



Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

NAS-сервер вместо облака: контроль над данными офиса до 50 РМ

Почему бизнес возвращает файлы из облака на своё железо и какие риски нужно закрыть заранее

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

Суть проблемы

Компания на 20–50 сотрудников платит за облачные диски сотни тысяч рублей в год, но данные ей не принадлежат: тарифы индексируются, вендор может отключить сервис в одностороннем порядке, интернет-канал тормозит работу, а ответственность за утечку по 152-ФЗ всё равно несёт бизнес. Свой NAS возвращает контроль и снижает затраты, но без бэкапов, VPN и мониторинга сам становится т...

Почему это важно бизнесу

- Файлы — операционный актив: день без доступа к договорам, 1С и документам клиентов останавливает бухгалтерию, продажи и производство
- Час простоя ИТ обходится российскому МСБ в 300+ тыс ₽, критичный инцидент — около 2 млн ₽
- Порядка 70% утечек данных приходится на малый и средний бизнес — атакуют не «кого-то большого», а именно вас
- С 30.05.2025 повторная утечка ПДн грозит оборотным штрафом 1–3% годовой выручки, минимум 20 млн ₽
- Облачные тарифы растут: Яндекс 360 индексирует базовый тариф с 319 до 485 ₽/мес за сотрудника с июля 2026



Ключевые параметры реализации

69%

организаций пережили атаку шифровальщика за год; лишь 10% восстановили более 90% данных

Veeam Ransomware Trends, 2025

+44%

рост числа атак шифровальщиков на российские компании за 2024 год

F.A.C.C.T., 2024

300 тыс ₺

и более стоит малому и среднему бизнесу в России один час простоя ИТ-систем

Киберпротект, 2025

20 000+

NAS-устройств QNAP по миру зашифровал вымогатель Deadbolt через доступ из интернета

Censys, 2022

до 500 млн

₺ — оборотный штраф за повторную утечку персональных данных с 30 мая 2025 года

152-ФЗ / КоАП, 2025

1,36%

годовая частота отказов жёстких дисков в дата-центрах: отказ диска — не ЧП, а норма эксплуатац...

Backblaze Drive Stats, 2025



Шифровальщик остановил СДЭК на три дня

Что настраиваем

СДЭК — один из крупнейших логистических операторов РФ, выручка ~70 млрд ₽ (2023)

Как мы это делаем

- 1 26 мая 2024: группировка Head Mage зашифровала ИТ-системы — приём и выдача посылок остановились по всей стране
- 2 27–29 мая: сайт и приложение не работают, отделения выдают посылки вручную по паспорту
- 3 Хакеры утверждали, что резервные копии в компании делались лишь раз в полгода
- 4 Частично сервисы ожили к 29–30 мая, полное восстановление заняло больше недели

РЕЗУЛЬТАТ

Оценки ущерба — от 300–400 млн до 1 млрд ₽ за трое суток полного простоя, плюс репутационные потери, сорванные отправления клиентов и отток к конкурентам.

КЛЮЧЕВОЙ НЮАНС

Решает не место хранения, а дисциплина резервного копирования: без свежих проверенных копий даже крупная компания восстанавливается неделями. Правило 3-2-1 обязательно и для NAS, и для облака.

Ведомости, РБК, Meduza, май–июнь 2024



Deadbolt: 20 000 NAS, открытых в интернет

Что настраиваем

Малые компании и ИП по всему миру — владельцы QNAP NAS с пробросом портов наружу

Как мы это делаем

- 1 Январь 2022: первая волна — около 5 000 устройств зашифрованы через уязвимость веб-интерфейса QNAP
- 2 Сентябрь 2022: число одновременно заражённых NAS достигало 19 000 (пик по данным Censys)
- 3 С каждого владельца требовали 0,03 BTC (~\$1 100); всего группа собрала около \$200 000
- 4 Волны атак повторялись весь 2022 год, несмотря на выпущенные вендором патчи

РЕЗУЛЬТАТ

Суммарно зашифровано более 20 000 устройств. У многих жертв NAS был единственным хранилищем — без копии вне устройства данные утрачены безвозвратно либо выкуплены у преступников.

КЛЮЧЕВОЙ НЮАНС

NAS, доступный из интернета через проброс портов, живёт до первой массовой уязвимости. Удалённый доступ — только через VPN, а резервная копия — всегда вне самого NAS.

Censys, The Record, Help Net Security, 2022



Март 2024: западные облака отключили юрлица РФ

Что настраиваем

Российские компании — корпоративные подписчики облачных сервисов Microsoft, Amazon и Google

Как мы это делаем

- 1 Март 2024: вендоры уведомили о приостановке доступа к облачным продуктам для организаций из РФ с 20 марта
- 2 Softline рекомендовала срочно выгрузить данные из всех облачных сервисов Microsoft, Amazon и Google
- 3 Компании за считанные дни эвакуировали терабайты файлов через ограниченные каналы
- 4 Часть сервисов (Power BI, Dynamics и др.) отключена; оплата подписок из РФ стала невозможна

РЕЗУЛЬТАТ

Бизнесы, хранившие рабочие файлы только в зарубежном облаке, рисковали потерять доступ в одночасье; аварийная миграция обернулась простоями, потерей структуры прав и версий документов.

