации удаленного доступа, в том числе для организации VPN-сетей между филиалами предприятий. Удаленный доступ может быть реализован с помощью двух продуктов из линейки «Континент»: комплекс из сервера доступа «Континент 3.7» и СКЗИ «Континент-АП 3.7», ПАК СКЗИ «Континент TLS VPN сервер» для реализации удаленного доступа к веб-ресурсам с шифрованием по ГОСТ 28147-89.

Решения иностранной компании Cisco опираются на числе продуктов, которые предлагают преимущественно больше, чем только терминирование VPN. AnyConnect Secure Mobility Client представляет основную часть программного обеспечения, предлагаемого Cisco для VPN-решений. Данный продукт может быть запущен на многих популярных настольных и мобильных операционных системах и предоставляет помимо поддержки виртуальных единичных сетей другие функции безопасности. AnyConnect обеспечивает поддержку TLS, DTLS и IPsec IKEv2 [10].

ИнфоТеКС можно рассматривать одним из лидеров отечественного рынка информационной безопасности. Данная компания является ведущим поставщиком программных и программно-аппаратных VPN-решений, средств криптографической защиты информации на рабочих станциях, серверах и мобильных компьютерах. ViPNet Coordinator – программный сервер защищенной сети ViPNet, работающий под управлением операционной системы, а также позволят выполнять операции приоритизации, фильтрации, шифрования и аутентификации, надежно защищая передаваемую по каналам связи информацию от несанкционированного доступа и подмены.

Российская компания ООО «С-Терра СиЭсПи» – один из ведущих отечественных разработчиков и производителей продуктов сетевой безопасности (VPN-продукты). Продукты «С-Терра» используют набор протоколов IPsec и российские криптографические алгоритмы по ГОСТ 28147-89, сертифицированы ФСБ России и ФСТЭК России и включены в Единый реестр российских программ для электронных вычислительных машин и баз данных (Реестр российского ПО).

Проблема перехода на отечественное ПО состоит не только в выборе, а также в подорожании в 2 раза, ведь во многих компаниях бюджеты были заложены заранее. Повышение цен связано с подорожанием комплектующих запча-

стей, а это в свою очередь связано с нарушением цепочек поставок и отсутствием новых аппаратных платформ на рынке. Также перестали работать VPN шлюзы, у которых были отозваны TLS сертификаты, и это вызвало трудности с перевыпуском и быстрым переподключением. Для решения данной проблемы необходимо переходить на сертификаты, подписанные российскими центрами сертификации, но для этого данные центры сертификации должны быть прописаны в браузеры. А это является еще одной трудностью.

На основании проделанного анализа можно сделать выводы, что компании могут оперативно выбрать технологии VPN в условиях блокировок ресурсов в сети Интернет из представленных программных продуктов на отечественном рынке. Также как показывает практика, не всегда официальная отмена поставок в Россию в действительности означает полную остановку. Некоторые производители перешли на другие каналы продаж. В связи с этим, необходимо перепроверять даже официальную информацию.

Рассмотрим недостатки одномоментного перехода на отечественное ПО. В первую очередь – это невозможность такого перехода. Переход на новое программное обеспечение – это всегда долговременный и трудоемкий процесс, в частности, в организациях с распределенной структурой, где филиалы территориально далеко друг от друга. Поэтому редактируя планы по цифровой трансформации, требуется учитывать временную возможность. Второй фактор – нехватка специалистов. В России не хватает кадров в сфере разработки. Не менее трети российских компаний соприкоснулись с проблемами поискаде IT-специалистов. Недостаток составляет 150 тысяч человек, а к 2024 году необходимость в высококвалифицированных кадрах усиливается на четверть и достигнет 290-300 тысяч человек в год [11]. Вероятнее всего, даже больше, так как из-за санкционных ограничений нет возможности продолжать использовать услуги разработчиков из зарубежных стран. Также стоит отметить сложности с комплектующими запчастями компьютеров. Сервера, процессоры, модемы, коммутаторы, маршрутизаторы — комплектующие для российского производства ввозятся из-за рубежа. Что-то можно заменить, но запустить высокотехнологичное производство без импортных комплектующих невозможно. Разумеется, найдутся обходные пути, но в любом случае, это создает дополнительные сложности. И последний важный пункт – интеграция между сервисами и технологиями. В процессе внедрения новой технологий, необходимо провести подготовительную работу. Различные языки программирования, отличия в протоколах и сертификатах — процесс интеграции между отличающимися технологиями это отдельная задача, сложная и трудоемкая. Соответственно, потребуется больше кадровых и временных ресурсов.

Заключение

Таким образом при проведении анализа решений для организации корпоративных VPN были выделены следующие рекомендации:

– необходимость изучения и выбор ПО в соответствии с требованиями регуляторов;

– выбор ПО с возможностью интеграции системы защищенного удаленного доступа с имеющейся сетевой инфраструктурой либо инфраструктурой сетевой безопасности на уровне управления или мониторинга.

– третий параметр выбора: поддержка системой удаленного доступа необходимых стационарных и мобильных операционных систем;

– анализ необходимого количества поддерживаемых сессий, архитектура сети и поддержка необходимых протоколов аутентификации и шифрования.

В значительном количестве современных сетей имеются решения для дистанционного подключения, но новые угрозы возникают ежедневно, особенно это актуально с широким распространением BYOD (концепция корпоративной мобильности). Рассмотренные решения в данной статье предлагают гибкость и дополнительную безопасность, которая отвечает требованиям современных сетей.

Полученные данные при сравнительном анализе будут использованы для формирования базы данных и дальнейшей разработки сервиса, предоставляющего оптимальное решение по заданным критериям при выборе корпоративной VPN.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Как организована удаленная работа в России и страна СНГ [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/remote-work-in-russia-and-the-cis-2020/ (дата обращения: 01.04.2022).

2. Гома Х. Проектирование систем реального времени, параллельных и распределенных приложений: Пер. с англ., - М: ДМК Пресс, 2011, - 704с

3. Ибе О. Сети и удаленный доступ: Протоколы, проблемы, решения: Пер.с англ., – М: ДМК, 2002. – 332с.

4. Запечников С.В. Основы построения виртуальных частных сетей / С.В. Запечников, Н.Г.Милославская, А.И. Толстой. – М: Горячая Линия, Телеком,211. – 248 с.

5. Платонов В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей: учеб. пособие для студ. высш. учеб. заведений/ В.В. Платонов. — М. : Издательский центр «Академия», 2006. — 240 с.

6. Реестр программного обеспечения [Электронный ресурс]. URL: https://reestr.digital.gov.ru/ (дата обращения: 05.04.2022)

7. Постановление Правительства РФ от 4 августа 2015 года № 785 «О создании правительственной комиссии по импортозамещению»

8. Распоряжение Правительства РФ от 4 августа 2015 года № 1492-р

9. Массовый уход иностранных компаний: проблемы и решения по импортозамещению в IT [Электронный ресурс]. URL: https://www.cloud4y.ru/blog/business-out-problems-and-solutions// (дата обращения: 05.04.2022).

10. Организация корпоративных сетей на основе VPN: построение, управление, безопасность [Электронный ресурс]. URL: https://www.kp.ru/guide/korporativnaja-set.html (дата обращения: 10.04.2022).

11. Сайт компании CISCO [Электронный ресурс]. URL: https://www.cisco.com/c/en/us/solutions/small-business/resource-center/security/how-to-setup-a-vpn.html (дата обращения: 10.04.2022).