

Аудит ИТ-инфраструктуры за 30 минут

Чек-лист для руководителя растущей компании.

Этот экспресс-аудит помогает быстро понять: **где вы теряете деньги из-за рисков ИТ, простоев и хаоса в управлении.**

Что вы получаете после такого аудита:

- Понимание главных рисков простоев и потерь;
- Приоритетный список улучшений на 90 дней;
- Четкое понимание, нужен ли вам директор по ИТ на аутсорсе.

Отмечайте только то, что действительно выполнено и подтверждено.

Защита от вынужденных остановок оборудования Серверы и оборудование — «надежность фундамента»

- ☐ У вас есть актуальный список всех серверов и ключевого оборудования (один документ)
- ☐ Вы знаете, какие системы критичны для остановки бизнеса
- ☐ Есть резервирование от отказа дисков/компонентов сервера/сервера/роутера
- ☐ Есть понятная схема инфраструктуры не только в голове вашего единственного сисадмина.

Если отмечено менее 3 пунктов — высокий риск внезапных простоев.

Защита от хакерских атак Защита от вирусов и взломов — «безопасность бизнеса»

- ☐ Обновления безопасности устанавливаются регулярно
- ☐ Блокировка запуска неизвестного ПО

- ☐ Пользователи неадмины на серверах и компьютерах
- ☐ Права доступа выдаются по принципу минимальных привилегий

Если отмечено менее 3 пунктов — высокий риск атак и шантажа (ransomware).

Бэкапы — «страховка от катастроф»

- ☐ Четко определено, что именно вы резервируете
- ☐ Реализовано правило 3-2-1 (разные носители и разные площадки)
- ☐ Бэкапы делаются автоматически по расписанию
- ☐ Вы хотя бы раз в квартал проверяете восстановление из бэкапа
- ☐ Есть защита от случайного удаления и шифрования

Если отмечено менее 3 пунктов — восстановление после аварии под вопросом.

Питание — «что будет при отключении света»

- ☐ Критичное оборудование подключено к ИБП
- ☐ ИБП обслуживаются и проверяются
- ☐ Серверы корректно выключаются при длительном отключении
- ☐ Часть критичных систем размещена в надежном дата-центре

Если отмечено менее 2 пунктов — один скачок напряжения может остановить бизнес.

Интернет — «что если канал упадет»

- ☐ Есть резервный интернет от другого провайдера или 4G/5G
- ☐ Переключение на резерв происходит автоматически
- ☐ Резервный канал регулярно проверяется
- ☐ Ключевые сервисы доступны удаленно при авариях

Если отмечено менее 2 пунктов — высокая зависимость от одного провайдера.

Мониторинг — «видите ли вы проблемы заранее»

- [] Вы видите доступность ключевых сервисов (uptime)
- [] Контролируется нагрузка серверов (CPU, RAM, диск)
- [] Оповещения приходят в удобный канал (Telegram/Email)
- [] Отслеживаются ошибки приложений и баз данных
- [] Есть ответственный за реакцию на алерты
- [] Регулярно проводится аналитика алертов

Если отмечено менее 3 пунктов — вы узнаете о проблемах от клиентов.

SLA и реагирование — «кто тушит пожар»

- [] Есть понятные SLA для критичных систем
- [] Определены время реакции и время восстановления
- [] Есть назначенная команда или подрядчик поддержки
- [] Есть понятный порядок эскалации при авариях
- [] Ведется журнал инцидентов и разборы после сбоев

Если отмечено менее 3 пунктов — реакция на аварии хаотична.

Защита от ухода ИТ-специалиста — «анти-bus-factor»

- [] Есть актуальная документация по инфраструктуре и ключевым системам
- [] Доступы хранятся централизованно и бекаются, а не только в голове одного человека.
- [] Пароли и ключи доступны компании, а не конкретному сотруднику
- [] Есть регламенты типовых операций: прием на работу, увольнение, предоставление доступов.
- [] Есть резервный исполнитель — внутренний или внешний

Если отмечено менее 3 пунктов — бизнес уязвим при уходе одного человека.

Как быстро интерпретировать результат

- Меньше 50% пунктов отмечено — критические риски для бизнеса.
- 50–75% — ИТ работает, но есть системные «мины замедленного действия».
- Более 75% — вы близки к управляемому и масштабируемому ИТ.

Всего в файле 37 пунктов.

У вас отмечено: _____

Если захотите обсудить, как снизить риски и повысить надежность ИТ-сервисов, напишите мне в [телеграм](https://t.me/AnatolySeregin).