Презентация на тему: «Информационная безопасность при удаленной работе».

Работу выполнили студенты группы
С8118-10.05.01-1СПЕЦ
Горюнов А.А.
Чистяков Н.А.
Масленников Н.С.

План:

1) Новые угрозы и риски безопасности и конфиденциальности при удалённой работе во время пандемии.
2) Обеспечение защиты информации удалённого рабочего стола.
3) Предупреждение инцидентов информационной безопасности при удаленной работе. Предотвращение утечек данных.
4) Вывод.

Риски и угрозы безопасности

- Кибербезопасность была одной из основных проблем во время пандемии, поскольку компании спешно переходили на новые технологические платформы для удаленной работы (и удаленного доступа к корпоративным системам) и делового взаимодействия.

- Злоумышленники отслеживали различные проблемы вызванные удаленной работой, а также общей пандемией, чтобы увеличить разнообразие и количество атак.

Риски и угрозы безопасности

- Риски и уязвимости распределены по двум основным направлениям:

- *1. Риски безопасности, связанные с сотрудниками, работающими удаленно.*

- *2. Риски, связанные с технологиями, которые были использовались во время пандемии.*

Риски безопасности, связанные с сотрудниками, работающими удаленно.

- - Повышенная вероятность стать жертвой кибератаки из-за отсутствия концентрации или отвлекающих факторов, вызванных домашней работой.
- - Отсутствие обучения по вопросам безопасности удаленной работы, что приводит к неэффективным методам обеспечения безопасности.
- - Доверенные/недоверенные лица в среде удаленной работы (или в семье) могут использовать новый доступ к корпоративным данным или услугам (например, используя разблокированный ноутбук или телефон, или прослушивание конфиденциального телефонного разговора).
- - Сотрудники, которые сейчас испытывают минимальный контроль или надзор со стороны руководства могут использовать эту возможность для кражи конфиденциальной информации у своего работодателя или злоупотребления корпоративными услугами.

Риски, связанные с технологиями, которые были использовались во время пандемии.

- - Поспешное внедрение технологий в связи с национальным блокированием, что приводит к развертыванию непроверенных или ненадежных технологий.
- - Незнание (или отсутствие навыков) новых технологий удаленной работы(например, Microsoft Teams, Zoom и т.д.), что приводит к ошибкам в использовании и управлении функциями безопасности.
- - Проблемы безопасности при использовании технологий удаленной работы и удаленной связи могут подвергнуть организацию повышенному риску.
- - Преднамеренное или непреднамеренное использование рабочих устройств для решения личных вопросов, в результате чего открывает дополнительные риски для рабочих устройств.
- - Рабочие устройства могут быть украдены из дома или из среды удаленной работы.
- - Сотрудники, возвращающиеся на работу после длительного периода удаленной работы, могут принести зараженные устройства в корпоративную сеть.

Угрозы конфиденциальности персональных данных сотрудников.

- Потенциальное нарушение неприкосновенности частной жизни сотрудников, вызванное использованием работодателями технологий наблюдения/мониторинга на рабочих местах является угрозой конфиденциальности персональных данных сотрудников.
- Это может быть мониторинг нажатия клавиш, экранов и посещаемых веб-сайтов. В некоторых случаях сотрудники могут используют свои собственные технологии (смартфоны, ноутбуки) для удаленной работы, тем самым предоставляя работодателям или компаниям, доступ к огромному количеству личных данных сотрудников.

