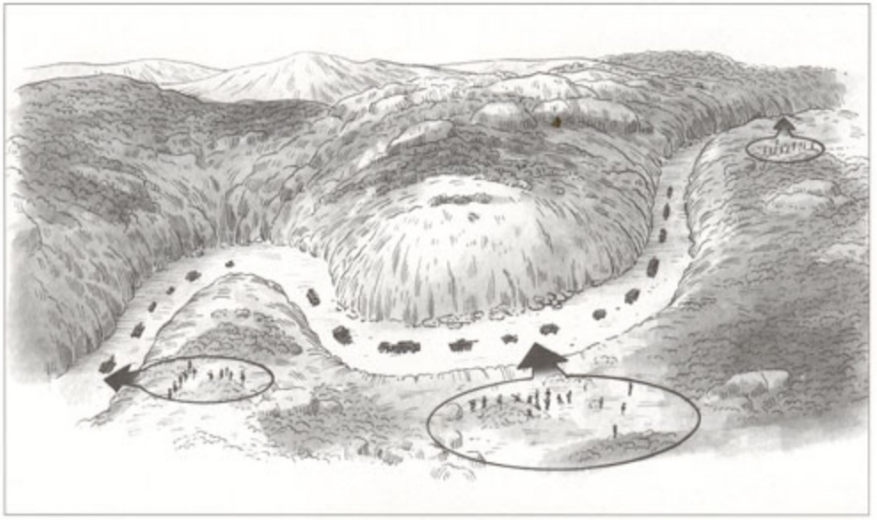
Типовые схемы удаленного доступа: архитектура и инструменты

Почему защищаться только наложенными СЗИ и ВНД не всегда эффективный подход или про ассиметричность ИБ



Злоумышленники		Защитники
1) Выбирают самые слабые места и атакуют наименее защищенные активы и конфигурации	VS	1) Вынуждены защищать всю инфраструктуру 24x7, быть всегда «на чеку»
2) Выбирают наиболее подходящее для атаки время		2) Не имеют плана защиты от всех возможных атак, могут только строить гипотезы
3) Имеют подготовленный план для своей атаки, включая инструменты		3) Ограничены человеческим и финансовым ресурсом; выполняют множество операционных задач не всегда напрямую связанных с ИБ
4) Имеют достаточный человеческий ресурс для проведения атаки		4) Находятся под грузом ответственности за безопасность своей инфраструктуры
5) Ничем особенно не рискуют, если атака не будет успешной		

Как максимально усложнить атаку на ИТ-инфраструктуру и сделать ее непривлекательной для злоумышленников?

1) **Только с помощью СЗИ все не защитить, надо харденить свою ИТ-инфраструктуру и прорабатывать ее архитектуру (желательно до внедрения в продуктив)**

