КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

КОД ИБ | КРАСНОЯРСК

23.03.2023

ОБО МНЕ

- Закончил Сибирский Федеральный университет по направлению «Информационная безопасность» в 2010 году
- Опыт защиты государственной тайны, персональных данных, критической информационной инфраструктуры
- Общий стаж в ИБ – 16 лет
- Люблю песни Ольги Бузовой

Организация защищенного удаленного доступа

Варианты организации удаленного доступа к инфраструктуре организации

Предоставление прямого доступа к инфраструктуре организации

Предоставление удаленного доступа к рабочим местам пользователей (RDP)

Предоставление удаленного доступа к терминальным серверам

Предоставление удаленного доступа к виртуальным рабочим местам (VDI)

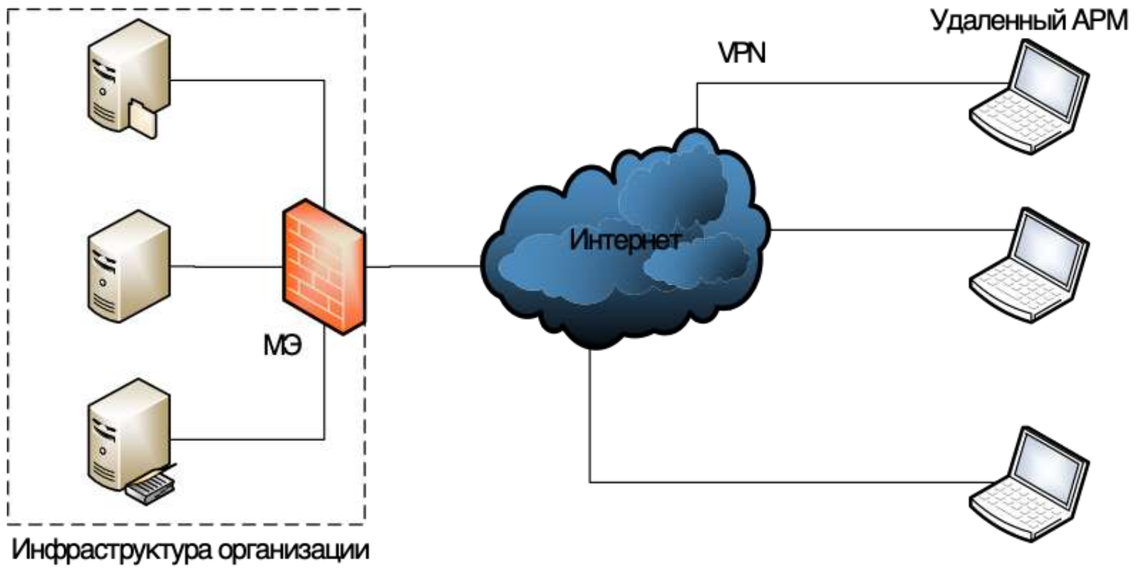
Предоставление прямого доступа к ресурсам организации

Преимущества:

- Низкая стоимость
- Простота реализации

Недостатки:

- Низкий уровень безопасности за счет прямого доступа к инфраструктуре организации
- Обработка информации на удаленном рабочем месте, что повышает вероятность утечки конфиденциальной информации
- Необходимость установки корпоративного ПО на каждое рабочее место
- Необходимость оказывать техническую поддержку на каждом удаленном АРМ



