УДК 316.733 https://doi.org/10.33619/2414-2948/70/45

ПРОБЛЕМЫ СЕТЕВОЙ БЕЗОПАСНОСТИ И ЭФФЕКТИВНАЯ ЗАЩИТА ОТ СЕТЕВЫХ АТАК

©Арзиева Ж., *Каракалпакский государственный университет им. Бердаха, г. Нукус, Узбекистан, a_jamila@karsu.uz*
©Нукусбаев Н. Ж., *Каракалпакский государственный университет им. Бердаха, г. Нукус, Узбекистан, nawriznukusbaev@gmail.com*

NETWORK SECURITY ISSUES AND EFFECTIVE PROTECTION AGAINST NETWORK ATTACKS

©Arzieva J., *Karakalpak State University named after Berdakh, Nukus, Uzbekistan, a_jamila@karsu.uz*
©Nukusbaev N., *Karakalpak State University named after Berdakh, Nukus, Uzbekistan, nawriznukusbaev@gmail.com*

Аннотация. В этой статье определяется VPN как виртуальная частная сеть. Эта технология основана на формировании внутренней сети внутри другой сети для обмена всей информацией между пользователями с целью обеспечения надежной защиты.

Abstract. This article defines a VPN as a virtual private network. This technology is based on the formation of an internal network within another network to exchange all information between users in order to provide reliable protection.

Ключевые слова: сетевая безопасность, виртуальная частная сеть, безопасность интернет-протокола, система обнаружения вторжений, протоколы, отказ в обслуживании, межсетевой экран, IP-адрес.

Keywords: Network Security, Virtual Private Network, Internet Protocol Security, Intrusion Detection System, Protocols, Denial of Service, Firewall, IP Address.

Развивается и модернизируется использование компьютерных и информационных технологий, телекоммуникаций, сетей передачи данных, интернет-услуг, которые входят в приоритеты политики нашей страны [13]. Широкое внедрение современных информационных технологий во все сферы нашего общества в повседневную жизнь обеспечит достижение наших будущих целей. Использование Интернета в любой отрасли увеличивает производительность [1-4].

Быстрый обмен данными по сети может сэкономить время. В частности, формирование электронного правительства в нашей стране и организация усиления взаимодействия власти и населения на его основе будет осуществляться с использованием сети. Эффективное использование сети обеспечит формирование демократического информационного общества. В таком обществе скорость обмена информацией увеличится, и будут более быстрые результаты в сборе, хранении, обработке и использовании информации.

Однако защита от таких проблем, как несанкционированный доступ к сети, использование и изменение информации, потеря информации стала актуальной проблемой. Предприятия, организации и государственные учреждения, которые подключаются к сети,

Т. 7. №9. 2021
https://doi.org/10.33619/2414-2948/70

должны уделять пристальное внимание сетевой безопасности, прежде чем подключаться к сети для обмена информацией. Сетевая безопасность достигается за счет использования различных инструментов и методов, мер и мер обеспечивающих надежную и систематическую передачу, хранение и обработку информации. Инструменты сетевой безопасности должны уметь быстро выявлять угрозы и реагировать на них. Существует много типов угроз сетевой безопасности, но они делятся на несколько категорий [5-8]:

- Подслушивание путем атаки на передачу информации;
- отказ в предоставлении услуг; (Отказ в обслуживании)
- Сканирование портов.

В процессе передачи информации информация может быть перехвачена, изменена и заблокирована без ведома пользователя с помощью телефонных линий, обмена мгновенными сообщениями через Интернет, видеоконференцсвязи и факсов с атакой на слушание и изменение. Эта атака может быть проведена через несколько протоколов сетевого анализа. С помощью программного обеспечения для атаки CODEC (преобразование аналогового видео- или аудио сигнала в цифровой и наоборот) легко преобразует цифровой звук в высококачественные аудиофайлы большого объема (WAV). Обычно процесс выполнения этой атаки для пользователя совершенно незаметен. Система выполняет указанные операции без чрезмерного напряжения и шума. Нет сомнений в краже информации. Только те, кто знает об этой угрозе заранее и хочет, чтобы отправляемая информация сохраняла свою ценность, смогут обмениваться информацией через защищенную сеть в результате специальных мер сетевой безопасности. Существует несколько технологий, которые могут быть эффективными против прослушивания и изменения информации, передаваемой по сети:

- протокол IPSec (безопасность интернет-протокола);
- виртуальная частная сеть VPN (Virtual Private Network);
- IDS (система обнаружения вторжений).