Протокол RDP

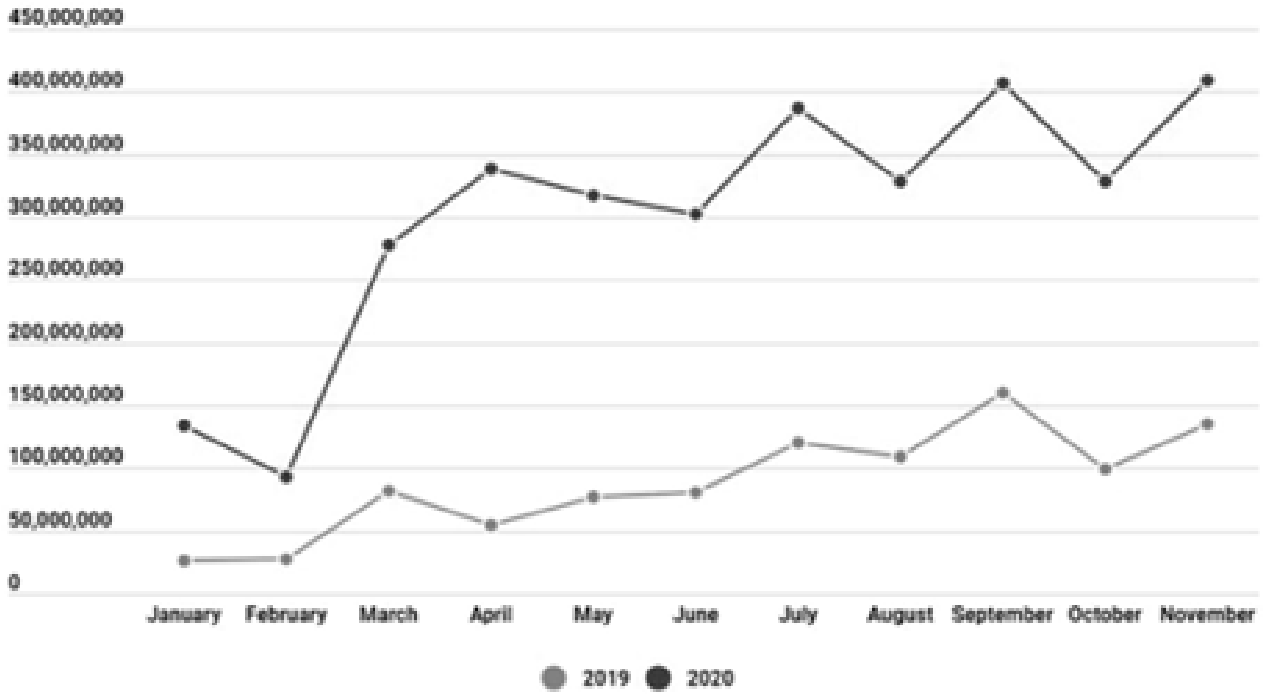


Рис.1 – Сравнительный график RDP-атак в 2019 и 2020 годах

Шифрование:

- Конфигурация компьютера – Административные шаблоны – Компоненты Windows – Службы удаленных рабочих столов – Безопасность – Требовать использования специального уровня безопасности для удаленных подключений по методу RDP(ВКЛ) – SSL. Алгоритм шифрования: «Установить уровень шифрования для клиентских подключений», установить уровень «Высокий». Финальный шаг: В этой же «ветке» - включить параметр «Требовать безопасное RPC-подключение».

Аутентификация на уровне сети:

- «Ветка» Конфигурация компьютера – Административные шаблоны – Компоненты Windows– Службы удаленных рабочих столов – Безопасность, параметр «Требовать проверку подлинности на уровне сети», а так же настроить список пользователей, которые могут подключаться по RDP (в этой же ветке).

