8 (987) 256-8192
maximov.online · Уфа

ЧЕК-ЛИСТ ДЛЯ РУКОВОДИТЕЛЯ

15 признаков, что ваша ИТ-инфраструктура в зоне риска

За 10 минут вы поймёте, где бизнес теряет деньги и данные. Без сложных терминов — только то, что вы можете проверить сами. В конце — базовый план действий на эту неделю.

10	15	0
минут на проверку	пунктов проверки	сложных терминов

> **«Если сегодня ночью всё зашифруют — с чего вы поднимаете бизнес и за сколько дней?»**
>
> Если у вас нет быстрого ответа на этот вопрос — этот чек-лист для вас.

8 (987) 256-8192
Будни 09:00–19:00

Как пользоваться

Открыв файл в программе для чтения PDF, вы можете ставить галочки прямо на компьютере — а счётчик на странице 5 сам посчитает результат. Или распечатайте и отмечайте ручкой. Ничего страшного, если галочек окажется много: это норма для растущей компании. Важно их увидеть.

1

Отметьте

Пройдите 15 пунктов и отметьте те, что про вашу компанию. Не уверены — считайте, что пункт про вас.

2

Посчитайте

Счётчик на странице «Результат» сложит галочки сам. На бумаге — сложите вручную.

3

Посмотрите итог

Узнаете, что означает ваш результат и с чего начать в первую очередь.

Честно: чек-лист показывает симптомы, а не ставит диагноз. Он не заменяет проверку специалистом, но точно покажет, стоит ли о ней задуматься — и сэкономит вам первый разговор.

A ДАННЫЕ И ВОССТАНОВЛЕНИЕ

● критично — может остановить бизнес ● высокий риск ● стоит устранить

☐ **1. Никто давно не проверял, восстанавливаются ли резервные копии — или их вообще нет** КРИТИЧНО

→ Если сервер выйдет из строя или данные зашифруют, вернуть их будет нечем.

☐ **2. Резервная копия хранится там же, где рабочие данные — на том же сервере или в той же сети** КРИТИЧНО

→ Шифровальщик уничтожит и данные, и копию одним махом.

☐ **3. Никто в компании не может быстро сказать, где физически лежат критичные данные: 1С, договоры, база клиентов** ВЫСОКИЙ РИСК

→ Нельзя защитить то, о чём не знаешь; при инциденте теряется самое важное.

8 (987) 256-8192
Будни 09:00–19:00

B ЛЮДИ И ДОСТУПЫ

☐ **4. Полный доступ ко всем системам и все пароли — у одного человека, и всё держится на нём** КРИТИЧНО

→ Уйдёт, заболеет или поссоритесь — и вы теряете управление собственной инфраструктурой.

☐ **5. Учётные записи уволенных сотрудников не отключаются сразу же** ВЫСОКИЙ РИСК

→ Бывший сотрудник или тот, кто знает его пароль, сохраняет доступ к вашим данным.

☐ **6. Доступ подрядчиков (1С, видеонаблюдение, кассы) выдан бессрочно, и никто не помнит, у кого он есть** ВЫСОКИЙ РИСК

→ Каждый такой вход — открытая дверь в вашу сеть, о которой вы забыли.

C ПАРОЛИ И ВХОД

☐ **7. Сотрудники используют простые или одинаковые пароли, пишут их на стикерах или в файле Excel** ВЫСОКИЙ РИСК

→ Подобрать такой пароль — минуты, а дальше открыт доступ к рабочим данным.

☐ **8. Вход в почту и удалённый доступ работает по одному паролю, без второго подтверждения** КРИТИЧНО

→ Украли или подобрали пароль — и защищаться больше нечем.

☐ **9. Сотрудники работают на своих компьютерах с правами администратора** ВЫСОКИЙ РИСК

→ Один клик по вложению из письма — и заражается вся сеть, а не одна машина.

D СЕТЬ И ЗАРАЖЕНИЕ

☐ **10.** **К рабочему столу можно подключиться прямо из интернета (RDP «наружу»)** КРИТИЧНО
→ Это вход №1 для шифровальщиков в малый бизнес.

☐ **11.** **Обновления Windows и программ ставятся «когда-нибудь» или не ставятся вовсе** ВЫСОКИЙ РИСК
→ Известные уязвимости остаются открытыми месяцами — именно ими и пользуются.

☐ **12.** **Антивирус вроде стоит, но его оповещения никто не смотрит** УСТРАНИТЬ
→ Заражение замечают, когда работа уже встала.

☐ **13.** **Гостевой Wi-Fi и рабочая сеть — это одно и то же** УСТРАНИТЬ
→ Телефон случайного гостя оказывается в одной сети с бухгалтерией.

