Ай-ТИ Фреш

АНАЛИТИЧЕСКИЙ РАЗБОР

Мониторинг ИТ-инфраструктуры и честный SLA для малого бизнеса

Почему «гарантируем 99,9%» без измерений ничего не значит — и во что обходится слепота к сбоям

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

У вас 20–50 рабочих мест, и об очередном сбое вы узнаёте от бухгалтера: «1С не работает». Подрядчик обещает в договоре «доступность 99,9%», но фактически её никто не измеряет, отчётов нет, а каждая авария живёт 30–60 минут, прежде чем её вообще начинают чинить. Сколько компания теряет на простоях за год — неизвестно, и непонятно, за что именно вы платите за ИТ-обслуживание.

Почему это важно бизнесу

- Час простоя офиса на 50 человек — порядка 40 000 ₽ только на зарплатах и упущенной выручке, без учёта штрафов и репутации
- Без мониторинга аварию первыми находят сотрудники — к моменту звонка она длится уже 15–30 минут, счётчик потерь включён
- SLA 99,9% — это почти 9 часов простоя в год; без измерения фактической доступности проверить обещание подрядчика нельзя
- Число ИТ-сбоев в российских компаниях выросло на 22% за 2024 год — среди причин устаревшее оборудование и ПО без поддержки

СТАТИСТИКА

Проблема в цифрах

+22%

рост числа сбоев ИТ-систем и оборудования в российских компаниях за 2024 год

Источник: Монк Диджитал Лаб / ComNews, 2025

~2 млн ₽

средняя стоимость одного значимого инцидента простоя в российской компании

Источник: Монк Диджитал Лаб / Известия, 2025

54%

компаний оценили свой последний серьёзный сбой дороже 100 000 долларов

Источник: Uptime Institute, Annual Outage Analysis 2024

$300 тыс.

во столько и дороже обходится час простоя у 90% средних и крупных компаний

Источник: ITIC Hourly Cost of Downtime Survey, 2024

24 дня

средняя длительность простоя бизнеса после атаки шифровальщика (данные по США)

Источник: Coveware / Statista, 2022

11 дней

длился сбой СДЭК в мае–июне 2024 — от остановки систем до полного восстановления сервисов

Источник: Ведомости / Habr, 2024

КЕЙС 1 ИЗ 3

СДЭК: 11 дней без доставки из-за шифровальщика и редких бэкапов

Ситуация

СДЭК — один из крупнейших логистических операторов России, тысячи пунктов выдачи по стране

Как развивались события

1. 26 мая 2024 группировка Head Mare запускает шифровальщик — ИТ-системы оператора останавливаются
2. 27 мая сайт и приложение недоступны, пункты выдачи по всей стране не принимают и не выдают посылки
3. Атакующие заявляют об уничтожении резервных копий и утверждают, что бэкапы делались лишь раз в полгода
4. Восстановление из архивных копий растягивается более чем на неделю; полная работа сервисов — только с 6 июня

ПОСЛЕДСТВИЯ

Около 11 дней деградации сервиса федерального масштаба: пункты выдачи не работали, отправления копились, часть клиентов ушла к конкурентам. Прямые потери компания не раскрыла; в прессе инцидент называли одной из самых разрушительных кибератак на российский бизнес 2024 года.

ГЛАВНАЯ ОШИБКА / ВЫВОД

Резервное копирование существовало «на бумаге»: целостность и восстановимость копий никто не контролировал. Проверяемые бэкапы и сегментация сети могли бы сократить простой с полутора недель до дней.

Источник: Ведомости, Lenta.ru, Habr — публикации мая–июня 2024

КЕЙС 2 ИЗ 3

Аэрофлот: год незамеченного взлома и день коллапса в Шереметьево

Ситуация

ПАО «Аэрофлот» — крупнейшая авиакомпания России

Как развивались события

1. По заявлениям группировок Silent Crow и «Киберпартизаны BY», доступ в корпоративную сеть у них был около года — незамеченным
2. 28 июля 2025 утром внутренние ИТ-системы выходят из строя; регистрация пассажиров и планирование рейсов останавливаются
3. За день отменено около 50 пар рейсов, всего отменено или задержано 42% рейсов; в Шереметьево — столпотворение пассажиров
4. Атакующие заявляют о краже 12–20 ТБ данных и уничтожении тысяч серверов; полёты по расписанию возобновляются только 29 июля

ПОСЛЕДСТВИЯ

За первый день отменено или задержано 42% рейсов, с проблемами столкнулись не менее 20 000 пассажиров. Совокупный ущерб эксперты оценивали в 10–50 млн долларов. Полёты по расписанию возобновились лишь на следующий день; проверка и восстановление внутренних систем заняли заметно дольше.