VPN-клиент

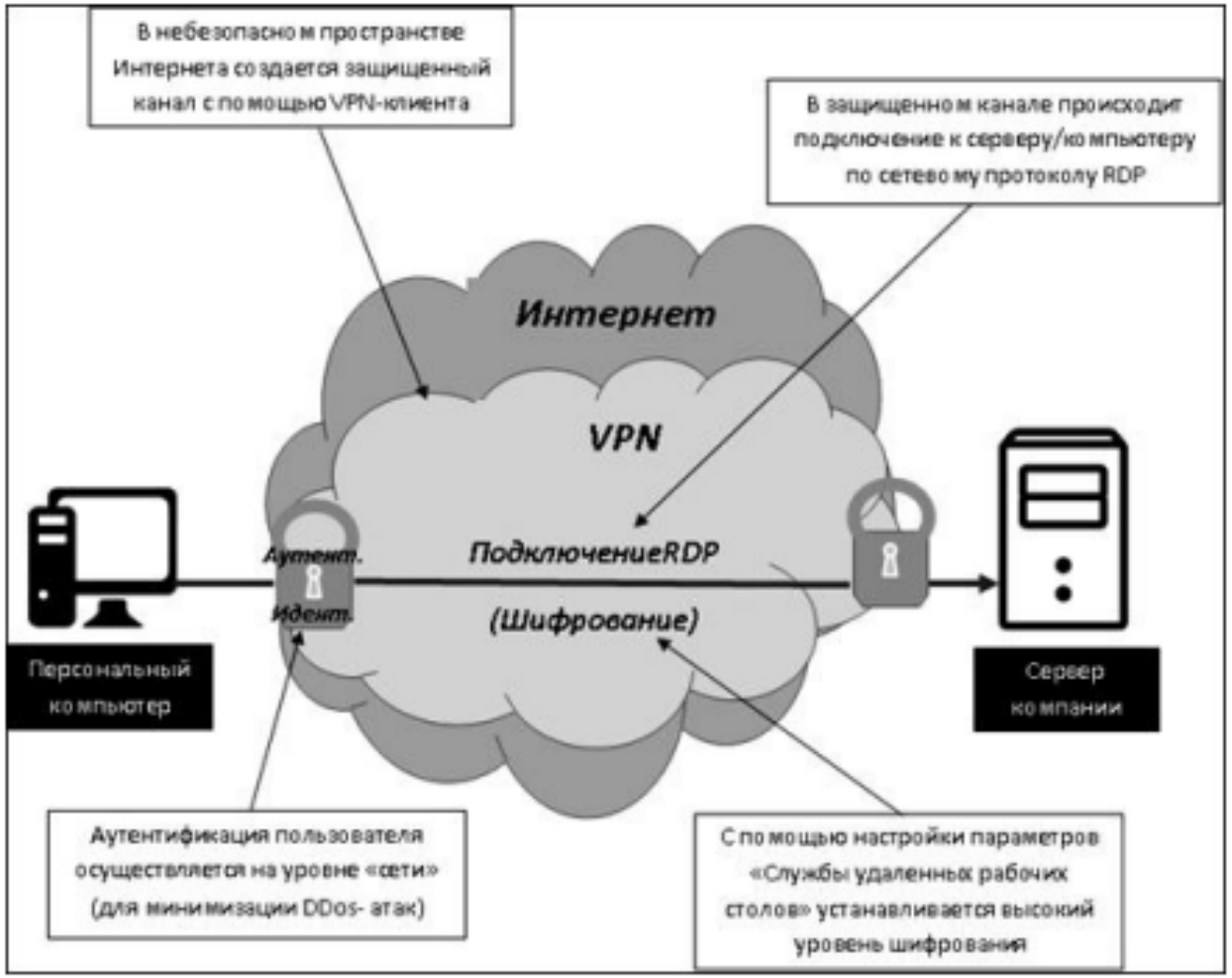


Рис.2 – Схема защищённого подключения к удалённому рабочему столу с использованием VPN-клиента.

