

Как бизнесу выжить в цифровом концлагере после карантина

Павел Миловидов

Специалист по защите информации
с 15-летним опытом. Руководитель
ИТ-компании «Безопасный Офис»

Цифровая безопасность
для тех, кому нечего
скрывать

1. Сдача отчетности с разных ip-адресов
2. Шифрованные мессенджеры и VPN
3. Анонимная почта на зарубежных серверах
4. Свой сервер в секретном месте
5. Прослушка телефонов
6. Вдруг вы сами нас сдадите?
7. Какие гарантии, что информация не пропадет?

1. Сдача отчетности с разных ip-адресов
2. Шифрованные мессенджеры и VPN
3. Анонимная почта на зарубежных серверах
4. Свой сервер в секретном месте
5. Прослушка телефонов
6. Вдруг вы сами нас сдадите?
7. Какие гарантии, что информация не пропадет?

Как организовать удаленку, чтобы чужаки не добрались до вашей информации

Удаленные рабочие места можно организовать пятью разными способами:

1. Свой сервер в офисе
2. Свой сервер в чужом помещении
3. Свой сервер в дата-центре
4. Арендванный сервер в дата-центре
5. Арендванные облачные рабочие места

Свой сервер выглядит надежнее, но на самом деле это не так. Как раз безопаснее именно арендовать готовые рабочие места:

	Свой сервер в офисе	Свой сервер в чужом помещении	Свой сервер в дата-центре	Аренда сервера в дата-центре	Аренда облачных рабоч. мест
Разовые вложения	200..500 тыс	200..500 тыс	200..500 тыс	-	-
Ежегодные вложения (амортизация, модерниз.)	50..100 тыс	50..100 тыс	50..100 тыс	-	-
Ежемесячные расходы	-	-	5-15 тыс	15-30 тыс	10-50 тыс
Требуется свой админ, имеет доступ ко всему	+	+	+	+	-
Риск поломки или технического сбоя	высокий	высокий	высокий	средний	низкий
Время восстановления после поломки	~ неделя	~ неделя	~ неделя	~ дни	без остановки
Риск потери данных за последний период	высокий	высокий	высокий	средний	-
Риск простоя из-за электричества или интернета	средний	высокий	низкий	низкий	низкий
Риск изъятия или кражи	высокий	средний	средний	-	-
Риск несанкционированного доступа изнутри	высокий	высокий	средний	средний	низкий
Риск несанкционированного доступа извне	высокий	средний	низкий	низкий	низкий

В чем отличие от бухгалтерий...

1. Сдача отчетности с разных ip-адресов
2. Шифрованные мессенджеры и VPN
3. Анонимная почта на зарубежных серверах
4. Свой сервер в секретном месте
5. Прослушка телефонов
6. Вдруг вы сами нас сдадите?
7. Какие гарантии, что информация не пропадет?

1. Сдача отчетности с разных ip-адресов
2. Шифрованные мессенджеры и VPN
3. Анонимная почта на зарубежных серверах
4. Свой сервер в секретном месте
5. Прослушка телефонов
6. Вдруг вы сами нас сдадите?
7. Какие гарантии, что информация не пропадет?

"Бесшовный" переезд офиса на удаленку

1 день

- установить офисное и специальное ПО
- Настроить антивирусную защиту
- Ограничить права пользователей
- Развернуть виртуальные рабочие столы
- Настроить резервирование
- Временно отключить буфер обмена
- На почту выслать инструкции
- Разослать сотрудникам доступ
- Объяснить 2 дня на перенос личных файлов

2 день

- Если в режиме "только" клиента - то поставить на удаленку клиентское приложение
- Если в режиме "только" клиента, то настроить драйвы на вход
- Если в режиме удаленки с рабочего стола, то настроить подключение
- СМС - просто настроить доступ
- Детальные: открыть науку и подключить на удаленку
- Файловый менеджер
- Скачать "веб-диск"
- В режиме РDP, то скопировать архивные файлы с почты
- Если через веб-интерфейс, то просто переадресовать
- Объяснить: просто настроить доступ
- Детальные: открыть науку и подключить на удаленку
- Простая: про-клиенты на телефоне
- Нужные приложения делаются на оффлайн АТС
- Или вручную: Архивировать готовую БДТС
- Разослать инструкции сотрудникам
- Проинструктировать телефонно на мобильные