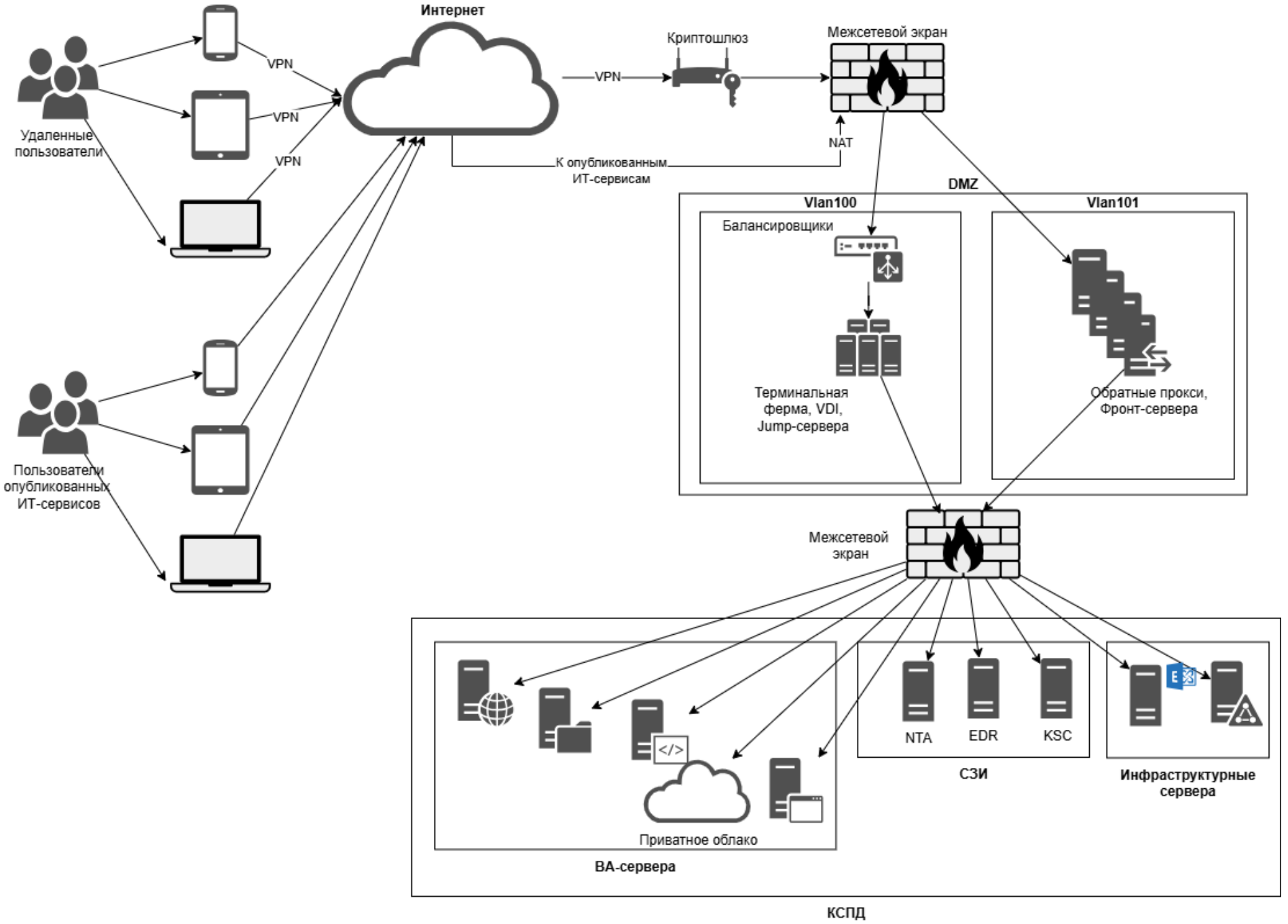
2) **Учитывать best practice, рекомендации и технологии вендоров в части безопасности архитектуры внедряемых решений. Любую, даже самую безопасную инфраструктуру можно сделать «дырявой», если внедрять неправильные архитектуры с неправильными настройками**

3) **Сделать акцент на технической невозможности эксплуатации уязвимостей и конфигураций, либо на эшелонированной, многоступенчатой защите, в том числе jump servers, dmz и т.п.**

