

# ЧЕК-ЛИСТ: КАК НАСТРОИТЬ КОРПОРАТИВНЫЕ ПРОЦЕССЫ И СЕРВИСЫ, ПРЕЖДЕ ЧЕМ ОТПУСТИТЬ ЛЮДЕЙ РАБОТАТЬ УДАЛЕННО

1. **Настройте соединение с внутренними сервисами по VPN-каналу, защищенному двухфакторной аутентификацией.**
2. **Проверьте, чтобы рабочие сервисы были доступны вне офиса и оцените пропускную ширину каналов интернета и резервных каналов связи.**
3. **Установите систему мониторинга работоспособности сервисов.**  
Программа нужна для оперативного оповещения ИТ-службы о нарушениях в работе сервисов.
4. **Обеспечьте дистанционную работу:**
  - А) **на корпоративном ПК:**
    - Введите запрет на доступ сотрудника к BIOS корпоративного ноутбука, чтобы он не мог загрузить операционную систему с флешки.
    - Включите шифрование дисков (Windows BitLocker или аналоги) на выносимых за пределы офиса компьютерах. И настройте бэкап в корпоративное облако.
  - Б) **на личном ПК:**
    - Проверьте, установлены ли обновления ОС, программ; работает ли в штатном режиме антивирусный пакет, проведена ли проверка на вирусы и вредоносное ПО.
    - Настройте терминальный доступ.
    - Настройте двухфакторную авторизацию к терминальному доступу.
5. **Измените настройки DLP-системы для работы с удаленными пользователями.**
  - Проверьте, чтобы на всех корпоративных устройствах был установлен агент DLP.
  - Настройте его на работу в удаленном режиме: добавьте альтернативные адреса серверов DLP, настройте правила перенаправления трафика на межсетевом экране.
  - Оптимизируйте настройки агентов под ширину и загрузку каналов связи.
  - Проведите аудит настроек агента: при необходимости запретите использование буфера обмена, заблокируйте переносные устройства.