Чистая процентная маржа ОАО «БПС-Сбербанк» рассчитана как разница между процентными доходами и процентными расходами, соотнесенная с величиной доходных активов и выраженная в процентах:

$$[(303,4 – 140,4) / 5043,1] \times 100 = 3,23\ \%.$$

С учетом налога на прибыль, который для банковских организаций составляет 25 %, прибыль банка составит:

$$25,38 \times 0,75 = 19,03 \text{ тыс. руб.}$$

Таким образом, произведенные расчеты показывают, что за счет внедрения новой кредитно-сберегательной карты типа Visa Junior ОАО «БПС-Сбербанк» при сложившемся уровне доходности сможет получить до 19,03 тыс. руб. прибыли даже в случае, если новый продукт будет принят только 1 % клиентов банка, являющихся целевой аудиторией по предлагаемой услуге.

Библиографические ссылки

1. Бизнес-план (стратегический план развития) банка : сайт ОАО «БПС-Сбербанк». URL: https://www.sber-bank.by/page/revealing (дата обращения: 15.04.2021).
2. Финансовая отчетность ОАО «БПС-Сбербанк» за 2020 г. : сайт ОАО «БПС-Сбербанк». Минск, 2020 URL: https://www.sber-bank.by/page/financial-statements (дата обращения: 17.03.2021).
3. Короткевич А. И., Шпарун Д. В., Табала Д. Ч. Финансы : электронный учебно-методический комплекс для специальности: 1-25 01 04 «Финансы и кредит» ; БГУ, Экономический фак., Каф. банковской экономики. Минск : БГУ, 2018. 380 с.

УДК 330: 004.056.53

ЗАЩИТА ИНФОРМАЦИИ В КОРПОРАТИВНОЙ СЕТИ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ VPN

Д. В. Аникин

магистрант, Национальный исследовательский университет ИТМО, г. Санкт-Петербург, Российская Федерация, e-mail: anikin406@gmail.com

В статье рассматриваются проблемы безопасности, с которыми сталкиваются современные сспециалисты по защите информации, невозможно устранить с помощью какого-либо одного приложения. Хотя повышение уровня безопас-

ности оборудования, контроль обращения с помощью аутентификации, авторизации и учета, а также функции межсетевых экранов являются составными частями надлежащей сетевой защиты, в банках в том числе, этих возможностей все еще недостаточно, чтобы обезопасить сеть от стремительно распространяющихся через Интернет-червей и вирусов. Сеть должна уметь мгновенно выявлять и нейтрализовать любые угрозы.

Ключевые слова: защита информации; сетевые атаки; виртуальная частная сеть (VPN); программное обеспечение (ПО); малый офис/домашний офис (SOHO); туннелирование; IP-туннели.

INFORMATION PROTECTION IN CORPORATE NETWORK WITH USE OF VPN TECHNOLOGY

D. V. Anikin

Master's student, National ITMO Research University, St. Petersburg, Russian Federation, e-mail: anikin406@gmail.com

Security concerns which face modern spatiality on information protection cannot be eliminated by means of any one application. Though increasing the level of security of the equipment, control of access by means of authentication, authorization, and accounting and also functions of firewalls are components of proper network protection, these opportunities are still not enough to secure network against the worms which are promptly extending via the Internet and viruses. The network shall be able to reveal and neutralize any threats instantly.

Keywords: Information protection; Network attacks; Virtual private area network (VPN); Software; Small Office / Home Office (SOHO); Tunneling; IP Tunnels.

Организациям требуются безопасные, надёжные и недорогие способы соединения между собой нескольких сетей, которые позволят подключать филиалы и поставщиков к сети главного офиса корпорации или банка. Кроме того, с учётом увеличения количества удалённых сотрудников предприятиям, банкам всё чаще требуются безопасные, надёжные и экономичные решения для подключения сотрудников, работающих в секторе SOHO (Small Office/Home Office – малый офис/домашний офис), а также в других удалённых местоположениях, к ресурсам корпоративных узлов.

Организации и банки используют сети VPN для сквозной конфиденциальной сетевой связи через сети сторонних компаний, например, через Интернет или сети экстранет. Туннель устраняет барьер, связанный с расстоянием, и позволяет удалённым пользователям получать доступ к сетевым ресурсам на центральном узле. VPN представляет собой частную сеть, которая создаётся с по-

мощью туннелирования в публичной сети (как правило, в Интернете). VPN – это среда передачи данных со строгим контролем обращения, позволяющим устанавливать равноправные подключения в пределах определённого целевого сообщества.

Интернет-вирусы могут распространяться по всему миру в считанные минуты. Сеть должна мгновенно выявлять и нейтрализовывать любые угрозы – от червей и вирусов. Межсетевые экраны могут многое, но они не в состоянии защитить от вредоносного ПО и разнообразных атак.