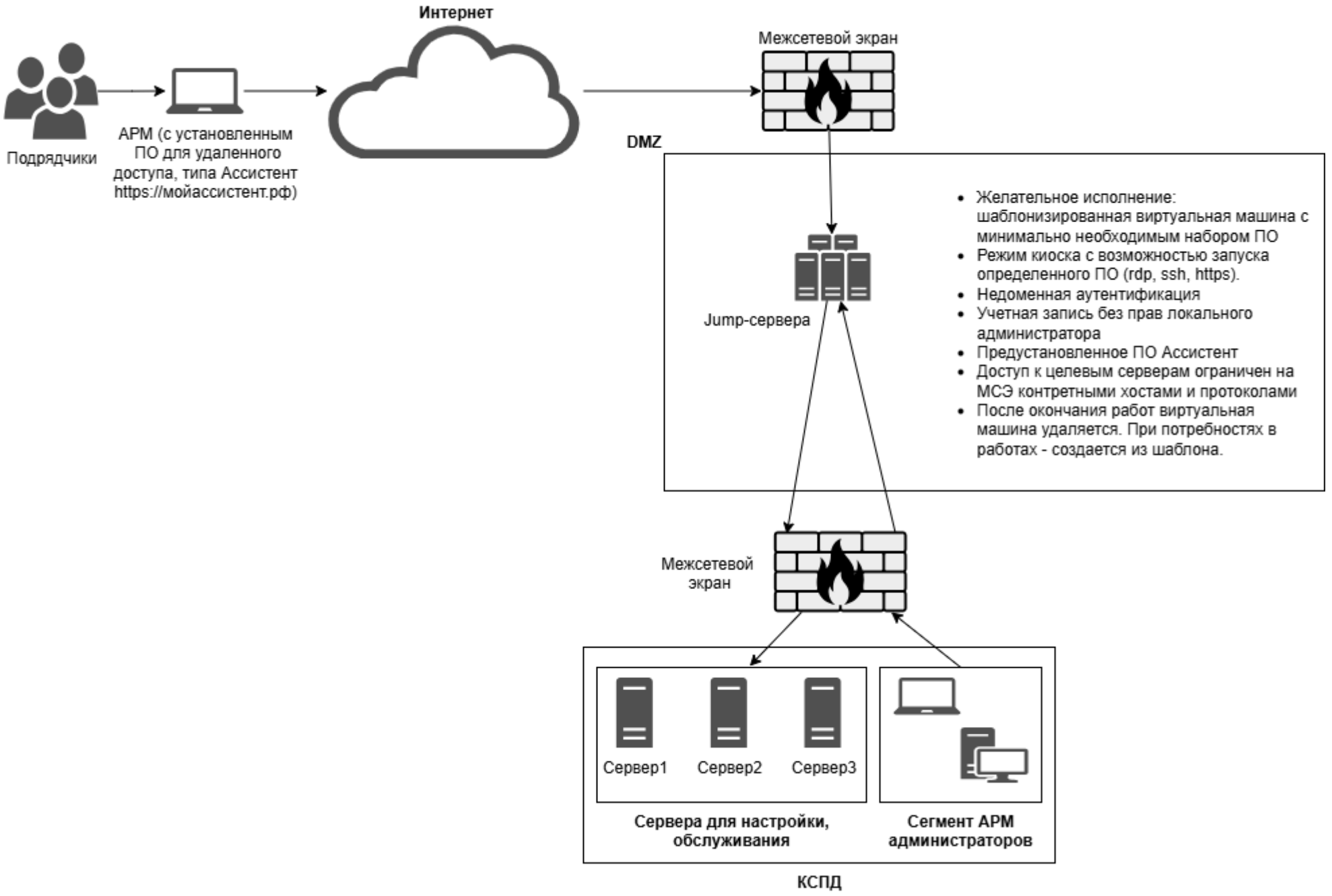
4) **Доступы к тестовым инфраструктурам и их элементам, включая учетные записи нужно ограничивать по времени пилота или выполнения работ, с автоматическим выключением или деактивацией по окончании этого периода. Как минимум, по таким компонентам должен быть определен ответственный и настроено автоматическое оповещение. К примеру, с помощью установки периода работы правил на межсетевом экране через планировщик или срока действия учетных записей в Active Directory.**

Для реализации такого подхода не нужно много ИБ-специалистов. На среднюю компанию достаточно несколько хороших ИБ-специалистов с задатками архитектора и ИТ-специалисты, с которыми дела на рынке обстоят намного получше.