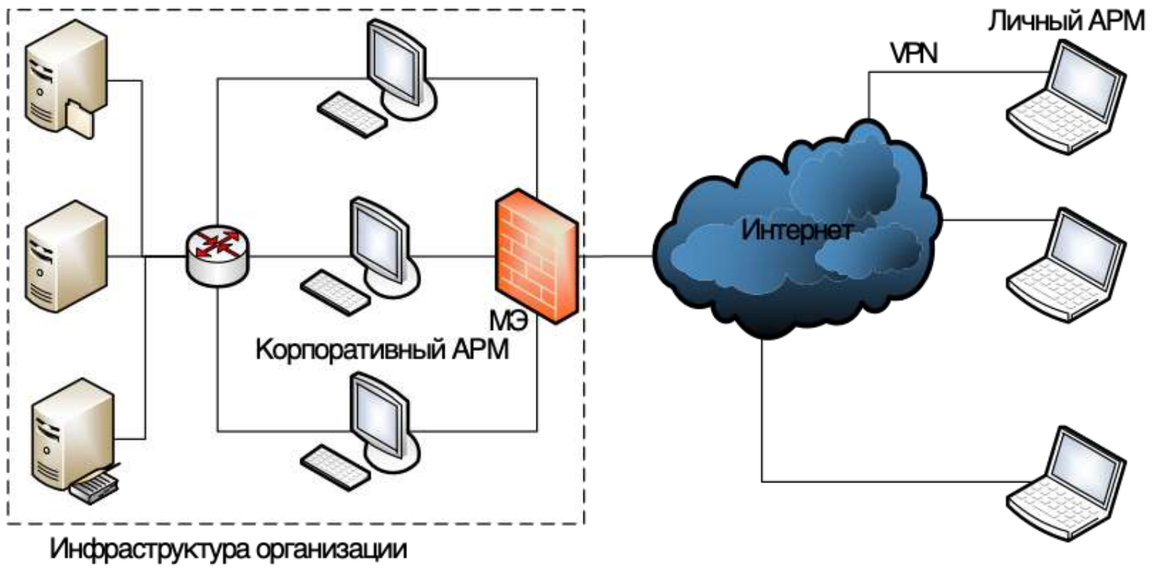
Предоставление удаленного доступа к рабочим местам пользователей (RDP)

Преимущества:

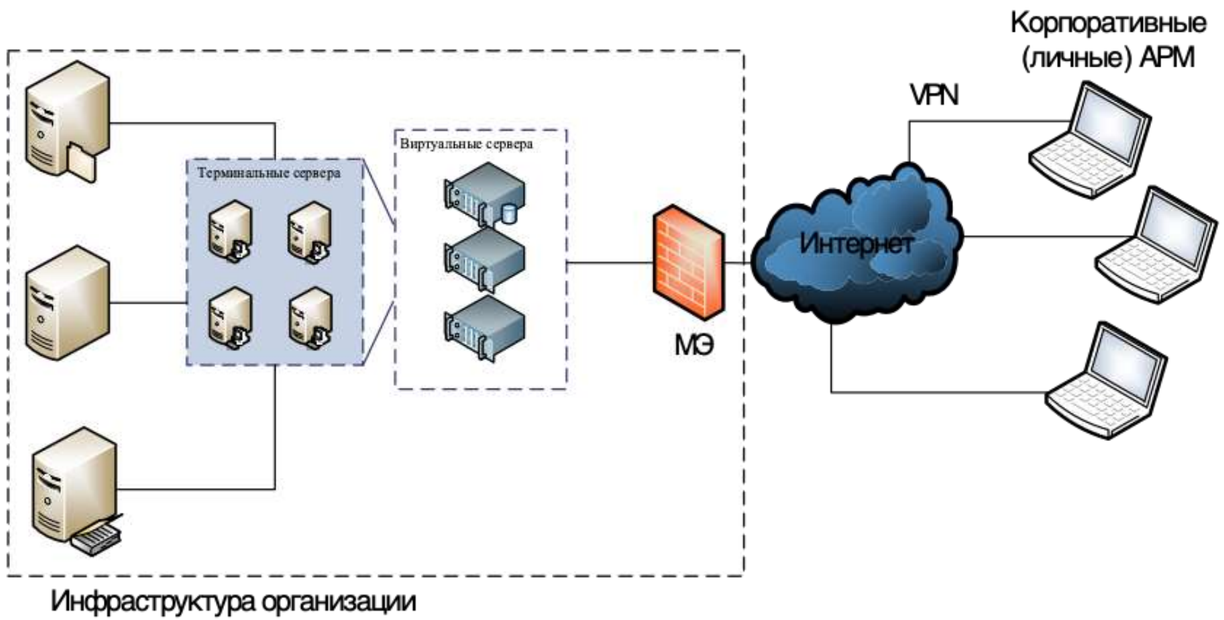
- Низкая стоимость
- Обработка информации производится с АРМ в периметре организации
- Инфраструктура организации остается без изменений

