+7 (995) 622-00-80
t.me/DmitrySecurity · itibdigital.tech

Чек-лист: 12 проверок безопасности офиса

Пройдитесь по пунктам за 15 минут и отметьте те, что у вас уже выполнены. Каждый неотмеченный пункт — реальный риск потерять данные или остановить работу.

Как пользоваться: если не уверены в ответе — считайте пункт невыполненным. «Кажется, настроено» и «настроено и проверено» — это разные вещи.

- [ ] **1 Резервные копии делаются автоматически и хранятся отдельно**
  Базы 1С, документы и почта копируются по расписанию. Правило 3-2-1: три копии, два разных носителя, одна — вне офиса или недоступна из рабочей сети.

- [ ] **2 Восстановление из копии проверяли за последние 3 месяца**
  Копия, из которой ни разу не восстанавливались, — это надежда, а не защита.

- [ ] **3 RDP и другие сервисы не открыты в интернет**
  Удалённый доступ — только через VPN. Открытый RDP — одна из самых частых причин заражения шифровальщиком.

- [ ] **4 Двухфакторная аутентификация включена**
  Для почты, VPN, облачных сервисов и банк-клиента — пароль плюс код из приложения или SMS.

- [ ] **5 У сотрудников нет прав администратора**
  Обычная учётная запись не даёт вирусу закрепиться в системе и установить лишнее.

- [ ] **6 Пароли уникальные и хранятся в менеджере паролей**
  Не в блокноте, Excel или на стикерах. Заводские пароли на роутерах, камерах и NAS сменены.

- [ ] **7 Обновления устанавливаются регулярно**
  Windows, программы и прошивки оборудования. Системы без поддержки производителя (Windows 7, 8.1, Windows 10 без расширенных обновлений) заменены или изолированы.

- [ ] **8** **Антивирус работает на всех компьютерах и серверах**
  Базы обновляются, а состояние защиты видно централизованно, а не «где-то стоит».

- [ ] **9** **Уволенные сотрудники отключаются в день ухода**
  Почта, VPN, 1С, облака; общие пароли, которые они знали, сменены.

- [ ] **10** **Гостевой Wi-Fi отделён от рабочей сети**
  Гости и личные телефоны не видят компьютеры, сервер и принтеры. Рабочий Wi-Fi — WPA2/WPA3 и надёжный пароль.

- [ ] **11** **Сотрудники умеют распознавать фишинг**
  Знают признаки поддельных писем и понимают, кому сообщить о подозрительном письме или ссылке.

- [ ] **12** **Есть план на случай инцидента**
  Кому звонить, что отключать, где лежат копии и доступы. Список систем и паролей актуален и хранится в защищённом месте.

11–12 ✓
Хороший уровень. Продолжайте проверять копии и обновления.

8–10 ✓
Есть заметные риски. Закройте их в ближайший месяц.

Меньше 8
Высокий риск потери данных и простоя. Начните с пунктов 1–4.

Если компьютеры уже зашифровали

- Отключите заражённые компьютеры от сети: кабель и Wi-Fi.
- Не перезагружайте и не выключайте серверы без специалиста — можно потерять следы и шанс на восстановление.
- Не платите вымогателям сразу и не удаляйте файлы с требованиями.
- Позвоните специалисту: чем раньше начать, тем больше данных удаётся спасти.

Проверю эти 12 пунктов за вас — бесплатно

Экспресс-аудит за 30 минут, удалённо или в офисе. Покажу реальные риски и что исправить в первую очередь.

+7 (995) 622-00-80 **t.me/DmitrySecurity** **itibdigital.tech**