УДК 004.056.5

ЗАЩИТА РЕСУРСОВ СЕТЕЙ НА ОСНОВЕ ТЕХНОЛОГИИ VPN

Храмов Н.Р.

ХТИ – филиал СФУ, Россия, Абакан, e-mail: khti@khakassia.ru

Возникновение VPN имеет прямую связь с услугой, используемой в конце 60-х годов Centrex, оказываемой в телефонных сетях. Centrex это термин всех методов оказания услуг деловой связи одновременно абонентам одной или нескольких компаний на базе одной обоюдно используемой учрежденческой станции PBX – Private Branch Exchange (приватная линия связи). С целью убрать ограничения, присущие Centrex, специалистами была выдвинута идея VPN, или виртуальной частной сети. Она предполагалась как объединение пользователей одной корпоративной сети, удаленных друг от друга. В наше время сервисы VPN уже сильно продвинулись вперед в развитии и теперь данную услугу может приобрести любой пользователь глобальной сети интернет. В данной работе рассматривается тема виртуальных частных сетей, что такое виртуальная частная сеть, достоинства и недостатки, а также будет приведена сравнительная таблица ресурсов, предоставляющих услуги VPN с помощью, которой будет осуществлена оценка и выявления лучшего сервиса среди остальных, по средствам основных критериев безопасности, обеспечивающих защиту файлов и документов, а также анонимность при использовании VPN. Так же будет рассмотрена проблема использования сервисов VPN с целью обеспечения единой корпоративной сети организации.

Ключевые слова: виртуальные частные сети, оценка, таблица, сравнение, безопасность, проблема.

PROTECTION OF NETWORK RESOURCES ON THE BASIS OF VPN TECHNOLOGY

Khramov N.R.

Khakassian Technical School (branch of Siberian Federal University), Abakan, e-mail: khti@khakassia.ru

The emergence of VPN has a direct connection with the service used in the late 60s Centrex, provided in telephone networks. Centrex is the term for all methods of providing business communications services simultaneously to subscribers of one or several companies based on one mutually usable office station PBX—Private Branch Exchange (private link). In order to remove the limitations inherent in Centrex, experts put forward the idea of a VPN, or virtual private network. It was intended as an association of users of the same corporate network, remote from each other. Nowadays, VPN services are already well advanced in development and now this service can be purchased by any user of the global Internet. This work discusses the topic of virtual private networks, what is a virtual private network, advantages and disadvantages, and also provides a comparative table of functions that provide VPN services, it will be used to determine the best VPN service among others providing anonymity and protecting data. There will also be considered the topic of using VPN service in order to ensure a single corporate network.

Keywords: private, assessment, table, comparison, security, problem, network, virtual

Введение. Появление интернета повлекло за собой развитие различных направлений в сфере поиска, использования, хранения, передачи информации и в то же время создало проблемы. К таким проблемам относится надежность хранения информации, актуализация информации и совместная работа с информацией [1].

Проникновение сетевых технологий во все сферы жизни вызвало необходимость создания защищенных сетей для работы компаний и крупных корпораций по причине приватности данных проходящих через рабочие компьютеры и личные устройства сотрудников данных предприятий. Для этого была изобретена технология под названием виртуальная частная сеть. Технология позволяет объединять сотрудников одной фирмы в одну сетевую среду, поверх основной, в которой происходит работа компании и её

документооборот. В наше время виртуальные частные сети используются во многих сферах информационных технологий и позволяют создавать безопасную рабочую среду для пользователей определенного сетевого окружения. Данные технологии имеют и негативную сторону такую как, доступ к запрещенным сайтам и информации. Итак, спрос на данную технологию очень велик, однако не все продукты, позволяющие войти в VPN, являются безопасными.

Цель исследования: оценить безопасность применения виртуальных частных сетей (VPN). Для достижения цели были поставлены следующие задачи: изучить понятие виртуальные частные сети; проанализировать свойства данных сетей их преимущества и недостатки, сравнить сервисы VPN; изучить достоинства применения сервисов VPN в масштабе предприятия, провести опрос с целью выяснения знаний студентов о сервисе VPN.