ГЛАВНАЯ ОШИБКА / ВЫВОД

Злоумышленники находились в сети около года. Без мониторинга аномалий, контроля привилегированных доступов и событий безопасности даже крупнейшая компания узнаёт об атаке в момент остановки бизнеса.

Источник: РБК, Ведомости, Forbes, CNews — публикации июля 2025

КЕЙС 3 ИЗ 3

CrowdStrike: одно обновление положило 8,5 млн компьютеров

Ситуация

Глобальный инцидент 19.07.2024: клиенты CrowdStrike — авиакомпании, банки, клиники, ритейл по всему миру

Как развивались события

1. 19 июля 2024 вендор выпускает штатное обновление контента Falcon Sensor с ошибкой в конфигурационном файле
2. Около 8,5 млн Windows-машин по всему миру уходят в циклический «синий экран» за считанные часы
3. Останавливаются авиакомпании, банки, клиники, ритейл и госсервисы; рейсы отменяются тысячами
4. Исправление требует ручного входа на каждый компьютер в безопасном режиме — восстановление тянется днями

ПОСЛЕДСТВИЯ

Прямые потери только компаний Fortune 500 — около $5,4 млрд (оценка Parametrix), из них авиакомпании потеряли суммарно $860 млн. Организации без инвентаризации парка и плана отката восстанавливались дольше всех — вручную, машина за машиной.

ГЛАВНАЯ ОШИБКА / ВЫВОД

Даже «доверенное» обновление вендора способно разом положить весь парк. Нужны поэтапная раскатка через пилотную группу машин и мониторинг, который мгновенно видит массовый отказ рабочих мест.

Источник: Fortune, Parametrix, Wikipedia — июль–август 2024

КАК ДЕЛАТЬ НЕ НАДО

Типовые ошибки

✕ **Мониторинг = пинг сервера**
Сервер отвечает на ICMP, а 1С выдаёт ошибку при проводке. Без проверок уровня сервисов «зелёный» мониторинг ничего не гарантирует.

✕ **SLA на словах, а не в договоре**
«Гарантируем 99,9%» без зафиксированного периметра, метода измерения и ежемесячного отчёта — маркетинг, а не обязательство. Проверить его невозможно.

✕ **Бэкапы делаются, но не проверяются**
Копия «где-то есть», но успешность и восстановимость никто не контролирует. Именно так СДЭК получил 11 дней простоя вместо дней.

✕ **Мониторинг живёт в той же сети**
Падает гипервизор или коммутатор — падает и система мониторинга. Авария есть, алертов нет. Мониторинг должен стоять отдельно и смотреть ещё и снаружи.

✕ **Алерты валятся всем и никому**
Сотни писем «disk 80%» в общий ящик приучают всех их игнорировать. Без приоритетов P1–P3, дежурного и эскалации критичный алерт тонет в шуме.

✕ **Нет бизнес-метрик**
Следят за CPU и RAM, но не за закрытием смены 1С, чеками ОФД и обменом с банком. Инфраструктура «зелёная», а бизнес стоит — и никто не видит.

✕ **Сертификаты и сроки вне контроля**
Истёкший SSL-сертификат, домен или лицензия валит сервис посреди рабочего дня. Это самый дешёвый в предотвращении и самый обидный класс аварий.

✕ **Обновления сразу на весь парк**
Раскатка без пилотной группы: одна кривая версия кладёт все машины разом — как обновление CrowdStrike положило 8,5 млн компьютеров за часы.

