Ай-ТИ Фреш

АНАЛИТИЧЕСКИЙ РАЗБОР

Резервные копии, которые не восстанавливаются

Почему «зелёный отчёт» о бэкапе не гарантирует восстановления — и что проверить уже сегодня

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

У вас настроен бэкап, отчёты приходят «успешно», и кажется, что данные защищены. Но копия, которую ни разу не разворачивали, — это гипотеза, а не страховка. Проверка случается в худший момент: после отказа сервера или шифровальщика. И слишком часто выясняется, что копия лежала на том же сервере, была пустой или зашифрована вместе с рабочей системой.

Почему это важно бизнесу

- Простой 1С и файлового сервера останавливает бухгалтерию, отгрузки и отчётность — теряет вся компания, не только ИТ
- Средний критичный ИТ-простой в российских компаниях стоит около 2 млн рублей (данные 2024 года)
- Шифровальщики целенаправленно уничтожают копии: в 94% атак была попытка добраться до бэкапов (Sophos, 2024)
- Утерянную базу 1С восстанавливают вручную из первички — это недели работы бухгалтерии
- Утрата персональных данных клиентов — риск штрафов по 152-ФЗ, с 2025 года включая оборотные

СТАТИСТИКА

Проблема в цифрах

94%

атак шифровальщиков включали попытку уничтожить резервные копии жертвы

Источник: Sophos, The Impact of Compromised Backups, 2024

57%

попыток компрометации бэкапов достигли цели — жертва осталась без рабочих копий

Источник: Sophos, The Impact of Compromised Backups, 2024

×8

настолько выше медианный счёт за восстановление, если атакующие добрались до бэкапов

Источник: Sophos, The Impact of Compromised Backups, 2024

10%

жертв шифровальщиков смогли восстановить более 90% своих данных

Источник: Veeam Ransomware Trends Report 2025

≈2 млн ₽

средняя цена одного критичного ИТ-простоя в российских компаниях

Источник: Киберпротект / РБК, данные 2024

70%

крупных российских компаний по-прежнему зависят от западных систем резервного копирования

Источник: Исследование K2Tex, 2026

КЕЙС 1 ИЗ 3

СДЭК: шифровальщик добрался и до резервных копий

Ситуация

СДЭК — один из крупнейших логистических операторов России

Как развивались события

1. 26 мая 2024: сайт и приложение СДЭК недоступны, пункты выдачи не принимают и не выдают посылки; ответственность взяла на себя группировка Head Mare
2. Атакующие заявили, что зашифровали данные и уничтожили резервные копии, — эксперты обсуждали, насколько изолированы были бэкапы компании
3. Три дня полной остановки приёма и выдачи отправлений по всей стране
4. К 29–30 мая пункты выдачи начали выдавать посылки; полное восстановление сервисов заняло около 10 дней

ПОСЛЕДСТВИЯ

Трое суток полной остановки основного бизнеса, около 10 дней до полного восстановления сервисов. По оценкам в СМИ, ущерб исчислялся сотнями миллионов рублей — недополученная выручка, компенсации клиентам и репутационные потери.

ГЛАВНАЯ ОШИБКА / ВЫВОД

Копии, достижимые из рабочей сети, погибают вместе с продуктивом. Против целевой атаки работают только изолированные и неизменяемые (immutable) резервные копии.

Источник: Ведомости, Lenta.ru, Хакер — май–июнь 2024

КЕЙС 2 ИЗ 3

GitLab: пять механизмов бэкапа — ни один не сработал

Ситуация

GitLab — международная ИТ-компания, сервис для миллионов разработчиков

Как развивались события

1. 31 января 2017: инженер при ночных работах случайно удалил каталог продуктивной базы данных — около 300 ГБ
2. Выяснилось, что регулярный дамп базы молча падал из-за несовпадения версий PostgreSQL — хранилище бэкапов оказалось пустым
3. Письма об ошибках копирования не доходили: их отбрасывал почтовый фильтр, и никто не знал о сбое
4. Восстанавливались из случайного снапшота тестовой среды шестичасовой давности — единственной уцелевшей копии
5. 18 часов полного простоя сервиса на глазах у всего мира

ПОСЛЕДСТВИЯ

18 часов простоя, безвозвратно потеряны 6 часов данных пользователей: около 5000 проектов, 5000 комментариев и 700 новых учётных записей. Репутационный урон компания честно описала в публичном постмортеме.

ГЛАВНАЯ ОШИБКА / ВЫВОД

Все пять уровней резервирования существовали на бумаге, но ни один не проверялся тестовым восстановлением, а ошибки бэкапа терялись молча. «Зелёный» процесс без проверки — это отсутствие бэкапа.

Источник: Официальный постмортем GitLab, 2017

КЕЙС 3 ИЗ 3

Maersk: компанию спас случайно выключенный сервер

Ситуация

Maersk — мировой лидер морских контейнерных перевозок

Как развивались события

1. Июнь 2017: вирус NotPetya за минуты парализовал глобальную сеть Maersk — офисы в 130 странах, порты и терминалы
2. Уничтожены все ~150 контроллеров домена Active Directory — их автономных офлайн-копий не существовало
3. Единственная уцелевшая копия нашлась в офисе в Гане: сервер был обесточен отключением электричества в момент атаки
4. Диск с копией везли в Лондон физически, самолётом — канал связи не позволял передать сотни гигабайт быстро
5. Десять дней на восстановление базовой ИТ-инфраструктуры, переустановлены десятки тысяч ПК и тысячи серверов

ПОСЛЕДСТВИЯ

Около 10 дней восстановления ИТ, недели сбоев в логистике по всему миру. Компания оценила потери в 250–300 млн долларов. От полной катастрофы спасла не система бэкапа, а случайность.