Использованы **методы исследования**: анализ литературы, опрос, наблюдение.

Результаты. Возникновение VPN связывается с услугой Centrex, используемой в конце 60-х годов в телефонных сетях [2]. Centrex – метод оказания услуги деловой связи одновременно абонентам на базе одной используемой учрежденческой станции PBX — Private Branch Exchange (приватная линия связи). С целью убрать ограничения, присущие Centrex, специалистами была выдвинута идея VPN, или виртуальной частной сети. Она предполагалась как объединение пользователей одной корпоративной сети, удаленных друг от друга. В наше время сервисы VPN уже сильно продвинулись вперед в развитии и теперь данную услугу может приобрести любой пользователь глобальной сети интернет. Аббревиатура VPN расшифровывается как Virtual Private Network. В переводе на русский — виртуальная частная сеть. VPN – технология, которая обеспечивает зашифрованное соединение поверх Интернет-соединения пользователя [3].

Отметим две основные функции VPN:

1. Виртуальная частная сеть маскирует реальный IP пользователя, создавая возможность полной анонимности в сети. То есть пользователь заходит на сайт, например, в одном регионе, а IP-пользователя считается как из другого региона. Иными словами, изменены свойства геолокации.

2. Виртуальная частная сеть зашифровывает соединение – ни провайдер обеспечивающий Интернет-соединение пользователя, ни системный администратор не смогут определить, точки входа пользователя. Системный администратор или провайдер, когда пользователь не подключен к VPN, имеет доступ к истории поиска пользователя. При подключении пользователя к VPN – только то что вы подключились через VPN. Данная функция защищает от действий злоумышленников по перехвату данных.

Для оценки безопасности сервисов VPN необходимо привести сравнить и сервисы по основным пунктам безопасности и выделить наиболее безопасный и удобный в использовании сервис. Сервисы VPN и характеристики, по которым они оценивались, приведены в таблицах 1 и 2.

Мы не оценивали сервисы по критерию стоимости, так как данные сервисы выполняют очень важную роль, их функциональность и качество обеспечиваются не маленькой ценой, но в ходе выбора сервиса VPN экономить не стоит так, как только качественный сервис может обеспечить безопасность на должном уровне.

Охарактеризуем выбранные нами критерии удобства использования виртуальных частных сетей:

Сложность установки – данный критерий был выбран для оценки данных сервисов так как их за частую используют не уверенные пользователи информационных систем, следовательно, данный процесс может вызвать трудности, а также в следствии не правильном установки может пострадать безопасность.

Сложность установки соединения – также, как и в случае с установкой сервиса, процесс установки соединения может быть довольно сложным, а также важным в данном случае так как от данного этапа зависит безопасность подключенного соединения.

Создание онлайн аккаунта – данный процесс больше относится к удобству обращения с сервисом и включен как критерий оценки удобства использования.

Количество поддерживаемых языков интерфейса – является одним из критериев оценки удобства для пользователей из разных стран.

Автоматическая установка соединения после перезагрузки – данный пункт важен и в удобстве, и в безопасности, так как при присутствии данной функции повышается и безопасность так как она нивелирует шанс подключения к сети интернет без включенного VPN по средствам автоматического подключения, и избавляет от необходимости вручную подключаться к VPN.

Обучение пользователя сервиса – данный пункт так же связан с удобством использования, так как обучение использованию программного обеспечения является залогом его внедрения в информационную систему организации (предприятия).

Заполнение данными таблиц основано на результатах проведенных опросов среди пользователей виртуальных частных сетей.

На основе анализа данных таблицы 1 выигрышно выглядит сервис VPN Avast Secure Line VPN, хотя по критериям он и не особо отличается от остальных сервисов, основным его отличием является количество языков интерфейса оно составляет 24 языка, что говорит о его распространенности и популярности.

