

# Удалённая работа для ИБ. Плюсы и минусы.

Докладчик: Богданов Денис Викторович  
Независимый эксперт в области информационной безопасности

# Плюсы? Для кого?



# Минусы. Новые риски.

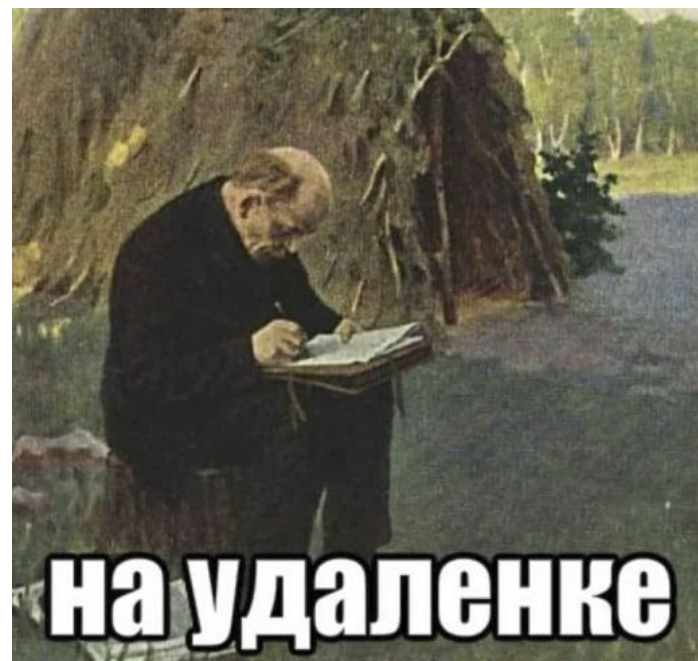
При удалённом подключении к своему рабочему ПК стоит помнить не только об обеспечении мер информационной безопасности на рабочем ПК, но и на тех устройствах, с которых вы осуществляете удалённый доступ к корпоративным ресурсам.

В этом вам помогут следующие меры:

- Использование лицензионного ПО;
- Наличие антивирусного ПО с актуальными антивирусными базами;
- Установка всех актуальных обновлений для операционной системы;
- Обновление ПО роутера и установка сложного пароля для доступа к нему. Инструкции по обновлению вы можете найти во вложении;
- Разделение учётных записей пользователей на одном ПК;
- Использование межсетевого экрана (брандмауэра или фаервола);
- Ограничение использования функции сохранения паролей в браузерах и иных консолях;
- Включение автоматической блокировки ПК в случае, если пользователь неактивен в течение длительного времени.

# Что должно быть запрещено:

- Хранить информацию ограниченного доступа на домашнем ПК и иных устройствах, не относящихся к корпоративным;
- Допускать к устройству третьих лиц во время запущенной сессии удалённого подключения;
- Использовать общественные Wi-Fi сети и иные незнакомые сети для подключения удалённого доступа;
- Сохранять скриншоты с рабочей информацией в открытом доступе, либо на личном устройстве;
- По завершении работы оставлять запущенную сессию удалённого подключения.



## Прочие рекомендации:

- Настоятельно рекомендуется использование двухфакторной аутентификации при организации безопасного соединения работника до своего рабочего ПК.
- Для обеспечения коммуникации с коллегами и партнерами Компании при установке корпоративных мессенджеров на домашний ПК или мобильные устройства iOS/Android стоит помнить о том, что дистрибутивы (установочные файлы) программ необходимо скачивать только с официальных ресурсов их производителей.
- В целях обеспечения безопасной работы с домашнего ПК и иных устройств, с которых осуществляется удалённый доступ к корпоративным ресурсам, настоятельно рекомендуем использовать антивирусное ПО крупных поставщиков данного софта. Практически у каждого поставщика антивирусного софта есть бесплатные версии ПО, которые могут обеспечить базовый уровень защиты домашних устройств. Также, поставщики софта предоставляют временную возможность использования пробных версий (trial version) данных продуктов. В настройках антивирусного ПО должна быть включена функция ежедневного обновления антивирусных баз.

## Прочие рекомендации:

- В целях обеспечения безопасности домашней сети с использованием Wi-Fi-роутера рекомендуется регулярно менять пароли для Wi-Fi и консоли администратора, а также обновить прошивку устройства.
- Если вам выдаётся сертификат для удалённого подключения, то всегда используйте его, а не авторизацию формата логин и пароль.
- Если домашним компьютером, с которого вы подключаетесь к рабочему, пользуются и другие члены семьи, необходимо создать для них отдельные учётные записи (или же создать одну отдельную УЗ под работу).



Спасибо за внимание!