ГЛАВНАЯ ОШИБКА / ВЫВОД

Критичная инфраструктура (Active Directory) не имела ни одной изолированной копии. План восстановления должен покрывать не только данные, но и системы, без которых данные не поднять.

Источник: Отчёты Maersk, Wired (2018), Control Engineering (2021)

КАК ДЕЛАТЬ НЕ НАДО

Типовые ошибки

✕ **Копия на том же сервере**
Второй диск в том же корпусе гибнет вместе с системой: отказ RAID-контроллера, пожар или скачок питания уничтожают и продуктив, и «бэкап».

✕ **Отчёт «успешно» без проверки содержимого**
Скрипт может месяцами копировать пустые каталоги или битые архивы и честно рапортовать об успехе. Проверяется не отчёт, а восстановление.

✕ **Бэкап доступен из сети на запись**
Шифровальщик целенаправленно ищет сетевые папки со словами backup и «архив». Копия без изоляции или режима неизменяемости — уже потерянная копия.

✕ **Восстановление никогда не тестировали**
Бэкап, который ни разу не разворачивали в тестовой среде, — гипотеза. Первый тест в день аварии почти всегда приносит сюрпризы.

✕ **Все доступы у одного человека**
Уволился админ, истёк оплаченный с его личной карты тариф — и облачное хранилище с копиями удалено провайдером вместе с данными.

✕ **RTO никто не считал**
Копия есть, но скачивание архива по офисному каналу занимает 30+ часов. Сколько часов простоя переживёт бизнес — нужно знать до аварии.

✕ **Ключ шифрования в одном экземпляре**
Шифрованный бэкап без ключа бесполезен. Если ключ хранит один человек — его отпуск или увольнение равносильны потере всех копий.

✕ **Облако и SaaS считают бэкапом**
Блокировка аккаунта, сбой или неоплата у провайдера — и данные недоступны. Данные, которые нельзя выгрузить в свою копию, вам не принадлежат.

РЕКОМЕНДАЦИИ И ПРАКТИКИ

Как правильно

МИНИМУМ

- Правило 3-2-1: три копии, два типа носителей, одна вне офиса
- Копия базы 1С и файлов на отдельном устройстве, не на продуктивном сервере
- Уведомления об ошибках копирования на групповой адрес, а не одному человеку
- Доступы к бэкапам и оплата хранилищ — на юрлицо, минимум у двух человек

НОРМАЛЬНО

- Тестовое восстановление ключевой системы (1С, файлы) минимум раз в квартал
- Неизменяемые копии: object lock в облаке или офлайн-носитель по расписанию
- Мониторинг заданий бэкапа с контролем размера и целостности архивов
- Задокументированные RTO/RPO по каждой системе, проверенные на стенде

ХОРОШО

- Изолированная офлайн-копия критичных систем, недостижимая из рабочей сети
- Ежегодные учения: полное восстановление офиса на резервном оборудовании
- Ключи шифрования продублированы: сейф директора + защищённое хранилище
- Независимая выгрузка SaaS-данных (CRM, почта, Битрикс24) через API в свою копию

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Вы лично видели восстановление данных из вашего бэкапа за последние три месяца?
- [ ] Есть ли копия, физически недоступная из офисной сети (офлайн или с запретом удаления)?
- [ ] Переживут ли ваши бэкапы шифровальщика, получившего права администратора сети?
- [ ] Знаете ли вы, сколько часов займёт полное восстановление 1С после потери сервера?
- [ ] Есть ли доступы к хранилищам бэкапов хотя бы у двух сотрудников компании?
- [ ] Оплачиваются ли облачные хранилища с корпоративного счёта, а не с личной карты?
- [ ] Хранится ли ключ шифрования бэкапов более чем в одном месте?
- [ ] Есть ли независимая копия данных из облачных сервисов — CRM, почты, порталов?
- [ ] Читает ли кто-то уведомления об ошибках резервного копирования — и доходят ли они вообще?
- [ ] Проверяет ли кто-то, что в архиве лежит рабочая база, а не пустые или временные файлы?

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 системы резервного копирования с реальным тестовым восстановлением критичной системы на ваш выбор
- Проектирование схемы 3-2-1 под офис до 50 рабочих мест: NAS в офисе плюс российское облако с object lock
- Регулярные тестовые восстановления и мониторинг бэкапов в рамках абонентского сопровождения
- Автоматическая выгрузка данных из облачных сервисов (Битрикс24, CRM, почта) в независимую копию
- Документирование RTO/RPO и плана восстановления, понятного руководителю, а не только админу

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 The Impact of Compromised Backups on Ransomware Outcomes (sophos.com — 2024)

02 Ransomware Trends Report (veeam.com — 2025)

03 Postmortem of database outage of January 31 (about.gitlab.com — 2017)

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

05 «Ответственность за атаку на СДЭК взяла на себя хак-группа Head Mare» (xakep.ru — 2024)

06 «Цена ИТ-простоев для российского МСБ» (cyberprotect.ru — 2026)

07 «K2Tex»: 70% крупных компаний зависят от западных систем РК (ru-bezh.ru — 2026)

08 The Untold Story of NotPetya, the Most Devastating Cyberattack (wired.com — 2018)

09 Throwback Attack: How NotPetya Took Down Maersk (controleng.com — 2021)

10 «Российские системы резервного копирования данных: обзор 2025» (anti-malware.ru — 2025)

11 «Час простоя ИТ-компании составил 21,7 млн руб.» (данные BI.ZONE) (comnews.ru — 2026)

12 GitLab suffers major backup failure after data-deletion incident (techcrunch.com — 2017)

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