Первые сети VPN представляли собой обычные IP-туннели, в которых проверка подлинности или шифрование данных не выполнялись. Например, универсальная инкапсуляция при маршрутизации (Generic Routing Encapsulation, GRE) – это протокол туннелирования, разработанный компанией Cisco, который позволяет инкапсулировать пакеты протоколов сетевого уровня различного типа внутри IP-туннелей. Благодаря этому создаётся виртуальный канал «точка-точка» до маршрутизаторов Cisco в удалённых точках поверх IP-сети.

В настоящее время под виртуальными частными сетями обычно понимают защищённую реализацию сети VPN с шифрованием (например, IPsec VPN). Для реализации сетей VPN требуется шлюз VPN. Шлюзом VPN может быть маршрутизатор, межсетевой экран или устройство адаптивной защиты Cisco ASA (Adaptive Security Appliance).

ASA – это автономный межсетевой экран, который объединяет в пределах одного образа программного обеспечения функции межсетевого экрана, концентратора VPN, а также системы предотвращения вторжений.

В сетях VPN применяются виртуальные подключения, которые проходят от частной сети организации через Интернет к удалённому узлу или компьютеру сотрудника. Информация, поступающая из частной сети, передаётся в защищённом режиме по публичной сети, что позволяет создать виртуальную сеть.

Преимущества сети VPN:

- *Сокращение затрат* – сети VPN позволяют организациям использовать предоставляемую сторонними компаниями недорогую транспортную среду Интернета для подключения удалённых офисов и пользователей к основному узлу, то есть отказаться от применения дорогостоящих выделенных каналов WAN и банков модемов. Кроме того, благодаря появлению недорогих технологий, обеспечивающих высокую пропускную способность (например, DSL), организации могут использовать сети VPN для сокращения своих затрат на организацию связи при одновременном повышении уровня пропускной способности удалённых подключений.

- *Масштабируемость* – благодаря сетям VPN организации могут использовать инфраструктуру Интернета в пределах интернет-провайдеров и устройств, что позволяет упростить процедуру добавления новых пользователей. Поэтому организации могут серьезно наращивать пропускную способность без значительного изменения инфраструктуры.

- *Совместимость с широкополосной технологией* – благодаря сетям VPN мобильные и удалённые сотрудники могут эффективно использовать высокоскоростную широкополосную связь, например, DSL и кабельные каналы, для обращения к сетям своих организаций. Широкополосная связь обеспечивает

высокую гибкость и эффективность. Высокоскоростные широкополосные подключения также позволяют создавать экономичные решения для подключения удалённых офисов.

- *Безопасность* – сети VPN могут поддерживать различные механизмы защиты, обеспечивающие наивысший уровень безопасности, благодаря применению сложных протоколов шифрования и аутентификации, позволяющих защищать данные от несанкционированного обращения [3].

Методы. Существуют сети VPN методы двух типов:

1. Site-to-site (межузловые или межфилиальные);
2. Remote access (удалённого обращения) [2].

1. *Site-to-site VPN.* Сеть Site-to-site VPN создаётся, когда устройства на обеих сторонах подключения VPN заранее знают настройки сети VPN.

Сеть VPN остается статической, и внутренние узлы не знают о существовании VPN. В межузловой сети VPN оконечные компьютеры отправляют и получают обычный трафик TCP/IP через шлюз VPN.

Шлюз VPN отвечает за инкапсуляцию и шифрование исходящего трафика для всего трафика, поступающего с конкретного объекта. Затем шлюз VPN передаёт этот трафик через туннель VPN по Интернету в равноправный соседний шлюз VPN на стороне приема. При получении данных соседний шлюз VPN удаляет заголовки, расшифровывает содержимое и передаёт пакет в узел назначения по своей частной сети.

Межузловая сеть VPN представляет собой расширение классической сети WAN. Межузловые сети VPN позволяют подключать друг к другу целые сети, например сеть филиала с сетью главного офиса компании. Ранее для подключения площадок между собой требовалась выделенная линия или подключение Frame Relay. Но так как сегодня большинство корпораций имеют доступ к Интернету, то вместо таких подключений можно использовать межузловые сети VPN (рисунок 1).

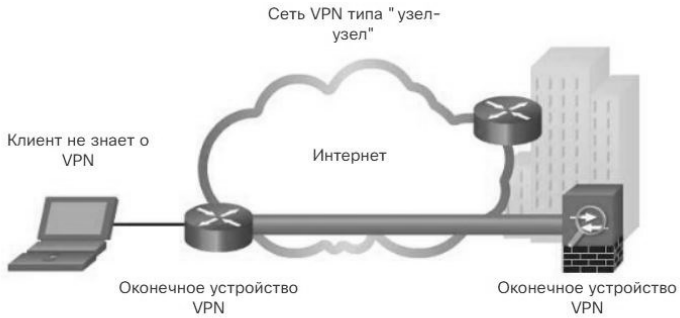

Рисунок 1 – **Межузловая сеть VPN**

Примечание – Источник: [1].