RD Gateway и двухфакторная аутентификация

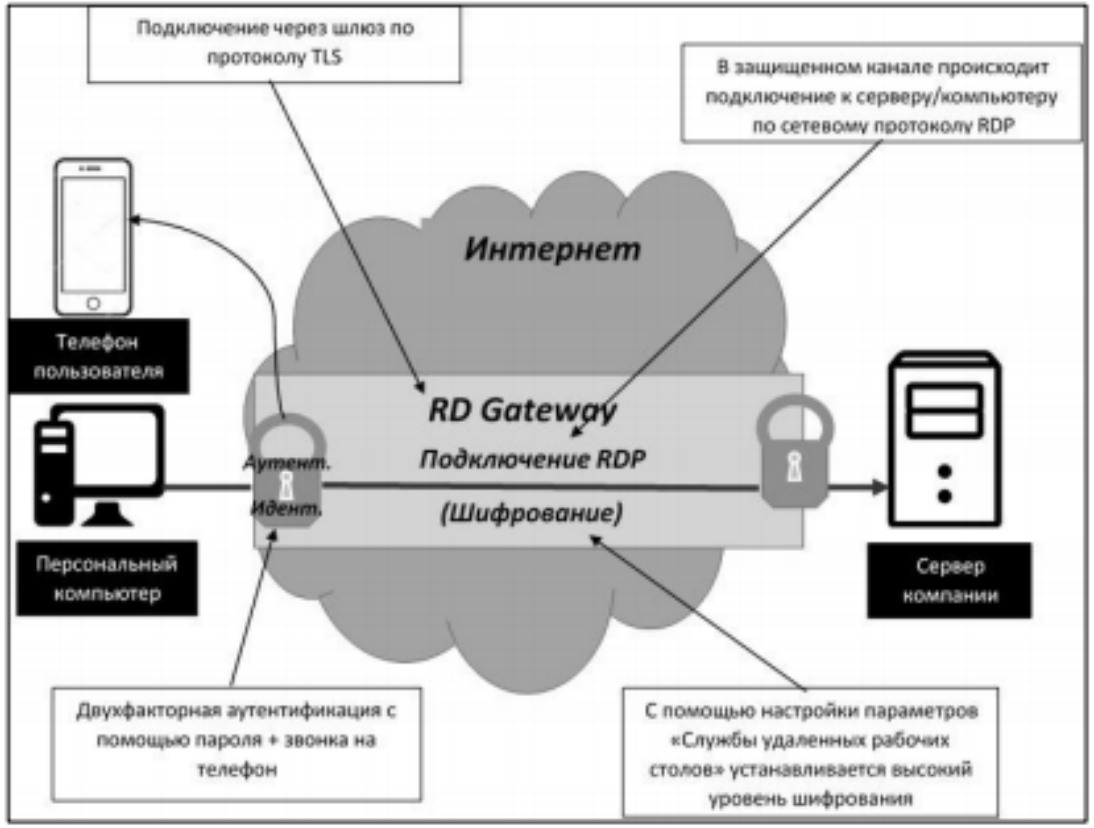