Недостатки:

- Доступ возможно организовать только с личных АРМ (иначе придется всем выдавать по два АРМ)
- Сложности реализации (необходимо каждому пользователю открыть доступ к его АРМ)
- Низкий уровень безопасности за счет подключений с личных АРМ
- Прямой доступ в инфраструктуру организации



Предоставление удаленного доступа к терминальным серверам



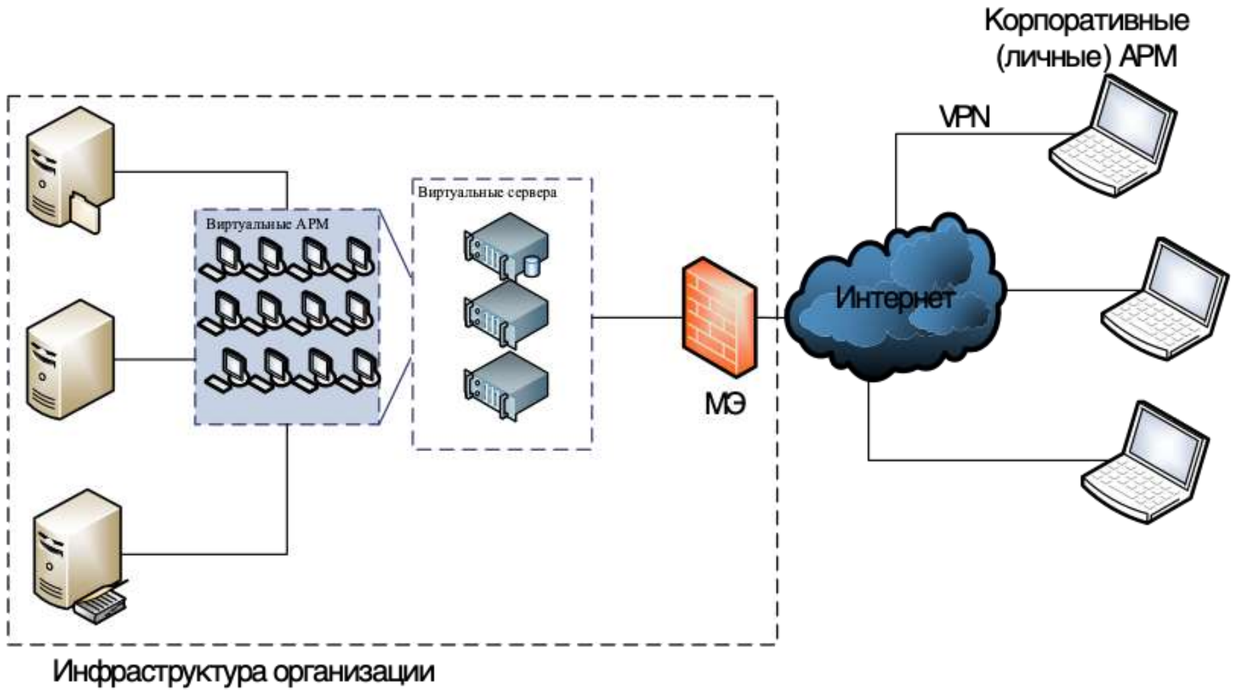
Преимущества:

- Повышенный уровень безопасности, за счет «буферной зоны» в виде терминальных серверов
- Обработка информации производится в периметре организации
- Возможно организовать DMZ для доступа извне
- Техническую поддержку необходимо оказывать на ограниченном количестве терминальных серверов

Недостатки:

- Невозможно настроить рабочее место индивидуально для каждого пользователя
- Необходимо балансировать нагрузку на каждый терминальный сервер
- Требуются достаточные серверные мощности

Предоставление удаленного доступа к виртуальным рабочим местам (VDI)



Преимущества:

- Повышенный уровень безопасности, за счет «буферной зоны» в виде виртуальных рабочих мест
- Обработка информации производится с виртуальных рабочих мест в периметре организации
- Возможно организовать DMZ для доступа извне
- Удобство технической поддержки