Ipsec (безопасность интернет-протокола) обеспечивает безопасный обмен информацией по сети с использованием этих протоколов безопасности и алгоритмов шифрования. Этот специальный стандарт обеспечивает совместимость программного обеспечения и данных, а также оборудования с компьютерами в сети. Протокол IPsec обеспечивает конфиденциальность информации, передаваемой по сети, т.е. только отправитель и получатель могут ее понять, чистоту информации и аутентификацию пакетов. Использование современных информационных технологий стало необходимым инструментом развития любой организации, а протокол IPsec обеспечивает эффективную защиту:

- подключение головных офисов и филиалов к глобальной сети;
- удаленное управление предприятием через Интернет;
- защита сети, подключенной к спонсорам;
- Повышение безопасности электронной коммерции.

VPN (виртуальная частная сеть) определяется как виртуальная частная сеть. Эта технология основана на формировании внутренней сети внутри другой сети для обмена всей информацией между пользователями с целью обеспечения надежной защиты. Интернет используется в качестве сетевой основы для VPN [9-12].

Преимущество технологии VPN. Подключив локальные сети к общей сети VPN, можно построить недорогой туннель с высокой степенью защиты. Для создания такой сети необходимо установить специальный шлюз VPN на одном компьютере в каждой части сети для обмена информацией между филиалами. Обмен информацией в каждом отделе осуществляется очень просто. Если вам нужно отправить данные в другую часть сети VPN,

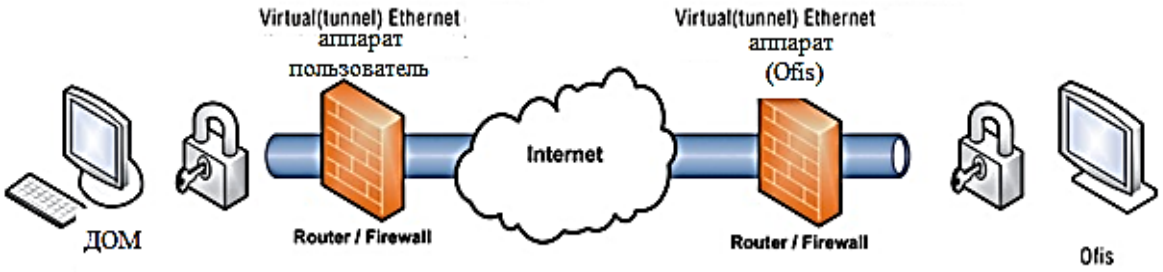
Т. 7. №9. 2021
https://doi.org/10.33619/2414-2948/70

то все данные будут отправлены на шлюз. Шлюз, в свою очередь, обрабатывает данные, шифрует их с помощью надежного алгоритма и отправляет через Интернет на шлюз в другом филиале. В указанный момент данные просто расшифровываются и передаются на конечный компьютер. Все это делается совершенно незаметно для пользователя и ничем не отличается от работы в локальной сети. Используя атаку подслушивания, услышанная информация будет непонятной.

Кроме того, VPN - отличный способ подключить отдельный компьютер к локальной сети организации. Допустим, вы в командировке со своим ноутбуком, и вам нужно подключиться к своей сети или получить оттуда некоторую информацию. С помощью специальной программы вы можете подключиться к VPN-шлюзу и вести себя как любой другой сотрудник в офисе. Это не только удобно, но и недорого.

Принцип работы VPN. Помимо нового оборудования и программного обеспечения, для настройки VPN требуются два основных компонента: протокол данных и инструменты безопасности.

Система обнаружения неавторизованного доступа (IDS) идентифицирует метод или средства, с помощью которых предпринимается попытка скомпрометировать систему или политику сетевой безопасности. Системы обнаружения несанкционированного доступа насчитывают почти четверть века. Первые модели и прототипы систем обнаружения несанкционированного доступа использовали анализ данных аудита компьютерных систем. Эта система делится на два основных класса. Он разделен на систему обнаружения сетевых вторжений и систему обнаружения вторжений на хост.