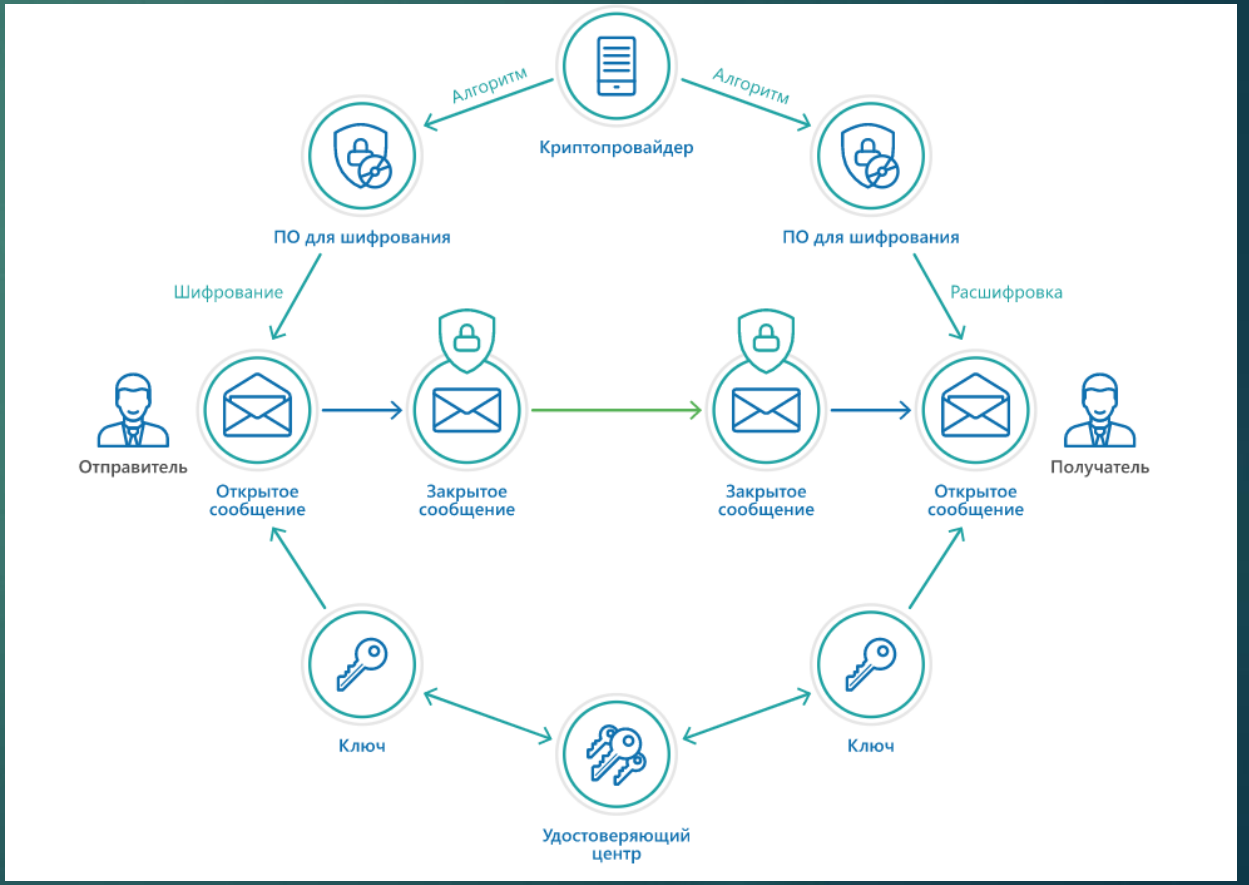


