УДК 654.16

Авласевич Д.В., студент,
4 курс, Институт финансов, экономики и управления,
Тольяттинский государственный университет,
Тольятти (Россия)
Дмитриев Н.А., студент,
4 курс, Институт финансов, экономики и управления,
Тольяттинский Государственный Университет,
Тольятти (Россия)
Кириллов А.А., студент,
4 курс, Институт финансов, экономики и управления,
Тольяттинский Государственный Университет,
Тольятти (Россия)
Бачинский А.Г. магистрант
1 курс, Институт машиностроения,
Тольяттинский государственный университет,
Тольятти (Россия)
Avlasevich DV, student,
4th year, Institute of Finance, Economics and Management,
Tolyatti State University,
Tolyatti (Russia)
Dmitriev NA, student,
4th year, Institute of Finance, Economics and Management,
Tolyatti State University,
Tolyatti (Russia)
Kirillov AA, student,
4th year, Institute of Finance, Economics and Management,
Tolyatti State University,
Tolyatti (Russia)
Bachinsky A.G. undergraduate

1 year, Institute of Mechanical Engineering,
Togliatti State University,
Tolyatti (Russia)

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ VPN ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

Аннотация: Мы проанализировали основные технологические процессы предоставления безвредности при использовании VPN соединений, а также изучили главные протоколы VPN, установили достоинства и недочеты единичных протоколов и технологические процессы в целом.

Ключевые слова: VPN соединения; протоколы VPN; технологии VPN; VPN

Using vpn technology to ensure information security.

***Annotation*:** We analyzed the basic technological processes of providing harmlessness when using VPN connections, and also studied the main VPN protocols, established the advantages and disadvantages of individual protocols and technological processes as a whole.

***Keywords*:** VPN connections VPN protocols VPN technology; VPN

В обстоятельствах наиболее массовой экономики фирмы приступают к поиску географического распределения, или взаимозависимое с налоговыми стимулами, или же с возможностью расширения. В этом случае работникам необходима независимость для реализации своей деятельности в отсутствии географического лимитирования и охраны данных, которую они предоставляют.

Теория виртуальной индивидуальной сети, знакомая как VPN, вышла как экономический вариант с целью охраны коммуникации посредством социальных связывающих каналы, подобных сети интернет, и в недалеком будущем стала технологией, которая обширно используется предложением,

нацеленным на сохранности, гарантирующая единство, секретность и подлинность данных.

VPN была далеко не первой технологией с целью удаленного подсоединения. Прежде более популярным способом считалось подсоединение компьютера среди нескольких офисов, заключался он в применении назначенной линии. Назначенные линии, подобные ISDN (числовая линия с встроенными предложениями, 128 Кбит/с), являются индивидуальными сетевыми сочетаниями, которые телекоммуникационная фирма способна брать в аренду для собственных покупателей. Назначенные направления дают для фирмы право повысить собственную личную сеть, которая располагается за границами ее прямой географической области. Данные объединения формируют общую всемирную сеть (WAN) с целью бизнеса. Арендованные линии являются надежными, но контракты об аренде обходятся недешево, при этом затраты увеличиваются согласно мере повышения дистанции между представительствами. [1]

В настоящий период сеть интернет стала наиболее доступной, нежели ранее, также поставщики интернет-услуг (ISP) продолжают совершенствовать более стремительное и достоверное обслуживание с минимальными расходами, чем назначенные линии. Для того чтобы пользоваться этим, значительная доля компаний поменяла назначенные направления новейшими технологиями, которые применяет интернет-объединения, никак не жертвуя производительностью и сохранностью. Компании начали с развития интрасетей, считающиеся индивидуальными внутренними сетями, специализированными с целью использования только лишь для работников фирмы. Сеть Интернет дала право удаленным сотрудникам функционировать совместно при поддержке подобных технологий, как коллективное применение рабочего стола. С поддержкой VPN, компании имеют все шансы увеличивать средства собственной интрасети, что дает возможность работникам функционировать удаленно.

Целью VPN считается предоставление безопасного и достоверного объединения среди компьютерных сетей посредством имеющейся общедоступной сети, известной как, сеть интернет.