В архитектуру систем IDS входят:

- сенсорная система, собирающая и анализирующая состояние безопасности защищаемых систем;

- система аналитического блока для обнаружения подозрительных движений и атак на основе данных датчиков;

- хранилище результатов анализа и исходных данных;

- Консоль управления, которая позволяет настраивать систему IDS, отслеживать состояние IDS и защищенной системы, а также отслеживать конфликты, обнаруженные системами анализа разделов.

Эта система делится на два основных класса. Он разделен на систему обнаружения сетевых вторжений и систему обнаружения вторжений хоста. Принцип работы системы несанкционированного доступа к сети (NIDS) следующий:

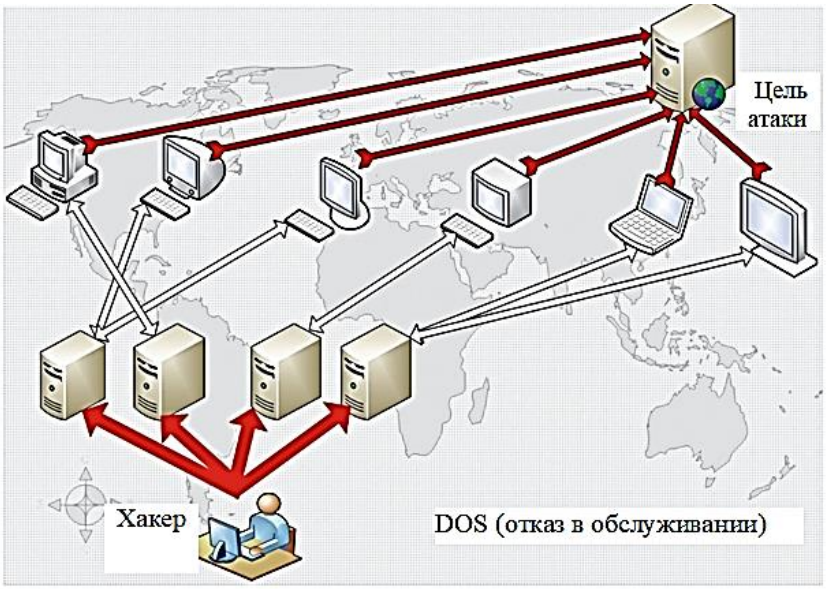
1. Проверяет трафик, имеющий доступ к сети;

2. Ограничивает вредоносные и неавторизованные пакеты.

Т. 7. №9. 2021
https://doi.org/10.33619/2414-2948/70

Подслушивание можно эффективно защитить, используя перечисленные меры безопасности.

DOS (отказ в обслуживании) Этот тип сетевой атаки называется атакой отказа в обслуживании. Злоумышленник пытается помешать легальным пользователям использовать систему или службу. Часто эти атаки осуществляются путем переполнения ресурсов инфраструктуры запросами на доступ к сервисам. Такие атаки могут быть нацелены на всю сеть, а также на отдельный хост. Перед атакой объект тщательно исследуется, то есть на наличие уязвимостей или недостатков используемых средств защиты сети, установленную операционную систему и максимальное время работы объекта. По результатам последующего обнаружения и проверки пишется специальная программа. На следующем этапе созданная программа отправляется на серверы самой высокой позиции. Серверы отправляют зарегистрированным пользователям в их базе данных. Пользователь, получивший приложение, устанавливает приложение, сознательно или не зная, что оно было отправлено доверенным сервером. Это может случиться с тысячами или даже миллионами компьютеров. Программа активируется на всех компьютерах в указанное время и непрерывно отправляет запросы на сервер атакуемого объекта. Сервер занят ответом на непрерывные запросы и не может выполнять свою основную работу. Сервер не обслуживает.



Наиболее эффективные способы защиты от атаки отказа в обслуживании:

- технология межсетевого экрана;
- Протокол IPsec.