Таблица 1 - Оценка удобства сервисов VPN

Критерии	СервисVPN				
	Avast SecureLine VPN	Avira Phantom VPN Pro	Cisco Any Connect Secure Mobiliti Client	ExpressVPN	F-secure FREEDOME VPN
Сложность установки ПО	Легкая	Легкая	Ориентирована на опытных пользователей	Легкая	Легкая
Простота установки соединения	Легкая	Легкая	Ориентирована на опытных пользователей	Легкая	Легкая
Создание онлайн аккаунта	Имеется	Имеется	Отсутствует	Имеется	Отсутствует
Автоматическая установка соединения после перезагрузки	Отсутствует	Отсутствует	Отсутствует	Имеется	Имеется
Обучение пользователя сервиса	Имеется и реализовано на хорошем уровне	Имеется, но реализовано на слабом уровне	Имеется и реализовано на лучшем уровне	Имеется, но реализовано на слабом уровне	Имеется и реализовано на хорошем уровне
Количество языков интерфейса	24	13	21	2	20

Далее оценим данные сервисы по критериям безопасности и конфиденциальности. Охарактеризуем выбранные нами критерии безопасности и конфиденциальности:

Проверка на наличие DNS-утечки – если происходит утечка DNS-запросов, то Интернет-провайдер или владельцы DNS-серверов могут видеть пользовательскую историю просмотров, посещаемые пользователем веб-сайты и все приложения, которыми он пользовался. Если VPN настроено правильно, то оно обеспечит защиту от угрозы утечки DNS-запросов. Проверка на утечку DNS позволяет оценить надежность работы VPN.

Проверка на наличие WebRTC-утечки – функция сервиса VPN позволяет отслеживать утечку Веб-коммуникации в режиме реального времени (WebRTC – WebReal-Time Communications). WebRTC представляют собой набор стандартизированных функций, позволяющих веб-браузерам напрямую обмениваться данными друг с другом без необходимости использования промежуточного сервера [2]. Преимущества WebRTC в более высокой скорости и меньшей задержке при использовании видеочатов и приложений для передачи файлов по сравнению со своими аналогами. Однако любые два устройства, взаимодействующие друг с другом напрямую через WebRTC, должны использовать реальные IP-адреса. В теории это может позволить стороннему веб-сайту использовать

функцию WebRTC в браузере, чтобы определить реальный IP-адрес и использовать его для идентификации устройства пользователя.

Защита P2P и Torrent – данный пункт безопасности обеспечивает отслеживания утечки скачиваемых или передаваемых данных так как не все сервисы VPN способны скачивать файлы без буферизации данных[5].

Проверка на наличие утечки HTTP запросов – данный аспект безопасности обеспечивает отслеживание утечки запросов, то есть безопасности поиска в интернете, следовательно, важная функция для пользователей сервисов VPN.

Оценивать будем по двоичной системе оценок 1 и 0, 1 – присутствует, 0 – отсутствует.

Таблица 2 – Оценка характеристик сервисов VPNпо критериям безопасности и конфиденциальности

Сервис VPN	Безопасность и конфиденциальность			
	Проверка на наличие DNS-утечки	Проверка на наличие WebRTC-утечки	Защита P2P и Torrent	Проверка на наличие утечки HTTP запросов
Avast Secure Line VPN	1	1	1	1
Avira Phantom VPN Pro	1	1	1	1
Cisco Any Connect secure Mobiliti Client	1	1	1	1
ExpressVPN	1	1	1	1
F-secure FREEDOME VPN	1	1	1	1

Все выбранные для сравнения сервисы VPN обладают необходимыми функциями защиты информации, это обусловлено тем, что данные функции являются самыми необходимыми для любой виртуальной частной сети.

Эффективное применение информационных технологий в сочетании с технологиями в области информационной безопасности является одним из важнейших стратегических факторов повышения конкурентоспособности современных организаций и предприятий. Так как сеть – это коммуникационная среда для работников предприятий [4]. Технология виртуальных частных сетей позволяет решать эти задачи, обеспечивая связь между сетями, а также между удаленным пользователем и корпоративной сетью с помощью защищенного канала, «проложенного» в сети Интернет.