Недостатки:

- Высокая стоимость реализации

Основные угрозы при применении удаленного доступа

Несанкционированное проникновение (злоумышленника, вируса) в периметр организации через удаленное рабочее место

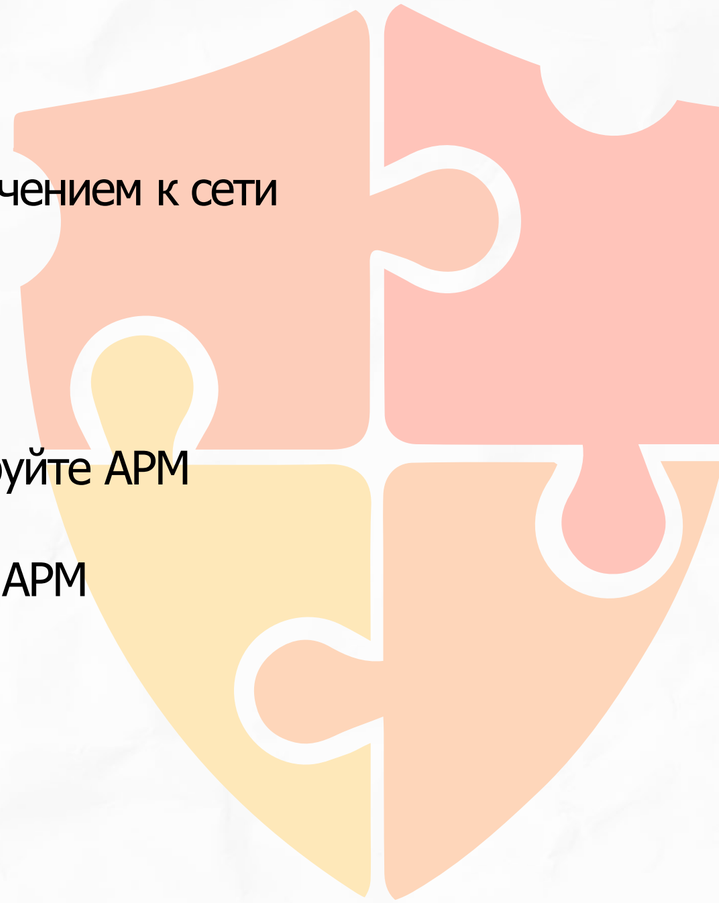
Перехват (модификация) конфиденциальной информации при передаче ее на удаленное рабочее место

Хищение конфиденциальной информации с удаленного рабочего места

Отсутствие своевременной и удобной технической поддержки удаленных рабочих мест

Рекомендации по обеспечению информационной безопасности

- Используйте варианты удаленного доступа с «буферной зоной»
- Используйте корпоративные АРМ для удаленного доступа
- Используйте средства проверки «compliance» удаленных АРМ перед подключением к сети организации
- Максимально ограничьте доступ к инфраструктуре организации с АРМ
- Запретите вывод информации на внешние носители информации, опломбируйте АРМ
- При использовании RDP запретите копирование информации на удаленный АРМ
- Ограничьте доступ с АРМ к ресурсам сети Интернет
- Размещайте терминальные сервера и виртуальные АРМ в DMZ
- Используйте доменные учетные записи на АРМ



Рекомендации по обеспечению информационной безопасности

- Используйте безопасный VPN
- Для защиты от перехвата учетной информации используйте двухфакторную аутентификацию
- При публикации ресурсов в сети Интернет используйте WAF
- Включите на межсетевом экране IPS, антивирусный контроль, SSL-inspection
- Установите клиент DLP на удаленных АРМ
- Проверьте, что у пользователя есть только пользовательские права, настроены политики безопасности, ОС обновлена
- Установите на АРМ средство антивирусной защиты, хостовый межсетевой экран с ограничением внешних подключений
- При использовании «мобильного рабочего места» используйте шифрование жесткого диска
- Установите на АРМ средство дистанционного доступа для оказания технической поддержки

Готов ответить
на ваши вопросы

E-mail: zhirakovvladimir@gmail.com