МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
Дальневосточный федеральный университет

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

Кафедра информационной безопасности

О Т Ч Е Т

о прохождении учебной (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практики

Выполнил студент
гр. С8118-10.05.01-1СПЕЦ
_____ Горюнов А. А.
(подпись)

Отчет защищен с оценкой

_____
_____ С.С. Зотов
(подпись) (И.О. Фамилия)
« 31 » июля 2021 г.

Руководитель практики
Старший преподаватель кафедры
информационной безопасности ШЕН
_____ С.С. Зотов
(подпись) (И.О. Фамилия)

Регистрационный № _____
« 31 » июля 2021 г.

_____ Е.В. Третьяк
(подпись) (И.О. Фамилия)

Практика пройдена в срок
с « 19 » июля 2021 г.
по « 31 » июля 2021 г.
на предприятии
Кафедра информационной безопасности ШЕН ДВФУ

г. Владивосток
2021

Содержание

Задание на практику

- Проведение исследования в области обеспечения защиты информации удалённого рабочего стола.
- Написание отчета по практике о проделанной работе.

Введение

Учебная (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практика проходила на кафедре информационной безопасности ШЕН ДВФУ в период с 19 июля 2021 года по 31 июля 2021 года.

Целью прохождения практики является приобретение практических и теоретических навыков по специальности, а также навыков оформления проведенного исследования в отчетной форме.

Задачи практики:

1. Ознакомиться с сетевым протоколом удаленного подключения RDP.
2. Ознакомиться с методами, позволяющими повысить безопасность удалённых подключений по протоколу RDP.
3. На основе полученных знаний написать отчет по практике о проделанной работе.

Обеспечение защиты информации удалённого рабочего стола

Аннотация:

В статье представлены практические рекомендации и методические подходы по защите данных при удаленной работе. Проанализирована информация о различных способах настройки защищенного удаленного подключения. Приведены основные аспекты настройки VPN-клиента и удаленного рабочего стола. Проведён сравнительный анализ атак на информационную систему при подключении сетевого протокола RDP и аргументирована необходимость повышения уровня информационной защищённости при организации удалённой работы. Разработаны схемы удаленного подключения с использованием различных средства защиты.

Введение

На современном этапе информатизации общества возрастает потребность в разработке и реализации эффективных решений в сфере информационных технологий, в том числе обеспечивающих удаленную работу. Рост числа угроз информационной безопасности и предпринятых атак со стороны потенциальных злоумышленников вызывает серьезную озабоченность для владельцев и пользователей конфиденциальной информации. В связи с этим задача обеспечения защиты информации при осуществлении удаленной работы сотрудников в современных условиях рынка информатизации имеет важное значение.

При осуществлении удаленного доступа необходимо обеспечить защиту информационных активов компании. Обеспечение конфиденциальности и целостности информации при удаленной работе сотрудников явилось для учреждений одной из главных задач. Основными способами усиления безопасности стали настройка шифрования и аутентификация пользователей на уровне сети.

В своих работах специалисты Иркутского государственного университета путей сообщения А.А. Бутин, Н. И. Глухов и др. акцентируют внимание на возрастающие угрозы информационной безопасности при удаленной работе и дают свои рекомендации по повышению уровня защиты информации. Важным шагом в построении защиты авторы считают настройку двухфакторной аутентификации в электронной почте, мессенджерах и при удаленном доступе, а также советуют использовать корпоративную технику. Помимо этого, специалисты предлагают альтернативные решения для усиления защиты: использование DLP-систем.

Специалисты компании Мультифактор предлагают свой способ защищенного подключения к удаленному рабочему столу без использования VPN-клиента. В их варианте используется RemoteDekstop Gateway (далее по

тексту – RD Gateway) для создания защищенного шлюза и Multifactor Radius Adapter для проведения двойной аутентификации.

Авторы с известного в России сайта habr.com. уже настаивают на использовании VPN-клиентов для создания защищенного подключения. Среди плюсов данных программ выделяют их многофункциональность, так как помимо непосредственного создания защищенного канала, они также выполняют аутентификацию, идентификацию пользователя, проверку сертификатов безопасности.

Сетевой протокол удаленного подключения RDP

Многие исследования доказывают, что на сегодняшний день самой популярной операционной системой является Windows. Согласно данным Statcounter данная ОС установлена почти на 77% компьютеров. В связи с этим, самым используемым сетевым протоколом подключения является RDP (RemoteDekstopProtocol – протокол удалённого рабочего стола). При организации удаленной работы необходимо помнить про такой важный аспект, как защита конфиденциальной информации. Сохранность данных является актуальной задачей для каждой крупной компании. Распространение, хищение, удаление и прочие вмешательства в важную информацию могут нанести компании как материальный, так и репутационный ущерб. До пандемии сотрудники компании работали в пределах локальной сети компании и контролировать процессы обмена данных было проще. Теперь же все работники, находясь в собственных квартирах и домах, подключаются к корпоративным серверам через глобальную сеть. Именно поэтому необходимо разработать дополнительный перечень защитных мер, учитывающих новые условия организации работы компании.