Рис.3 – Схема зищищённого подключения к удалённому рабочему столу с использованием двухфакторной аутентификации.

Способы и рекомендации для повышения информационной безопасности.

Аутентификация

СКЗИ



Облачные сервисы

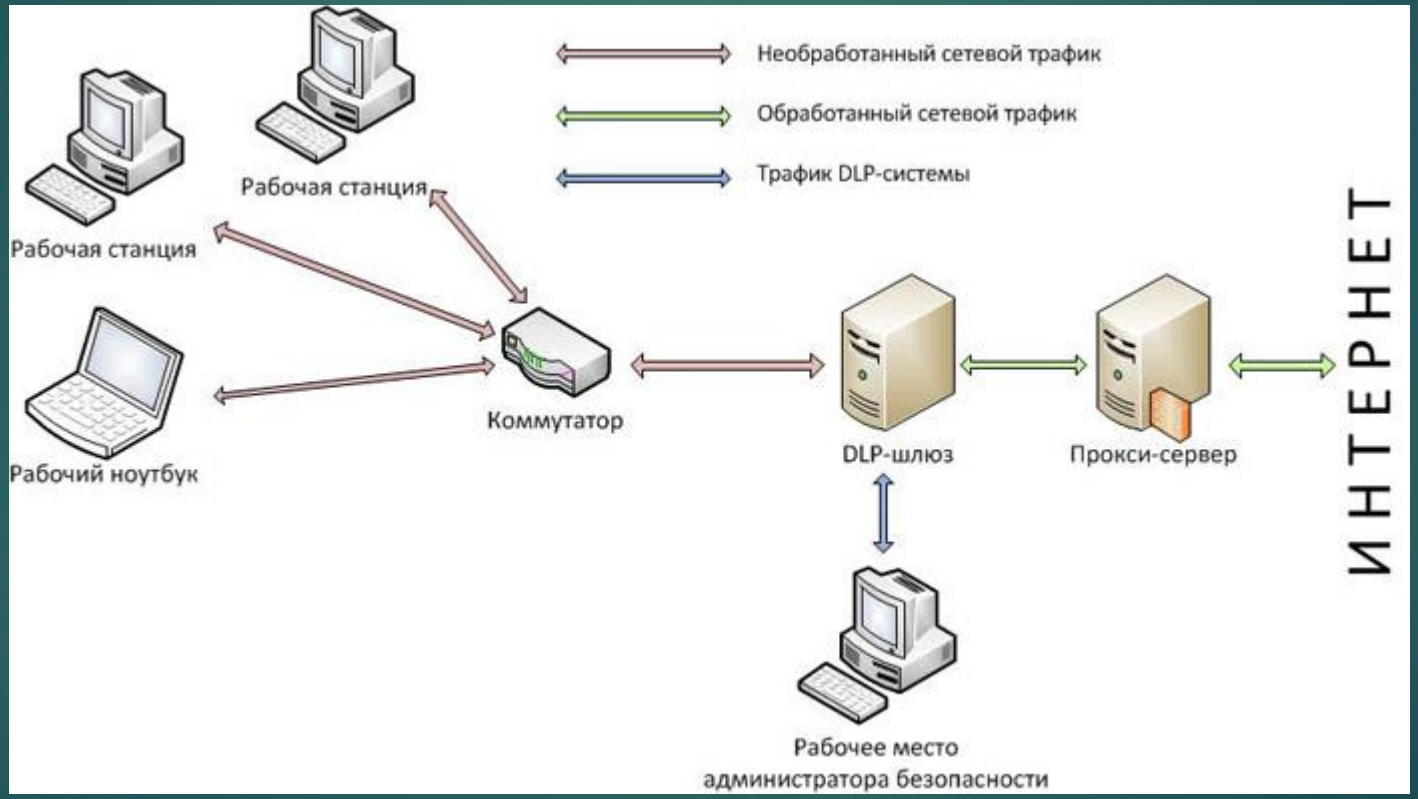
Сетевой экран

Антивирусные программы

SIEM-системы

Сквозное шифрование

DLP-системы. Защита от утечки информации.



Основными каналами утечки информации являются:

— съемные носители;

— электронная почта;

— распечатанные с компьютера документы;

— сервисы для общения.

2 способа распознавания конфиденциальной информации:

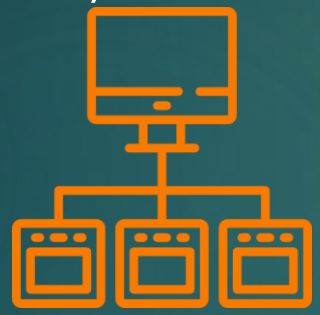
-анализ формальных признаков (хэш-значения, специальные метки и т.д.)

-анализ контента

Обычный состав DLP-системы включает:

-центр управления и мониторинга;

-модули сетевого уровня;



-компоненты уровня хоста.

Вывод:

После теоретического анализа различных статей можно сделать вывод, что вопрос о защите информации и защите от утечек конфиденциальной информации как никогда актуален. 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. Был выявлен ряд существенных рисков, поэтому необходимо, чтобы организации проверяли, соответствует ли безопасность требованиям. Важно, чтобы организации при введении нового программного обеспечения переобучали сотрудников для работы с ним и, чтобы переобучение включало навыки минимизации рисков для безопасности при работе удалённо.

Спасибо за внимание!