E ДЕНЬГИ И ЗАКОН

☐ **14.** **Нет привычки перепроверять смену реквизитов в письме по другому каналу — звонком** ВЫСОКИЙ РИСК
→ Мошенничество с подменой счёта в письме бьёт по малому бизнесу чаще, чем взлом.

☐ **15.** **Не оформлены документы по персональным данным: согласия, уведомление в Роскомнадзор** ВЫСОКИЙ РИСК
→ Штрафы за утечку и нарушения с 2025 года исчисляются миллионами рублей.

8 (987) 256-8192
Будни 09:00–19:00

Что означает ваш результат

Если вы отмечали галочки в программе для чтения PDF, счётчик уже показал число ниже. На бумаге — сложите отмеченные пункты сами и найдите свой диапазон.

ОТМЕЧЕНО ИЗ 15

Ваш результат — считается автоматически

Число слева — сколько признаков риска вы отметили галочками. Ваша зона отметится галочкой в таблице ниже. Помните: красные (критичные) пункты весят больше любого счёта — один такой уже требует действий.

0–2
ГАЛОЧКИ

Базовая гигиена есть

Инфраструктура в целом в порядке. Но если среди отмеченного есть хоть один красный пункт — займитесь им: он не про «неудобно», а про «однажды остановит бизнес».

☐ ВАША ЗОНА

3–6
ГАЛОЧЕК

Слабые места накопились

Типичная картина для растущей компании. Часть пробелов — критичные. Разумно разобраться планово, пока проблема не превратилась в инцидент с простоем и потерями.

☐ ВАША ЗОНА

7+
ГАЛОЧЕК

Красная зона

Серьёзный сбой или атака — вопрос времени, а не вероятности. Начните с критичных пунктов уже на этой неделе, не откладывая.

☐ ВАША ЗОНА

Важно: любой отмеченный красный пункт важнее общего счёта. Можно набрать всего две галочки, но если одна из них — «резервная копия хранится рядом с данными», риск потерять весь бизнес за одну ночь у вас уже высокий.

8 (987) 256-8192
Будни 09:00–19:00

Базовый план действий

Пять шагов, которые закрывают большую часть рисков из чек-листа и которые можно начать без бюджета уже на этой неделе. Порядок важен: он идёт от самого дорогого риска к менее острым.

1 **Проверьте резервную копию делом**

Не «есть ли бэкапы», а восстановите один файл или базу и убедитесь, что данные открываются. И проверьте главное: хотя бы одна копия должна лежать отдельно, вне рабочей сети, куда не дотянется шифровальщик.

2 **Закройте лишние двери снаружи**

Уберите прямой доступ к рабочему столу из интернета и включите второе подтверждение (SMS или приложение) на почте и удалённом доступе. Это закрывает два главных входа для атак.

3 **Наведите порядок в доступах**

Отключите учётные записи уволенных сотрудников. Составьте список: у кого есть права администратора, кто из подрядчиков имеет удалённый доступ и зачем. Лишнее — уберите.

4 **Уберите пароли из Excel и со стикеров**

Заведите менеджер паролей — отдельно для ИТ и для бухгалтерии. Это дешёвая мера, которая закрывает сразу несколько пунктов чек-листа.

5 **Назначьте ответственного**

Один человек, который отвечает за ИТ-безопасность, знает, где лежат критичные данные и у кого к ним доступ. Без ответственного любой план остаётся на бумаге.

ГЛУБОКОЕ IT-ПОГРУЖЕНИЕ

Хотите точную картину, а не самопроверку?

Чек-лист показывает симптомы. «Глубокое IT-погружение» — это полная диагностика вашей инфраструктуры: мы проверяем всё из чек-листа и ещё сотню параметров, тестируем восстановление данных вживую и отдаём отчёт с приоритетами — на языке денег и сроков, а не терминов.

- ✓ Аудит доступов и учётных записей
- ✓ Анализ сети и уязвимостей периметра
- ✓ Проверка документов по 152-ФЗ
- ✓ Проверка бэкапов с тестовым восстановлением
- ✓ Оценка защиты серверов и рабочих мест
- ✓ Отчёт для руководителя + план работ

> **Стоимость диагностики вычитается из первого месяца обслуживания,** если вы заключаете договор. Фактически аудит получается бесплатным.

ТЕЛЕФОН

8 (987) 256-8192

WHATSAPP · TELEGRAM

Напишите нам в мессенджер — ответим в рабочее время

САЙТ · ГОРОД

maximov.online · Уфа
Будни 09:00–19:00, дежурный инженер 24/7 по SLA

Позвоните или напишите — покажем, что нашли, и с чего начать.