Способ подключения к удалённому рабочему столу

Способ заключается в следующем:

1. Через меню «Параметры» находим пункт «Система» -> находим функцию «Удаленный рабочий стол» и устанавливаем флаг «Включить удаленный рабочий стол» в положение «Вкл.»;

2. Добавить в группу «Пользователи удаленного рабочего стола» перечень учетных записей, которые имеют право подключаться к данному компьютеру.

3. Подключить пользователя к удаленному рабочему столу с помощью одного из доступных методов: поиск в системе (в строке поиска ввести «Подключение к удаленному рабочему столу»/mstsc);

через диалоговое окно «Выполнить» (ввести в строку mstsc и в результате откроется окно клиента подключения к удаленному рабочему столу); через меню «Пуск» найти в стандартных утилитах «Подключение к удаленному рабочему столу и тд.

Однако, как показывает практика, стандартное подключение по данному протоколу является небезопасным. Согласно исследованиям специалистов компании «CheckPoint», работающей в сфере IT-безопасности, в ходе исследования безопасности данного протокола выявили 25 уязвимостей, среди которых были и критические. Помимо этого, аналитики «Лаборатории Касперского» сравнили количество RDP-атак с января по ноябрь в 2019 и 2020 годах и пришли к выводу, что количество атак увеличилось в 3,4 раза (см. рис.1). Данный факт связан с массовым переходом сотрудников различных компаний на удаленный режим работы: число подключений по RDP значительно увеличилось, чем и поспешили воспользоваться злоумышленники

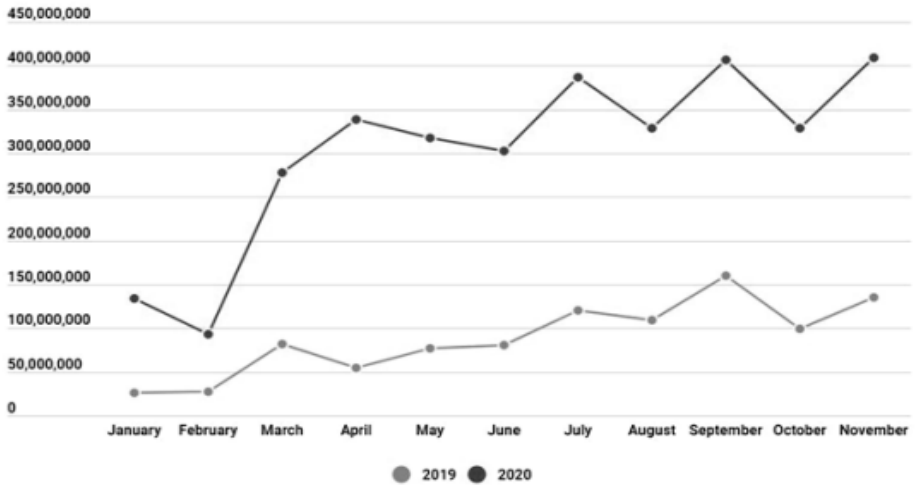

Рис.1 – Сравнительный график RDP-атак в 2019 и 2020 годах

С другой стороны, долгое существование данного протокола и постоянные обновления от компании Microsoft делают протокол RDP более защищенным, чем любые другие решения для удаленного доступа. Помимо этого, существует ряд действий, позволяющих повысить безопасность удаленных подключений по методу RDP.

Ряд методов, повышающих безопасность удаленных подключений по RDP

Во-первых, с помощью редактора локальной групповой политики можно установить шифрование данных. Для этого необходимо в редакторе локальной групповой политики выбрать компоненту Конфигурация компьютера – Административные шаблоны – Компоненты Windows – Службы удаленных рабочих столов – Безопасность – Требовать использования специального

уровня безопасности для удаленных подключений по методу RDP, установить значение «Включено» и выбрать уровень безопасности – SSL (TLS1.0). Далее необходимо настроить алгоритм шифрования. Для этого в той же «ветке» необходимо выбрать параметр «Установить уровень шифрования для клиентских подключений», установить уровень «Высокий» (включится 128-битное шифрование). Также при желании можно настроить через параметр системная криптография уровень шифрования FIPS140-1. Финальным шагом необходимо в «ветке» Конфигурация компьютера – Административные шаблоны – Компоненты Windows – Службы удаленных рабочих столов – Безопасность включить параметр «Требовать безопасное RPC-подключение» для требования подключающимся клиентам обязательного шифрования согласно настроенным установкам.

