УДК 004

К ВОПРОСУ О ЗАЩИТЕ СЕТЕЙ НА ОСНОВЕ ТЕХНОЛОГИИ VPN

♦♦♦♦♦

TO THE QUESTION OF PROTECTION OF NETWORKS BASED ON VPN TECHNOLOGY

Багдасарян Р.Х.
кандидат технических наук,
доцент,
Краснодарский государственный институт культуры
rafael_555@mail.ru

Андреева А.А.
студентка,
Краснодарский государственный институт культуры
gelechka357@yandex.ru

Аннотация. VPN (Virtual Private Network) – это технология, которая позволяет создавать защищенное соединение между компьютерами или устройствами через Интернет. В статье рассматриваются причины возникновения данной системы, а также её сильные и слабые стороны. Данная тема является особо актуальной в настоящее время, что подчёркивает необходимость её всестороннего исследования.

Ключевые слова: VPN, информационная безопасность, информационные технологии, виртуальная частная сеть.

Bagdasaryan R.Kh.
Candidate of Technical Sciences,
Associate Professor,
Krasnodar State Institute of Culture
rafael_555@mail.ru

Andreeva A.A.
Student,
Krasnodar State Institute of Culture
gelechka357@yandex.ru

Annotation. VPN (Virtual Private Network) is a technology that allows you to create a secure connection between computers or devices over the Internet. The article discusses the causes of this system, as well as its strengths and weaknesses. This topic is particularly relevant at the present time, which emphasizes the need for its comprehensive study.

Keywords: VPN, information security, information technology, virtual private network.

Появление интернета привело к достижениям в различных областях поиска, использования, хранения и передачи информации, но оно также послужило источником некоторых проблем. Например, к таким проблемам относятся надежность хранения информации, обмен информацией. Проникновение сетевых технологий во все аспекты жизни создало потребность в безопасных сетях через рабочие компьютеры, персональные устройства и мобильные гаджеты. Именно поэтому была изобретена технология, известная во всем мире как виртуальные частные сети (VPN).

VPN (Virtual Private Network) – это технология, которая позволяет создавать защищенное соединение между компьютерами или устройствами через Интернет. Она используется для обеспечения безопасности и конфиденциальности данных при передаче их по сети. Однако, не все VPN-сети одинаково надежны и безопасны. Сегодня виртуальные частные сети используются во многих областях IY и позволяют пользователям в данной сетевой среде создать безопасное рабочее поле. Эта технология имеет и свои негативные стороны. Например, если виртуальная частная сеть настроена неправильно, могут произойти утечки DNS и IP-адресов, чем с удовольствием воспользуются в различных незаконных целях хакеры. На технологию VPN существует высокий спрос, но не все продукты, обеспечивающие доступ к VPN, являются безопасными.

Истоки VPN связаны со службой Centrex, которая использовалась в телефонных сетях в конце 1960-х годов. Основное преимущество Centrex заключается в том, что фирмы и компании при создании выделенных корпоративных сетей сэкономили значительные средства, необходимые для покупки, установки и эксплуатации собственных станций. Хотя абоненты Centrex используют общедоступные сетевые ресурсы и оборудование для связи друг с другом, сами они образуют так называемые закрытые группы пользователей CUG (Closed Users Group) с ограниченным внешним доступом, для которых на сетевых станциях внедряются виртуальные АТС (Private Branch Exchange). Чтобы преодолеть ограничения Centrex, специалисты придумали идею VPN или виртуальной частной сети. Он был разработан для подключения удаленных поль-

зователей к одной корпоративной сети. Сегодня услуги VPN прошли долгий путь, и приобрести эту услугу может любой пользователь глобальной сети Интернет. VPN расшифровывается как виртуальная частная сеть (виртуальная частная сеть). VPN – это технология, обеспечивающая зашифрованное соединение через Интернет.

Сегодня многие бесплатные сервисы предлагают возможность просто скачать приложение или конфигурационный файл с готовыми к использованию настройками. Несколько кликов – изменили свой IP-адрес и геолокацию. Но на самом деле бесплатные VPN-сервисы ненадежны. Цена и уровень безопасности – основные различия между бесплатными и платными VPN. Платные VPN различаются по типу и силе шифрования, оба из которых являются ключом к обеспечению высокого уровня безопасности. VPN эффективно устраняет узкие места и контролирует скорость провайдера. Чего не скажешь о бесплатных VPN, которые обычно вызывают заметное падение скорости. Разные VPN используют разные протоколы (например, открытый протокол, WireGuard) для защиты своих клиентов. Сетевые протоколы – это наборы правил, по которым участники сети взаимодействуют друг с другом.