Достоинства использования виртуальных частных сетей для защиты информации в распределенных сетевых информационных системах масштаба организации (предприятия):

1. возможность защиты всей корпоративной сети — от крупных локальных сетей офисов до отдельных рабочих мест;

2. возможность защиты на всех участках сети – от локальных сетей до коммуникационных каналов глобальных сетей;

3. масштабируемость системы защиты – защита объектов различной сложности и производительности [3];

4. использование ресурсов открытых сетей в качестве отдельных коммуникационных участков корпоративной сети – угрозы, возникающие при использовании сетей общего пользования, будут предотвращены средствами защиты;

5. обеспечение подконтрольности работы сети и достоверная идентификация всех источников информации – обеспечена аутентификация трафика на уровне отдельных пользователей;

6. сегментация информационной системы и организация безопасной эксплуатации системы, обрабатывающей информацию различных степеней конфиденциальности, программными средствами защиты информации.

Исходя из приведенных выше достоинств VPN, следует, что данная технология является одной из важнейших необходимых для составляющих обеспечения информационной безопасности предприятий. «Если злоумышленники попытаются захватить данные, они не смогут их прочитать или использовать» [3, с. 62].

Среди недостатков технологии VPN недостатки, связанные с использованием протоколов [3,4]. Устранение и минимизация недостатков включают этапы:

1. обеспечение безопасности сетевого оборудования, внутренних ресурсов сети компании,

2. организации безопасного взаимодействия между удаленными офисами,

3. контроль доступа в интернет [4].

Учитывая актуальность применения технологии VPN, мы провели опрос среди студентов начальных курсов направления 09.03.03 Прикладная информатика, которые готовятся применить свои знания в сфере государственного и муниципального управления, до реализации дисциплины «Информационная безопасность».

На вопрос «Знаете ли вы что такое виртуальная частная сеть?» положительно ответили 42 % опрошенных студентов, 25 % ответили, что что-то слышали и видели в браузере и 33 % ничего не знают о технологии VPN.

Среди студентов, положительно ответивших на наш вопрос о знании VPN большая часть студентов, это 73 % используют технологию иногда, 9 % часто и 18 % никогда не используют. Возможно, это связано с тем, что лишь примерно треть из них (36 %) доверяют данной технологии. Многие студенты высказали опасение, что через сеть у них могут

«украсть» файл. И совсем не много опрошенных используют сети для занятий, не связанных с учебой (работой).