Во-вторых, для минимизации DDoS-атак необходимо настроить аутентификацию пользователя на уровне сети («ветка» Конфигурация компьютера – Административные шаблоны – Компоненты Windows– Службы удаленных рабочих столов – Безопасность, параметр «Требовать проверку подлинности на уровне сети»). Также стоит включить параметр «Учетные записи», разрешить использование пустых паролей только при консольном входе» («ветка Конфигурация компьютера – Административные шаблоны – Компоненты Windows– Службы удаленных рабочих столов – Безопасность) и настроить список пользователей, которые могут подключаться по RDP.

Помимо этого есть свободно распространяющееся программное обеспечение –IPBan. Приложение проверено и работает во всех версиях Windows, начиная с WindowsServer 2008. Алгоритм работы данного приложения заключается в фиксации неудачных попыток входа в систему, и после пяти таких попыток злоумышленника подобрать пароль, блокирования его IP-адреса на 24 часа.

Второй важной компонентой для того, чтобы среда передачи данных была безопасна является виртуальная частная сеть или VirtualPrivateNetwork (далее VPN). VPN – это обобщенное название технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх другой сети. С помощью VPN возможно создать надежную и защищенную сеть на основе ненадежной (как правило – Интернет). Для использования VPN на персональном компьютере используется специальное программное обеспечение VPN-клиент. На сегодняшний день имеется несколько таких программ: CiscoAnyConnect, OpenVPN, WireGuard, ShrewSoftVPNClient(для ОС: Windows 2000, XP, Vista) и др. Данные VPN-клиенты решают сразу несколько задач защиты информации: создание VPN, аутентификация/идентификация пользователя, защищенный доступ,

оценка соответствия сертификатов и др. Стоит отметить тот факт, что RDP и VPN являются взаимодополняемыми компонентами для обеспечения более безопасного подключения. Схема подключения с одновременным использованиям средств защиты Windows и VPN-клиента изображена на рисунке 2.

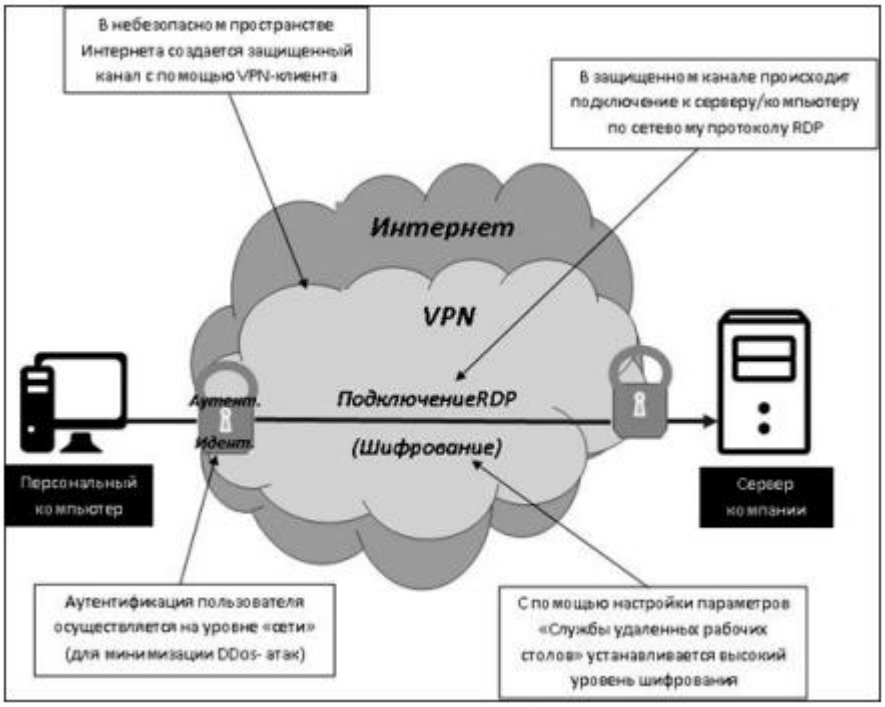

Рис.2 – Схема защищённого подключения к удалённому рабочему столу с использованием VPN-клиента.