1-2 недели

- Начать плановые перенос из офиса внутрь удаленки
 - Включить шифрование рабочих столов
 - Организовать дублирование бекапов
 - По окончании можно отключить все офисное компьютерное хозяйство!
 - Возврат в офис не потребует никаких дополнительных работ!
- файлообменной папки
 - Сервера 1С с базами
 - Почтового сервера
 - Тревожная кнопка
 - Пароль знает только учредитель
 - В другой ЦОД
 - Оформлен не на вас
 - У айтишников есть доступ только на запись
 - Тоже зашифровано
 - В офисе останется только роутер для интернета
 - Рабочие компьютеры можно зачистить и обнулить
 - Все сервера выключить и больше не использовать
 - Компьютеры-"телевизоры" теперь взаимозаменяемы
 - Техника не требует модернизации и обслуживания
 - Сломался компьютер - пересели за резервный и г

3-4 день

- Банк-клиенты
 - Через СМС - Продолжаем работать как обычно, но через удаленку
 - Через ЭЦП - Установить на удаленку ПО криптопровайдера (Крипто-прс)
 - Настроить работу ЭЦП
- ЭЦП
 - Флешки
 - Обычные флешки - просто скопировать в удаленку
 - Другие флешки - Настроить антивирус на локалке
 - Крипто-контейнер - Скопировать на виртуалку бух. и директора
 - РyToren и E-Token перевести в цифровой вид
 - Настроить USB-сканалки
 - Пробросить USB-сканалки
- ЭДО (СБИС, Контур, Астрал...)
 - Онлайн-версии - прописать сертификаты на виртуальном рабочем столе, продолжить пользоваться
 - Локальные версии - по возможности перейти на онлайн-версии, сертификаты на вход
- МОУ
 - Принтеры
 - USB - Пробросить на удаленку с локального компьютера
 - сетевые - Поставить программу Remote-Scan
 - USB - Установить на удаленку драйвер и пробросить как локал

1. Сдача отчетности с разных ip-адресов
2. Шифрованные мессенджеры и VPN
3. Анонимная почта на зарубежных серверах
4. Свой сервер в секретном месте
5. Прослушка телефонов
6. Вдруг вы сами нас сдадите?
7. Какие гарантии, что информация не пропадет?

Как организовать удаленку, чтобы чужаки не добрались до вашей информации

Удаленные рабочие места можно организовать пятью разными способами:

1. Свой сервер в офисе
2. Свой сервер в чужом помещении
3. Свой сервер в дата-центре
4. Арендванный сервер в дата-центре
5. Арендванные облачные рабочие места

Свой сервер выглядит надежнее, но на самом деле это не так. Как раз безопаснее именно арендовать готовые рабочие места:

	Свой сервер в офисе	Свой сервер в чужом помещении	Свой сервер в дата-центре	Аренда сервера в дата-центре	Аренда облачных рабоч. мест
Разовые вложения	200..500 тыс	200..500 тыс	200..500 тыс	-	-
Ежегодные вложения (амортизация, модерниз.)	50..100 тыс	50..100 тыс	50..100 тыс	-	-
Ежемесячные расходы	-	-	5-15 тыс	15-30 тыс	10-50 тыс
Требуется свой админ, имеет доступ ко всему	+	+	+	+	-
Риск поломки или технического сбоя	высокий	высокий	высокий	средний	низкий
Время восстановления после поломки	~ неделя	~ неделя	~ неделя	~ дни	без остановки
Риск потери данных за последний период	высокий	высокий	высокий	средний	-
Риск простоя из-за электричества или интернета	средний	высокий	низкий	низкий	низкий
Риск изъятия или кражи	высокий	средний	средний	-	-
Риск несанкционированного доступа изнутри	высокий	высокий	средний	средний	низкий
Риск несанкционированного доступа извне	высокий	средний	низкий	низкий	низкий

В чем отличие от бухгалтерий...

1. Сдача отчетности с разных ip-адресов
2. Шифрованные мессенджеры и VPN
3. Анонимная почта на зарубежных серверах
4. Свой сервер в секретном месте
5. Прослушка телефонов
6. Вдруг вы сами нас сдадите?
7. Какие гарантии, что информация не пропадет?

1. Сдача отчетности с разных ip-адресов
2. Шифрованные мессенджеры и VPN
3. Анонимная почта на зарубежных серверах
4. Свой сервер в секретном месте
5. Прослушка телефонов
6. Вдруг вы сами нас сдадите?
7. Какие гарантии, что информация не пропадет?

1. Сдача отчетности с разных ip-адресов
2. Шифрованные мессенджеры и VPN
3. Анонимная почта на зарубежных серверах
4. Свой сервер в секретном месте
5. Прослушка телефонов
6. Вдруг вы сами нас сдадите?
7. Какие гарантии, что информация не пропадет?

Заполните анкету и получите материалы

Павел Миловидов

www.безопасный-офис.рф

p.milovidov@bzpoffice.ru

[Facebook.com/Pavel.Milovidov](https://www.facebook.com/Pavel.Milovidov)

+7 495 980-05-44