Хорошо спроектированная VPN предоставляет плюсы:

• Расширенные объединения в различном географическом расположении без участия назначенной линии.

• Усиленная защищенность при обмене сведениями.

• Гибкость для удаленных представительств, но кроме того для работников при применении интрасети с поддержкой имеющегося интернет-соединения, как в случае, если бы они были подсоединены непосредственно к сети.

• Экономия средств и времени.

• Высокая степень производительности для географически распределенных ресурсов.

От VPN постоянно необходимо:

• Безопасность. VPN обязан охранять сведения в период их перемещения в доступной сети, с целью защиты от захвата и использования ваших данных злоумышленником

• Надежность. У работников и удаленных представительств должна быть возможность присоединяться к VPN без каких-либо трудностей, а VPN обязан обеспечивать одинаковое качество объединения для каждого пользователя, в том числе и если он обрабатывает наибольшее число синхронных подсоединений.

• Масштабируемость. У VPN-сервисов должен быть право расширения.

Виртуальная индивидуальная сеть – это надежный туннель в ряду двух либо больше компьютерами в сети интернет, что дает возможность им

приобретать допуск друг к другу, так же, как в локальной сети. Раньше VPN-сети применялись фирмами для надежной связи удаленных отделений либо подсоединения роуминг-сотрудников к офисной сети, в настоящий период они кроме того считаются значимым предложением для покупателей, оберегают их от атак при подсоединении к доступным беспроводным сетям.

Открытые беспроводные сети имеют все шансы быть значительной опасностью для пользователей, так как преступники, которые сидят в тех же сетях, смогут пользоваться разными способами с целью наблюдения интернет-трафика и в том числе и присвоения учетных записей на веб-сайтах, в случае если они не применяют протокол защищенности HTTPS. Кроме того, определенные операторы сетей Wi-Fi осознанно вводят рекламу в интернет-траффик, а это может послужить причиной нежелательному отслеживанию.

В определенных регионах мира, правительства отслеживают пользователей, посещающих конкретные страницы сайтов, с целью раскрытия их политической принадлежности и установления диссидентов, грозящих свободе слова и правам человека.

Применяя VPN-соединение, весь трафик можно надежно маршрутизировать посредством сервера, находящегося в любом другом месте мира. Это содействует охране от локальных попыток отслеживания и взлома, но кроме того скрывает настоящий адрес интернет-протокола с интернет-страниц и сфер, к которым совершается обращение. [2]

Имеются разнообразные технологические процессы VPN с различной степенью кодирования. К Примеру, акт туннелирования «точка-точка» (PPTP) функционирует стремительно, однако значительно менее безопасен, нежели прочие протоколы, подобные IPSec либо OpenVPN, что применяет SSL/TLS (Secure Sockets Layer/Transport Layer Security). Кроме того, применяя VPN в базе TLS также значимы вид метода кодирования и протяженность ключа.

Несмотря на то, что OpenVPN удерживает большое число композиций шифров, протоколов обмена ключами и алгоритмов хеширования, более популярной реализацией, предлагаемой поставщиками услуг VPN для сочетаний OpenVPN, считается кодирование AES с обменом ключами RSA также сигнатурами SHA. Подходящими параметрами являются кодирование AES256 с источником RSA протяженностью не меньше 2048 бит также шифровальная хэш-функция SHA-2 (SHA256) взамен SHA-1.

Необходимо выделить, то, что кодирование способно воздействовать на быстроту объединения. Подбор схемы VPN и способов кодирования обязан производиться в любом конкретном случае, в зависимости от сведений, которые начнут передаваться.

VPN, кроме того, используется с целью допуска к интернет-контенту, недосягаемому в конкретных регионах, несмотря на то что это находится в зависимости от того, как хорошо обладатели контента применяют ограничения. Поставщики услуг VPN как правило запускают серверы в множества стран по всему миру, но кроме того дают возможность пользователям просто переходить среди них. Например, пользователи могут присоединяться через сервер одного государства для получения допуска к ограниченному содержимому в их собственной либо другой стране.

Пользователи таких государств, как Китай либо Турция, где правительства зачастую заблокируют допуск к конкретным интернет-сайтам, по причине политических факторов, как правило применяют VPN, для того чтобы обойти данные ограничения.