Третьим возможным вариантов удаленного подключения (без использования VPN-клиента) является применение RD Gateway и MultiFactor Radius Adapter. RD Gateway – компонент Windows сервера, позволяющий подключаться к рабочему столу через шлюз, который выполняет функции VPN, создавая зашифрованное подключение по протоколу TLS. MultiFactor Radius Adapter – RADIUS сервер, разработанный и поддерживаемый компанией Мультифактор для двухфакторной аутентифиакции пользователей при использовании удаленного доступа. Данный компонент распространяется для Windows бесплатно. Главное преимущество такого решения в том, что не требуется развертывание VPN-сервера. На рисунке 3 приведена схема удаленного подключения с использованием двухфакторной аутентификации и RD Gateway.

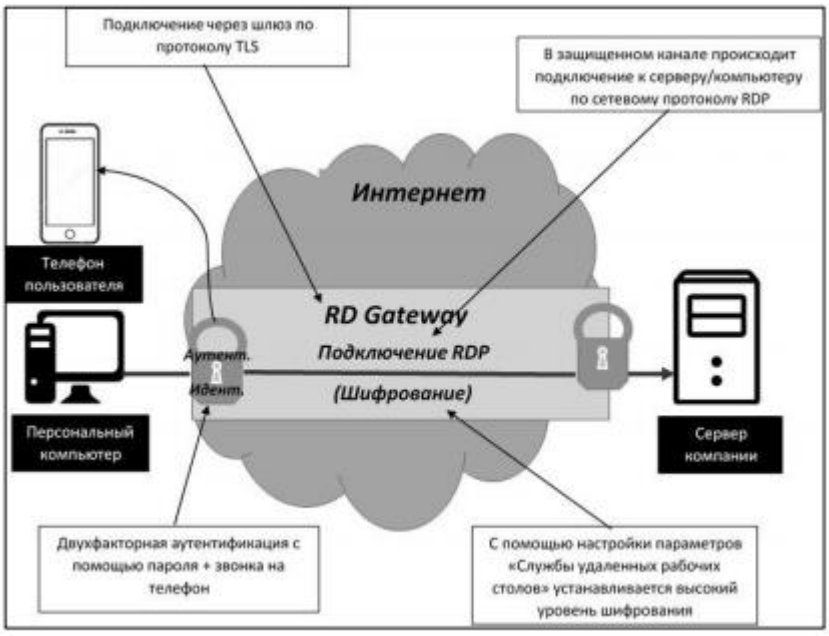

Рис.3 – Схема зищищённого подключения к удалённому рабочему столу с использованием двухфакторной аутентификации.

Заключение

Подводя итог изложенному, можно констатировать тот факт, что защита информации является важной и достижимой задачей для обеспечения удаленной работы. Хотя на сегодняшний день существует большое количество средств и методов обеспечения защиты данных при удаленном подключении, также необходимо использовать соответствующие рекомендации отечественных регуляторов по мерам обеспечения информационной безопасности: Рекомендации Банка России; Рекомендации НКЦКИ; Рекомендации ФСТЭК России.

Заключение

Для достижения данной цели, в процессе прохождения учебной (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практики ознакомился с сетевым протоколом удалённого подключения RDP, с методами повышения безопасности удалённых подключений по протоколу RDP.

Также были изучены требования к написанию отчета по практике. В результате прохождения практики был составлен отчет по практике, соответствующий предъявленным требованиям.

В ходе прохождения практики все задачи были выполнены, а цель достигнута.

Список используемых источников

1)Особенности защиты информации при удалённом доступе [Электронный ресурс]. – Электрон. дан. – Режим доступа: https://elibrary.ru/item.asp?id=45738072 (дата обращения: 17.07.2021)

2)Логинова Е.В. Обеспечение информационной безопасности коммерческого предприятия при переводе сотрудников на удаленную работу. [Электронный ресурс]. – Электрон. дан. – Режим доступа: https://www.elibrary.ru/item.asp?id=44196784 (дата обращения: 17.07.2021)

3)Афанасьева Д.В. Информационная безопасность при удаленной работе. [Электронный ресурс]. – Электрон. дан. – Режим доступа: https://www.elibrary.ru/item.asp?id=46327373 (дата обращения: 20.07.2021)

4)Remote Working Pre- and Post-COVID-19: An Analysis of New Threats and Risks to Security and Privacy ⋆ https://arxiv.org/abs/2107.03907 (дата обращения: 20.07.2021)

5)Multifactor [Электронный ресурс] – режим доступа: https://multifactor.ru/ (дата обращения: 23.07.2021)

6)Securitylab.ru [Электронный ресурс] – режим доступа: https://www.securitylab.ru/ (дата обращения: 23.07.2021)

7)Operating System Market Share Worldwide [Электронный ресурс] – режим доступа: https://gs.statcounter.com/os-market-share (дата обращения: 23.07.2021)