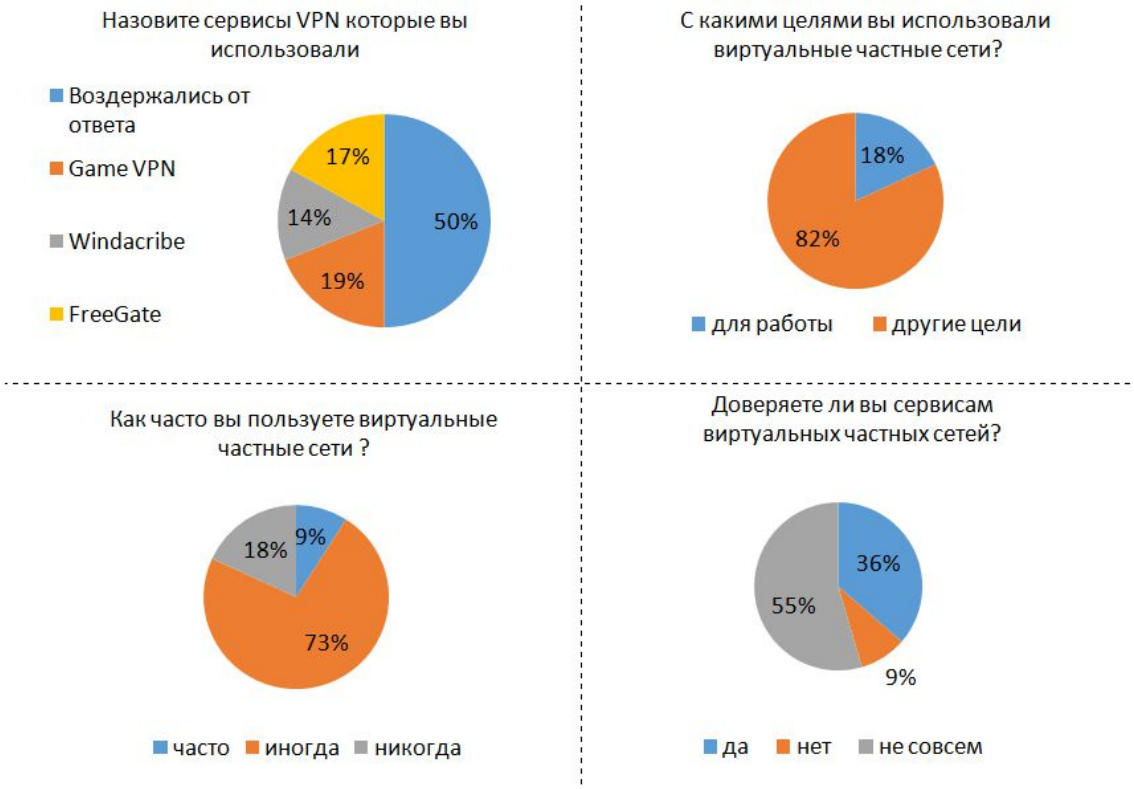

Рисунок 1 – Диаграммы по результатам опроса студентов

Заключение. В ходе данного исследования было выявлено что: виртуальные частные сети являются очень удобным и необходимым инструментом для осуществления безопасного документооборота предприятия Интернет и являются хорошим способом сохранения анонимности в сети интернет для обеспечения кибербезопасности. Следовательно, данная технология являются перспективной. Технология способна обеспечить решение рабочих задач в сети и информационную безопасность как предприятий, так частных лиц. В ближайшем будущем VPN будут являться одной из важнейших технологий к использованию которой, будут обращаться все предприятия и особенно те из них, которые работают на основе рассредоточенных в пространстве офисов.

Однако опрос студентов показал, что осведомленность студентов начальных курсов о технологии VPN связана со стереотипом о ней как исключительно о технологии-анонимайзере. В то время технология является одним из путей обеспечения информационной защиты, необходимость в которой обусловлена технологическим и информационным вызовами обществу и образованию в связи с обновляющимися

элементами культуры, инструментарием (компьютеры, ноутбуки, нетбуки, планшеты коммуникаторы, смартфоны т.д.) без преимуществ которых сложно представить учебный или производственный процесс [5]. В таких условиях сложно переоценить значение дисциплин содержанием которых является информационная безопасность.

Литература

1. Шафаль А. А. А. и др. Модернизация сети передачи данных //Вестник казанского технологического университета. – 2012. – Т. 15. – №. 18.

2. Дружинин Б.Н., Терехин И.Э. Развитие архитектуры доступа к услуге IP Centrex [Электронный ресурс]. URL: http://lib.tssonline.ru/articles2/fix-op/razv_arh_dost_uslug_ip_centrex (дата обращения 03.01.2019).

3. Николахин А.Ю Использование технологии VPN для обеспечения информационной безопасности // Экономика и качество систем связи. 2018. №3 (9). URL: https://cyberleninka.ru/article/n/ispolzovanie-tehnologii-vpn-dlya-obespecheniya-informatsionnoy-bezopasnosti (дата обращения: 03.01.2019).

4. Наполова Е.И., Кожевников С.В. Защита компьютерных сетей на основе технологии Virtual Private Network // Экономика и качество систем связи. 2018. №2 (8). URL: https://cyberleninka.ru/article/n/zaschita-kompyuternyh-setey-na-osnove-tehnologii-virtual-private-network (дата обращения: 03.01.2019).

5. Янченко И.В. Информационный и технологический вызовы образованию как точки роста // Актуальные проблемы гуманитарных и естественных наук. 2016. № 2-5. С. 8-10.