При развертывании VPN на интернациональном уровне необходимо удостовериться в том, что законы и правила различных государств никак не нарушаются, так как далее могут быть ограничены сервисы VPN. Целесообразно выделить, что в Российской Федерации существовали предложения о запрете VPN, однако, до тех пор, пока их не поддержали. Суть заключена в том, чтобы исследовать законы в различных государствах,

где станет располагаться модуль VPN, для того чтобы удостовериться в его законности и наличии правил, которые могут ослабить конфиденциальность.

По мере увеличения разнообразия и интенсивному росту кибер-угроз, сетевым администраторам нужно сбалансировать стремление полностью заблокировать внутренние сети своей организации с целью доступа через интернет, одновременно необходимо обеспечить повсеместный доступ к внутренней сети из множества удаленных гаджетов, сотрудников, клиентов и IoT. Данный баланс можно достигнуть в результате использования виртуальной частной сети (VPN), которая использует интернет с целью обеспечения безопасного доступа к виртуальной сети.

Наилучшим методом охраны конфиденциальных сведений и приложений считается ограничения допуска к ним посредством «общедоступных сетей», такие как сеть интернет. Сети, связывающие инфраструктуру, в которой хранится конфиденциальная информация, отделены от сети интернет, с целью их охраны, применяются IP-адреса, недосягаемые посредством интернета. Защищенность усиливается в связи с лимитированием доступа к данным сетям, отталкиваясь от этого, допуском к ним обладает только конкретный траффик и только с авторизированных наружных девайсов. Данные отделенные и односторонние сети именуются «частными сетями».

Организация имеет право обладать своей сетью, которая связывает частную ИТ-инфраструктуру и пк работников с коллективной интрасети. Эта сеть предоставляет возможность получения допуска ко всем внутренним ИТ-услугам, подобным заработной плате, электронной почте и т. д. в основном офисе компании. По мере роста компании индивидуальная сеть так же имеет возможность расширяться до необходимого количества филиалов.

С целью определения взаимосвязи среди представительств для их индивидуальной сети, при сохранении сети в отдельности от сети интернет зачастую используется отведенный транспорт сведений с арендованными

направлениями электросвязи. Телекоммуникационные обслуживание, которое применяется в формировании данной взаимосвязи между местоположениями достаточно дороги, для данного нужны наиболее экономные варианты.

Вследствие достижений в сфере криптографии, вычислительной техники и интернета возникла возможность зашифровывать трафик сведений и туннелировать его посредством сети интернет на компьютер, находящийся в индивидуальной сети. Безопасный туннель формирует виртуальную взаимосвязь, расширяющую личную сеть посредством общедоступной.

VPN способен использовать одну из множества технологий, подобных защищенности протокола IP (IPsec), защищенность транспортной степени (SSL/TLS), защищенность транспортной степени данных (DTLS), безопасное подсоединение девайсов либо сетей посредством общедоступной сети, с целью расширения либо создания личной сети.

Эта же методика, применяемая с целью формирования виртуального объединения среди сетей, может использоваться с целью подсоединения приборов пользователя к индивидуальной сети. Единое применение VPN – это обеспечение отдаленных сотрудников безопасного допуска посредством сети интернет к ИТ-услугам собственной фирмы. Работники используют VPN-клиентов, которые определены в коллективных ноутбуках либо мобильных девайсах, с целью подсоединения к VPN-серверу, пребывающего в индивидуальной сети фирмы.

Случай применения удаленного доступа никак не обладает ограничения для работников. Каждое устройство, подключенное к сети интернет, способно применять VPN, для того чтобы быть составляющей индивидуальной сети. Приборы могут быть как вычислительные, так также интеллектуальные.

Отталкиваясь от этого, по мере подключения большего количества приборов к глобальной сети, увеличивается степень угроз кибер-атак. VPN-допуск к важным приборам предоставляет шанс уменьшить возможные опасности. Грамотно реализованная VPN дает возможность только испытанным приборам получать допуск к индивидуальной сети и внедрять жесткие ресурсы контроля допуска для его снабжения с минимальными привилегиями. Подобные мероприятия сокращают число атак, которые доступны взломщикам, чтобы поставить под угрозу защищенность сети.