КЛЮЧЕВОЙ НЮАНС

Облако — это чужой сервер и чужие правила: доступ может исчезнуть по решению вендора или регулятора без компенсаций. Локальная копия критичных данных должна существовать всегда.

РБК, Softline, iXBT, март 2024

Подводные камни

✗ **Десктопные диски в массиве 24/7**

Диски для ПК не рассчитаны на круглосуточную работу и вибрации массива: отказывают в разы чаще NAS-серий, ресурс падает с ~5 лет до 1,5-2.

✗ **NAS наружу через проброс портов**

Именно так Deadbolt зашифровал 20 000+ устройств по миру. Удалённый доступ — только через VPN или защищённый обратный прокси.

✗ **RAID вместо бэкапа**

RAID переживает отказ диска, но не шифровальщика, ошибку сотрудника, пожар или сгоревший контроллер. Нужна отдельная копия вне устройства.

✗ **Бэкап «настроим потом»**

Хранилище запускают, а копирование откладывают. 89% атакующих целятся именно в резервные копии — инцидент ждать не будет.

✗ **Экономия на ECC-памяти и UPS**

Бытовая ошибка RAM молча портит файлы, а скачок питания рушит файловую систему. Экономия 30-60 тыс ₽ против данных на миллионы.

✗ **Нет мониторинга дисков и места**

Отказ диска замечают, когда падает второй. SMART-алерты и контроль заполнения — обязательная часть эксплуатации, а не опция.

✗ **Общие пароли и права «всем всё»**

Без доменных групп доступа любой сотрудник — и любой вирус на его ПК — видит и шифрует все папки компании разом.

✗ **Восстановление никто не проверял**

Бэкап без тестового восстановления — лотерея: 57% атакованных компаний вернули меньше половины данных (Veeam, 2025).



Как правильно

МИНИМУМ

- Диски NAS-серии и RAID с чётностью — никакого RAID 0 для рабочих данных
- UPS с корректным автозавершением работы при пропадании питания
- Ежедневная резервная копия на отдельный носитель вне NAS
- Удалённый доступ только через VPN, без проброса портов наружу

НОРМАЛЬНО

- ECC-память, снапшоты по расписанию, еженедельная проверка целостности (scrub)
- Правило 3-2-1: вторая копия на другом носителе плюс копия вне офиса
- Права доступа по группам Active Directory, разделение отделов
- Мониторинг SMART и заполнения хранилища с алертами ответственному

ХОРОШО

- Шифрование датасетов (требования 152-ФЗ) и неизменяемые копии против шифровальщика
- Ежеквартальное тестовое восстановление из бэкапа с протоколом результата
- Репликация на второй NAS или в независимое хранилище вне площадки
- Договор сопровождения: замена диска и реакция за часы, а не недели

Чек-лист самопроверки

- Вы знаете, где физически лежат все рабочие файлы компании и кто имеет к ним доступ?
- Если облачный сервис завтра отключит вас или поднимет тариф вдвое — есть план и локальная копия?
- Есть ли копия критичных данных вне офиса и вне основного хранилища (правило 3-2-1)?
- Проверяли ли вы восстановление из резервной копии за последние три месяца?
- Закрыт ли доступ к файловому хранилищу из интернета без VPN?
- Разграничены ли права: видит ли бухгалтерия документы юристов, а продажи — кадровые файлы?
- Узнаете ли вы об отказе диска или переполнении хранилища раньше, чем встанет работа?
- Хранятся ли персональные данные клиентов с шифрованием и с учётом требований 152-ФЗ?
- Есть ли у базы 1С отдельный ежедневный бэкап с контролем успешности?
- Понимаете ли вы, во сколько компании обойдётся один день без доступа к файлам?

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



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).

- Бесплатный аудит хранения файлов: где лежат данные, сколько стоит облако, где риски потери
- Расчёт и внедрение NAS под ключ: железо, TrueNAS, интеграция с AD, миграция из облака
- Настройка резервного копирования по правилу 3-2-1 с шифрованием и копией вне офиса
- Сопровождение: мониторинг дисков, тестовые восстановления, замена дисков в течение часов
- Защищённый удалённый доступ к файлам через VPN — без открытых портов и лишних рисков

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

Техническая база

- 01** Veeam Ransomware Trends Report (veeam.com — 2025)
- 02** Censys: Tracking Deadbolt Ransomware (censys.com — 2022)
- 03** F.A.C.C.T. — киберугрозы 2024/2025 (обзор РБК) (rbc.ru — 2024)
- 04** Киберпротект: цена ИТ-простоев для МСБ (cyberprotect.ru — 2025)
- 05** Компьютерра: 70% утечек приходится на МСБ (computerra.ru — 2025)
- 06** КонсультантПлюс: штрафы за ПДн с 30.05.2025 (consultant.ru — 2025)
- 07** Ведомости: причиной сбоя СДЭК стал шифровальщик (vedomosti.ru — 2024)
- 08** Meduza: ущерб СДЭК до 1 млрд рублей (meduza.io — 2024)
- 09** Softline: приостановка облаков Microsoft/AWS/Google (softline.ru — 2024)
- 10** Backblaze Drive Stats (итоги 2025) (backblaze.com — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.