Межсетевой экран — первое устройство защиты внутреннего и внешнего периметра. Межсетевой экран управляет входящими и исходящими данными в информационно-коммуникационных технологиях (ICT) и обеспечивает защиту ICT путем фильтрации данных, выполнения проверки информации на основе определенных критериев и принятия решения о том, должны ли пакеты входить в систему. Брандмауэр видит все пакеты, проходящие через сеть, проверяет пакеты в обоих направлениях (вход, выход) в соответствии с установленными правилами и решает, разрешить их или нет. Брандмауэр также обеспечивает защиту между двумя сетями, то есть защищает защищаемую сеть от открытой внешней сети. Перечисленные ниже преимущества средства защиты, особенно функция

Т. 7. №9. 2021
https://doi.org/10.33619/2414-2948/70

фильтрации пакетов, являются эффективным средством защиты от DOS-атак. Управление пакетными фильтрами:

- физический интерфейс, откуда приходит посылка;
- IP-адрес источника;
- IP-адрес получателя;
- порты отправления и приема транспортных средств.

Межсетевой экран не обеспечивает полную защиту от DOS-атак из-за некоторых недостатков:

- ошибки или упущения в конструкции - различные технологии межсетевых экранов не охватывают все точки доступа к защищаемой сети;

- Недостатки реализации — у каждого межсетевого экрана есть ошибки, если это сложный набор программного и аппаратного обеспечения. Кроме того, отсутствует общая методология тестирования, позволяющая определить качество реализации программного обеспечения и убедиться, что все указанные функции реализованы на межсетевом экране;

- Недостатки в использовании — работа межсетевых экранов, настройка на основе политики безопасности очень сложна, и во многих случаях встречаются случаи неправильной настройки межсетевых экранов. Эти недостатки можно устранить с помощью протокола IPsec. Подводя итог вышесказанному, можно обеспечить адекватную защиту от атак DOS за счет правильного использования межсетевых экранов и протокола IPsec.

Тип атаки сканирования портов используется чаще, чем компьютеры, предоставляющие сетевые службы. Нам нужно уделять больше внимания виртуальным портам, чтобы обеспечить безопасность сети. Потому что порты - это средство передачи данных по каналу. В компьютере 65 536 стандартных портов. Компьютерные порты можно сравнить с дверью или окном в доме. Атака на контрольно-пропускные пункты порта, кажется, указывает на то, что воры знали, были ли двери и окна открыты или закрыты, прежде чем войти в дом. Если вор заметит, что окно открыто, ему будет легче войти в дом. Хакер использует атаку проверки портов, чтобы получить информацию о том, открыт порт или не используется во время атаки.

Одновременно отправляется сообщение для анализа всех портов, в результате чего в режиме реального времени определяется, какой порт пользователь использует на компьютере, что является тонкой точкой компьютера. Точный номер порта позволяет определить, какую службу использует пользователь. Например, если анализ показывает следующие номера портов, по этим номерам можно определить имя службы.

- Порт №21: протокол обмена файлами FTP (протокол передачи файлов);
- Порт №35: частный сервер печати;
- Порт №80: протокол обмена гипертекстом HTTP-трафика (протокол передачи гипертекста [транспортный]);
- Порт №110: порт электронной почты POP3 (почтовый протокол 3).

Типы атак	эффективное решение
подслушивание (*Eavesdropping*)	IPSec(Internet protokol security) VPN(Virtual Private Network) виртуальная частная сеть IDS(Intrusion Detection system) обнаружение несанкционированного доступа
отказ в обслуживании(Denial-of-service)	протокол межсетевого экрана(Firewall) IPSec протокол
сканирование портов (*Port scanning*)	технология межсетевого экрана(Firewall)

Т. 7. №9. 2021
https://doi.org/10.33619/2414-2948/70

Эффективное решение для защиты от атак управления портами. Эффективное использование технологии отображения брандмауэра дает ожидаемый результат. Атаку можно предотвратить, введя в брандмауэр специальное правило, которое будет отвечать на запросы одновременной проверки всех портов.

Список литературы::

1. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей. М., 2017. 416 с.

2. Ганиев С. К., Каримов М. М., Ташев К. А. Ахборат хавсизлиги. Олий ўқўв юрти талабалари учун ўқўв қолланма. Тошкент, 2016.

3. Ганиев С. К., Каримов М. М., Ташев К. А., Арзиева Ж. Т. Информацияларды қорғаў Олий ўқўв юрти талабалари учун ўқўв қолланма. Нөкис, 2018.

4. Мазурова В. А. Ахборот хавфсилигининг жиноят-хукуклари. Barnaul:нашр Олтой университети (нашриет), 2004. S. 92-288.