2. *Сети VPN удалённого обращения***.** В то время как межфилиальная сеть VPN используется для подключения целых сетей, сеть VPN удалённого обращения (remote access) соответствует потребностям удалённых и мобильных сотрудников, а также позволяет передавать трафик от потребителей к компаниям через экстранет. VPN удалённого обращения создаётся в тех случаях, когда информация о VPN не является статической, и может изменяться динамически, а сам канал может включаться и отключаться. Сети VPN удалённого обращения поддерживают архитектуру «клиент-сервер», в рамках которой клиент VPN (удалённый компьютер) получает защищённый доступ к корпоративной сети через сервер VPN на границе сети.

Они используются для подключения отдельных компьютеров, которым требуется безопасный доступ к корпоративной сети через Интернет. Как показано на рисунке, при работе через Интернет удалённые сотрудники обычно используют широкополосные, DSL, беспроводные или кабельные подключения.

На оконечных устройствах мобильных пользователей может требоваться установка клиентского ПО для VPN. Например, на всех узлах может быть установлено ПО Cisco AnyConnect Secure Mobility Client.

Когда узел пытается отправить любой трафик, клиентское ПО Cisco AnyConnect VPN инкапсулирует и шифрует этот трафик. Затем зашифрованные данные отправляются через Интернет на шлюз VPN на границе сети назначения. При получении данных шлюз VPN работает точно так же, как для межузловых сетей VPN (рисунок 2).

Результаты. В ходе защиты информации в корпоративной сети при помощи технологии VPN, выяснилось, что предложенная технология способна обеспечивать надёжное шифрование при передаче данных по открытым каналам связи.

Данная технология предоставляет отчёт по соединению между узлами в режиме реального времени, а также аномалий в сети, независимо от ее масштаба, что гарантирует высокую степень её защищённости.

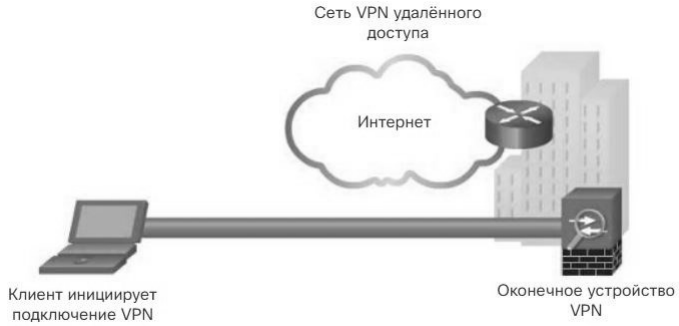

Рисунок 2 – **VPN удалённого обращения**

Примечание **–** Источник: [1].

Библиографические ссылки

1. Виды сетевых атак : сайт. URL: https://moluch.ru/conf/tech/archive/5/1115 (дата обращения: 12.05.2021).
2. KDD Cup 1999 Data : сайт. URL: https://kdd.ics.uci.edu/databases/kdd-cup99/task.html (дата обращения: 23.04.2021).
3. Middlemiss M., Dick Grant. Feature Selection of Intrusion detection data using a hybrid genetic of hybrid Intelligent systems. IOSPress Amsterdam // Design and application of hybrid intelligent systems. January 2003. P. 519–527.

УДК 331.5

СТИМУЛИРОВАНИЕ РАЗВИТИЯ РЫНКА ТРУДА В РЕСПУБЛИКЕ БЕЛАРУСЬ

Т. С. Астрейко[1)], А. В. Вериго[2)]

[1)] *студентка 3 курса, Белорусский государственный университет, г. Минск, Республика Беларусь, e-mail: tatianaastreyko@gmail.com*

[2)] *кандидат экономических наук, кафедра банковской экономики, Белорусский государственный университет, г. Минск, Республика Беларусь, e-mail: anverigo@yandex.ru*

В данной статье выявлены особенности безработицы в Республике Беларусь, её виды, проведен анализ безработицы в Республике Беларусь. Определены проблемы возникновения безработицы. Представлены пути стимулирования рынка труда Республики Беларусь.

Ключевые слова: рынок; безработица; труд; инновации; предприятие; заработная плата.

STIMULATING THE DEVELOPMENT OF THE LABOR MARKET IN THE REPUBLIC OF BELARUS

T. S. Astreyko[1)], A. V. Verigo[2)]

[1)] *3rd year Student, Belarusian State University, Minsk, Republic of Belarus, e-mail: tatianaastreyko@gmail.com*

[2)] *PhD in Economics, Department of Banking Economics, Belarusian State University, Minsk, Republic of Belarus, e-mail: anverigo@yandex.ru*