Типовая схема удаленного доступа

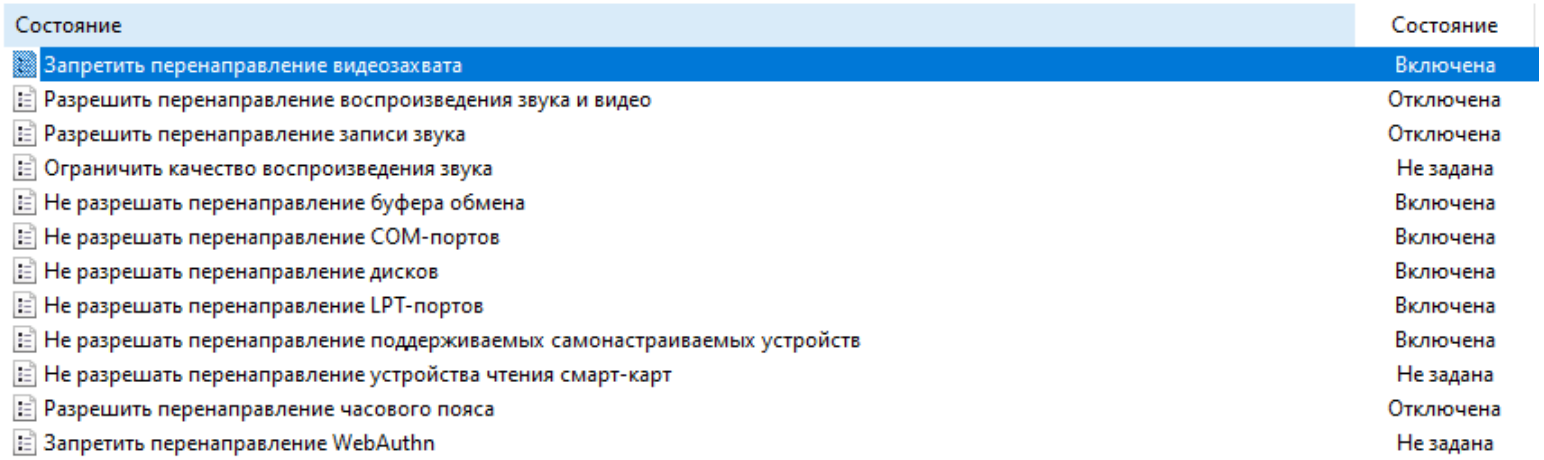


Типовая схема удаленного доступа(для подрядчиков)



Настройка терминальной фермы для удаленного доступа

1) **Настройка параметров групповых политик для терминальной фермы (раздел GPO Конфигурация компьютера -> Политики -> Административные шаблоны -> Компоненты Windows -> Службы удаленных рабочих столов) :**
   - **Клиент подключения к удаленному рабочему столу**
     - **Запретить сохранение паролей - включено**
     - **Запрашивать учетные данные на клиентском компьютере - включено**
   - **Узел сеансов удаленных рабочих столов -> Безопасность**
     - **Всегда запрашивать пароль при подключении - включено**
   - **Узел сеансов удаленных рабочих столов -> Ограничение сеансов по времени**
     - **Задать ограничение по времени для активных, но бездействующих сеансов служб удаленных рабочих столов - к примеру, 2 часа**
     - **Завершать сеанс при достижении ограничения по времени - включено**
   - **Узел сеансов удаленных рабочих столов -> Перенаправление принтеров**
     - **Не разрешать перенаправление для клиентского принтера - включено**
   - **Узел сеансов удаленных рабочих столов -> Перенаправление узлов и ресурсов**



Состояние	Состояние
Запретить перенаправление видеозахвата	Включена
Разрешить перенаправление воспроизведения звука и видео	Отключена
Разрешить перенаправление записи звука	Отключена
Ограничить качество воспроизведения звука	Не задана
Не разрешать перенаправление буфера обмена	Включена
Не разрешать перенаправление COM-портов	Включена
Не разрешать перенаправление дисков	Включена
Не разрешать перенаправление LPT-портов	Включена
Не разрешать перенаправление поддерживаемых самонастраиваемых устройств	Включена
Не разрешать перенаправление устройства чтения смарт-карт	Не задана
Разрешить перенаправление часового пояса	Отключена
Запретить перенаправление WebAuthn	Не задана