РЕКОМЕНДАЦИИ И ПРАКТИКИ

Как правильно

МИНИМУМ

- Мониторинг (Zabbix) на отдельной VM вне основной сети
- Базовые проверки: пинг, диски, службы, бэкапы, SSL-сертификаты
- Алерты в Telegram конкретному дежурному, а не в общую почту

НОРМАЛЬНО

- Мониторинг сервисов: 1С, SQL, AD, файловые шары, телефония
- Внешние blackbox-проверки из двух независимых точек
- Матрица приоритетов P1–P3 и регламент эскалации по времени
- Ежемесячный SLA-отчёт по фактической доступности

ХОРОШО

- Синтетические сценарии: бот проходит путь бухгалтера в 1С
- Бизнес-метрики: смены 1С, чеки ОФД, эквайринг, статус бэкапов
- Два интернет-канала с автопереключением и контролем обоих
- Регулярное тестовое восстановление из резервной копии

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Вы узнаёте о сбоях от системы мониторинга раньше, чем от сотрудников?
- [ ] В договоре с ИТ-подрядчиком SLA прописан в часах простоя, с периметром ответственности?
- [ ] Вы получаете ежемесячный отчёт о фактической доступности, а не только счёт за услуги?
- [ ] Кто-то ежедневно проверяет, что вчерашний бэкап сделан и из него реально можно восстановиться?
- [ ] Сервер мониторинга переживёт падение основной сети и всё равно сообщит об аварии?
- [ ] Сроки SSL-сертификатов, доменов и лицензий контролируются автоматически?
- [ ] Вы знаете, во сколько обходится час простоя именно вашей компании?
- [ ] Есть дежурный и понятная эскалация, если авария случится ночью или в выходной?
- [ ] Отслеживается ли главная бизнес-метрика — чеки, смены 1С, заявки, — а не только «железо»?

Если хотя бы на два вопроса ответ «нет» или «не знаю» — тема требует внимания.

ЧТО МЫ ДЕЛАЕМ

Как поможет ITFresh

ITFresh — ИТ-аутсорсинг для юридических лиц до 50 рабочих мест в Москве и области. 15+ лет практики, собственная инфраструктура в дата-центре МТС (8 серверов Dell Xeon Platinum).

- Аудит текущего мониторинга и честный расчёт фактической доступности вашей инфраструктуры за прошлый год
- Внедрение мониторинга Zabbix + Prometheus + Grafana — от пинга до бизнес-метрик, за 5–7 рабочих дней
- Сопровождение с измеримым SLA и ежемесячным отчётом по каждому инциденту
- Дежурная линия с матрицей эскалации: реакция на критичный алерт — до 5 минут, круглосуточно

15+
лет в ИТ-поддержке

50
рабочих мест — наш профиль

МТС
дата-центр, Москва

КОНТАКТЫ

Обсудить вашу задачу

Сайт	**itfresh.ru**
Телефон	**+7 903 729-62-41**
Telegram	**@ITfresh_Boss**

Бесплатно посмотрим вашу инфраструктуру по этому чек-листу и скажем, где тонко — без обязательств.

itfresh.ru

НА ЧЁМ ОСНОВАН РАЗБОР

Источники

01 Российские компании стали чаще сталкиваться со сбоями в работе ИТ-систем (comnews.ru — 2025)

02 Сбои в ПО обходятся компаниям примерно в 2 млн рублей за инцидент (iz.ru — 2025)

03 Annual Outage Analysis 2024 (uptimeinstitute.com — 2024)

04 ITIC 2024 Hourly Cost of Downtime Survey (itic-corp.com — 2024)

05 Average length of downtime after a ransomware attack (Coveware) (statista.com — 2022)

06 Причиной сбоя в работе СДЭК мог стать вирус-шифровальщик (vedomosti.ru — 2024)

07 Крупный сбой в работе СДЭК: хакерская атака и её последствия (habr.com — 2024)

08 Хакеры взяли на себя ответственность за сбой «Аэрофлота» (rbc.ru — 2025)

09 «Аэрофлот» столкнулся с мощнейшей хакерской атакой из-за рубежа (vedomosti.ru — 2025)

10 Атака на самолеты: сколько стоит удар хакеров по «Аэрофлоту» (forbes.ru — 2025)

11 CrowdStrike outage will cost Fortune 500 companies $5.4 billion (fortune.com — 2024)

12 CrowdStrike's Impact on the Fortune 500 (Parametrix) (parametrixinsurance.com — 2024)

Все данные пересказаны по открытым источникам; точность на дату публикации разбора.