5. Гольдштейн Б. С., Пинчук А. В., Суховицкий А. Л. IP-телефония. М.: Радио и связь, 2006.

6. Полканов Е. И., Шнепс-Шнеппе М. А., Крестьянинов С. В. Интеллектуальные сети и компьютерная телефония.:М., 2001.

7. Кислов Д. В., Летяго И. В. IP-телефония. Интернет. Мобильные телефоны. Компьютеры. М., 2007.

8. Галичский К. Компьютерные системы в телефонии. М., 2002. 400 с.

9. Днепров А. Бесплатные звонки через Интернет, Skype и не только. М., 2012.

10. Трошин М. В., Прокди Р. Г. Skype. Бесплатные телефонные звонки и видеосвязь через Интернет. М., 2011.

11. Браун С. Виртуальные частные сети VPN. М., 2002.

12. Ахборот технологияси. Ахборотларни криптографик мухофазаси. Маълумотларни шифрлаш алгоритми. Ўзбекистон Давлат стандарти. 2006.

13. Атамуратова Н. Б. Влияние информационных технологий на развитие туризма Узбекистана // Бюллетень науки и практики. 2020. Т. 6. №12. С. 297-305. https://doi.org/10.33619/2414-2948/61/33

References:

1. Shan'gin, V. F. (2017). Informatsionnaya bezopasnost' komp'yuternykh sistem i setei. Moscow. (in Russian).

2. Ganiev, S. K., Karimov, M. M., & Tashev, K. A. (2016). Akhborat khavsizligi. Olii ўқўv yurti talabalari uchun ўқўv қollanma. Toshkent.

3. Ganiev, S. K., Karimov, M. M., Tashev, K. A., & Arzieva Zh. T. (2018). Informatsiyalardy қorғaў Olii ўқўv yurti talabalari uchun ўқўv қollanma. Nөkis.

4. Mazurova, V. A. (2004). Akhborot khavfsiligining zhinoyat-khukuklari. *Barnaul:nashr Oltoi universiteti (nashriet),* 92-288.

5. Gol'dshtein, B. S., Pinchuk, A. V., & Sukhovitskii, A. L. (2006). IP-telefoniya. Moscow.

6. Polkanov, E. I., Shneps-Shneppe, M. A., Krest'yaninov, S. V. (2001).Intellektual'nye seti i komp'yuternaya telefoniya.: Moscow. (in Russian).

7. Kislov, D. V., & Letyago, I. V. (2007). IP-telefoniya. Internet. Mobil'nye telefony. Komp'yutery. Moscow. (in Russian).

8. Galichskii, K. (2002). Komp'yuternye sistemy v telefonii. Moscow. (in Russian).

9. Dneprov, A. (2012). Besplatnye zvonki cherez Internet, Skype i ne tol'ko. Moscow. (in Russian).

10. Troshin, M. V., & Prokdi, R. G. (2011). Skype. Besplatnye telefonnye zvonki i videosvyaz' cherez Internet. Moscow. (in Russian).

11. Braun, S. (2002).Virtual'nye chastnye seti VPN. Moscow. (in Russian).

12. Akhborot tekhnologiyasi. Akhborotlarni kriptografik mukhofazasi (2006). Ma"lumotlarni shifrlash algoritmi. Ўzbekiston Davlat standarti.

13. Atamuratova, N. (2020). Effect of Information Technologies on Development Tourism of Uzbekistan. *Bulletin of Science and Practice, 6*(12), 297-305. (in Russian). https://doi.org/10.33619/2414-2948/61/33

Работа поступила
в редакцию 08.08.2021 г.

Принята к публикации
12.08.2021 г.

Ссылка для цитирования:

Арзиева Ж., Нукусбаев Н. Ж. Проблемы сетевой безопасности и эффективная защита от сетевых атак // Бюллетень науки и практики. 2021. Т. 7. №9. С. 479-485. https://doi.org/10.33619/2414-2948/70/45

Cite as (APA):

Arzieva, J., & Nukusbaev, N. (2021). Network Security Issues and Effective Protection Against Network Attacks. *Bulletin of Science and Practice, 7*(9), 479-485. (in Russian). https://doi.org/10.33619/2414-2948/70/45