   - **Узел сеансов удаленных рабочих столов -> Подключения**
     - **Ограничить пользователей служб удаленных рабочих столов одним сеансом служб удаленных рабочих столов - включено**

Настройка терминальной фермы для удаленного доступа

2) **Настройка Software Restriction Policies (SRP). Пример https://winitpro.ru/index.php/2016/10/21/blokirovka-virusov-i-shifrovalshhikov-s-pomoshhyu-software-restriction-policies/.**

   Обратите отдельное внимание на типы файлов в разделе *Designated File Types*: в типах файлов есть ярлыки, которые нужно исключить из проверки, иначе пользователи не смогут их запускать.

   Требует предварительного тестирования и отладки, но с «лихвой» окупает временные затраты.

3) **Подготовка типовых конфигураций для групп терминальных серверов (бизнес-пользователи, администраторы ИТ-инфраструктуры, разработчики ИС)**

   - **Определение и установка необходимого набора ПО, выключение не требуемых компонентов ОС**
   - **Создание групп безопасности для каждой группы терминальных серверов и предоставление им доступа на конкретные терминальные сервера**
   - **Установка для всех, кроме администраторов терминальной фермы прав обычного пользователя**
   - **Настройка сетевых доступов на МСЭ для каждой группы терминальных серверов**
   - **Если пользователю требуется специализированное ПО, которое больше никому не требуется — лучше рассмотреть вариант с VDI или сделать выделенную виртуальную машину с персональным доступом, пользовательской ОС и требуемым набором ПО**

Настройка пользовательской техники для удаленного доступа

1) **Установка типового образа ОС, минимально необходимого набора ПО, отключение не требуемых компонентов Windows, установка сложного пароля, соответствующего требованиям парольной политики или лучше автоматически сгенерированного в соответствии с параметрами сложности.**
2) **Настройка режима киоска с запуском нескольких приложений**
   - **Windows:**

     https://learn.microsoft.com/ru-ru/windows/configuration/assigned-access/configure-multi-app-kiosk?tabs=ps

     https://winitpro.ru/index.php/2024/05/21/vkluchit-rezhim-kioska-windows/
   - **Linux:**

     https://wiki.astralinux.ru/pages/viewpage.action?pageId=67108883

     https://marukhin.ru/2024/02/22/graphical-kiosk-astra-linux/
3) **Настройка Software Restriction Policies (SRP) в Windows аналогично настройке на серверах терминальной фермы, если не устраивает режим киоска или в дополнение к нему**
4) **Включение шифрования Bitlocker для Windows, VeraCrypt или аналоги для Linux. Настройка с использованием VeraCrypt https://habr.com/ru/articles/558254/ или https://1cloud.ru/help/security/nastroika-diska-veracrypt.**
5) **Включение пароля на доступ к жесткому диску. Защита снимается сбросом BIOS, но на ноутбуках это более проблематично, чем на стационарных компьютерах.**
6) **Использование иммутабельных ОС. https://www.linux.org.ru/articles/desktop/17444828/page2**
7) **Использование тонких клиентов. Один из примеров, https://getmobit.ru/gm-box-g1-ru.**
8) **Использование MFA (при наличии бюджета).**

Настройка jump-серверов для удаленного доступа подрядчиков

1) **Настройка режима киоска с запуском нескольких приложений**
2) **Настройка Software Restriction Policies (SRP) в Windows аналогично настройке на серверах терминальной фермы, если не устраивает режим киоска или в дополнение к нему**

СПАСИБО ЗА ВНИМАНИЕ!

И помните, наша победа, как всегда, неизбежна!