VPN-решения, кроме того гарантируют обоюдную аутентификацию, в которой как VPN сервер, так и соединительный механизм аутентифицируют друг друга. При успехе пользователь, приобретающий допуск к сети, отожествится с применением имени пользователя/пароля и, свободно, с использованием иной формы аутентификации, которая способна быть маркером защищенности, к примеру, применяя мобильный телефон либо смарт-карту. Сразу после аутентификации устройства и пользователя VPN сервер способен использовать принципы допуска, для того чтобы пользователь приобретал допуск только лишь к этим подмножествам систем/служб, к которым у него имеются полномочия допуска. [3]

Иное преимущество защищенности, которое гарантирует применение VPN, это кодирование сведений, что предоставляет охрану от подслушивания и утраты сведений.

На сегодняшний день набирает известность применение SaaS сервисов. Они могут гарантировать распределенное использование ресурсов.

Однако не все дополнения SaaS дают достаточно большую степень безопасности. Как правило дополнения SaaS рассчитывают только лишь на аутентификацию имени пользователя и пароля. Никак не придерживаясь рекомендаций по безопасности для защиты паролем и блокировки учетных записей при безуспешных попытках, для того чтобы приобрести запрещенный допуск, могут применяться атаки и эксплойты с

использованием грубой силы в незначительных механизмах возобновления пароля. По этой причине целесообразным шагом станет решение принудительных коллективных политик защищенности с поддержкой VPN для подсоединения к коллективной сети, а потом с целью допуска к приложениям SaaS посредством коллективной сети.

HTTPS, кроме того, никак не способен рассматриваться в качестве альтернативы VPN. HTTPS никак не может регулярно применяться в период всего сеанса веб-просмотра. Он, как правило, используется только лишь на определенных веб-сайтах и только лишь с целью конкретных транзакций, в которых передаются конфиденциальные сведения, подобные имени пользователя/паролю либо сведения о кредитной карте. HTTPS совершает хорошую работу в целях охраны конфиденциальных данных в период применения, однако для конфиденциальности всего сеанса просмотра веб-страниц, а также охраны трафика в целом при подсоединении к ненадежным сетям, правильнее всего применять VPN.

HTTPS применяет TCP также гарантирует защищенность для интернет-приложений. Таким образом, он никак не способен гарантировать траффик со всех не интернет-приложений, которые могут применяться в организации, таких как электронная почта либо VoIP и потоковые приложения, которые никак не полагаются в TCP, подобные Skype либо Spotify. При применении VPN полный траффик с устройства, вне зависимости от приложения, формирующего траффик, возможно уберечь. Пребывая защищенным транспортным протоколом определенного дополнения, HTTPS не действует как виртуальная индивидуальная сеть, по этой причине не способен гарантировать все без исключения достоинства VPN, такие как допуск к единым папкам файлов, сетевым принтерам и иным ресурсам наиболее крупной индивидуальной сети. [4]

Главной целью VPN считается предоставление безопасного допуска к индивидуальной сети, не присоединенной непосредственно к физической

индивидуальной сети. Подобным способом, VPN расширяет все без исключения сервисы, которые доступны в индивидуальной сети, как и в случае если бы приборы непосредственно подключались к ней. Коллективные ИТ-эксперты имеют все шансы обеспечивать подобные обслуживание, как файловые серверы, серверы прессы, веб-сайты интрасети, концепции ERP, серверы дополнительного снятия копий и т. д. Данные работы предусмотрены только лишь для внутреннего применения, однако с использованием VPN работник никак не может являться ограничен физическим месторасположением, а напротив, обладает непосредственным подсоединением к внутренней ИТ-сети с каждой географической точки.

Список используемой литературы:

1. Браун, Стив Виртуальные частные сети / Стивен Браун; Пер.с англ. О. Труфанов. – М.: Лори, 2001г. – XX.
2. Макаренко С. И. Информационная безопасность: учебное пособие для студентов вузов. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009г.
3. Родичев Ю.А. "Нормативная база и стандарты в области информационной безопасности", 2017г.
4. Нестеров А.С. "Основы информационной безопасности", 2016г.