Не меньшее влияние на установку VPN оказывают бюджетные факторы, так как покупка серверов стоит немалых денег, но, в отличие от бесплатных VPN, платные могут предложить сотни качественных серверов, обеспечивающих хорошую анонимность в сети. Очевидно, что платные VPN выигрывают в этом отношении. На сегодняшний день самым надежным и безопасным способом подключения к VPN является покупка собственного сервера (VPS) на конфиденциальном хостинге, тогда вы сможете напрямую настроить протоколы VPN, такие как OpenVPN или WireGuard.

Эффективное использование информационных технологий, наряду с технологиями защиты информации, является одним из важнейших стратегических факторов повышения конкурентоспособности современных организаций и предприятий. Потому что сеть – это средство коммуникации для сотрудников корпорации. Технология виртуальных частных сетей (VPN) позволяет решить эти задачи за счет предоставления защищенного канала связи между сетями, а также между удаленным пользователем и корпоративной сетью, «проложенной» в Интернете.

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

1) возможность защиты всей корпоративной сети – от большой локальной сети офисов до отдельных рабочих станций;

2) обеспечение подотчетности сетевых операций и надежной идентификации всех источников информации – аутентификация трафика на уровне отдельных пользователей;

3) возможность защиты всех частей сети – от локальных вычислительных сетей до каналов глобальной сети связи;

4) сегментация информационной системы и организация безопасной работы системы, обрабатывающей информацию различных уровней классификации с помощью программных средств защиты.

Вышеуказанные преимущества VPN делают эту технологию одним из самых необходимых элементов информационной безопасности, поскольку эта технология не позволяет злоумышленникам завладеть данными пользователя. Однако помимо преимуществ использования VPN-сети есть и определенные недостатки. К ним относятся проблемы, связанные с использованием протоколов, так как их неправильное использование может привести к утечке персональных данных [3, 4]. Предотвращение и минимизация дефектов включает в себя такие шаги, как: обеспечение безопасности сетевого оборудования, внутренних ресурсов корпоративной сети; контроль доступа в Интернет; организация безопасной связи между удаленными офисами.

Данное исследование показало, что виртуальные частные сети являются удобным и необходимым инструментом для обеспечения безопасности в Интернете и достойным способом сохранения анонимности в сети. Данная технология является перспективной, потому что она может решить проблемы создания деловых сетей и ин-

формационной безопасности как для предприятий, так и для частных лиц. В ближайшем будущем VPN станет одной из важнейших технологий, используемых всеми предприятиями, особенно теми, которые основаны на децентрализованных офисах.

Технология является одним из способов обеспечения информационной безопасности, необходимость которой вытекает из технологических и информационных вызовов, стоящих перед обществом и образованием, обновления элементов культуры и устройств (компьютеров, ноутбуков, планшетов, смартфонов и т.д.), без преимуществ которых трудно представить образовательный или производственный процесс. В таком контексте трудно переоценить значение дисциплин, содержанием которых является информационная безопасность.

Литература

1. Храмов Н.Р. Защита ресурсов сетей на основе технологий VPN / Н.Р. Храмов // Международный студенческий научный вестник. – 2019. – № 1.
2. Максименко В.Н. Особенности оценки качества инфокоммуникационных услуг контакт центра / В.Н. Максименко // Телекоммуникации и транспорт. – 2010. – № 10. – С. 39.
3. К вопросу организация хранения данных в мобильном приложении / В.А. Атрощенко [и др.] // Электронный сетевой политематический журнал «Научные труды КубГТУ». – 2014. – № 1. – С. 189–197.
4. К вопросу оценки достоверности информации для предотвращения mitm-атаки при передаче закрытой информации по открытым каналам связи / В.А. Атрощенко [и др.] // Современные проблемы науки и образования. – 2013. – № 3. – С. 82.

References

1. Khramov N.R. Protection of network resources based on VPN technologies / N.R. Khramov // International Student Scientific Bulletin. – 2019. – № 1.
2. Maksimenko V.N. Features of assessing the quality of infocommunication services of the contact center / V.N. Maksimenko // Telecommunications and transport. – 2010. – № 10. – C. 39.
3. On the issue of organizing data storage in a mobile application / V.A. Atroshchenko [et al.] // Electronic network polythematic journal «Scientific works of KubGTU». – 2014. – № 1. – P. 189–197.
4. On the issue of assessing the reliability of information to prevent a mitm attack when transmitting classified information via open communication channels / V.A. Atroshchenko [et al.] // Modern problems of science and education. – 2013. – № 3. – P. 82.