Ай-ТИ Фреш

АНАЛИТИЧЕСКИЙ РАЗБОР

Защита офиса до 50 ПК от шифровальщиков

Аналитический разбор: реальные инциденты, статистика и план защиты для малого бизнеса

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Вы руководите компанией на 20–50 рабочих мест и считаете, что шифровальщики — проблема корпораций. На деле атаки идут автоматически: боты сканируют весь интернет и сами находят открытый RDP или уязвимый роутер, а найденный доступ продаётся как товар. Однажды утром бухгалтерия не открывает 1С, файлы и почта зашифрованы, на экране — требование выкупа, и бизнес встаёт на недели.

Почему это важно бизнесу

- Атаки автоматизированы: жертву выбирает сканер, а не человек — размер и известность компании не имеют значения
- Шифрование сервера 1С и файлов останавливает бухгалтерию, продажи и отгрузки одновременно — весь бизнес, не один отдел
- Типичный выкуп для малого бизнеса в России — от 100 тыс. до 5 млн руб., а простой часто обходится дороже выкупа
- Если затронуты персональные данные — уведомление Роскомнадзора за 24 часа и штрафы вплоть до оборотных
- Средний простой после атаки — около 24 дней; малый бизнес такой паузы может не пережить

СТАТИСТИКА

Проблема в цифрах

500+

атак шифровальщиков на российские компании за 2024 год — в 1,5 раза больше, чем годом ранее

Источник: F6 (ex-F.A.C.C.T.), итоги 2024 года

51%

кибератак в 2025 году длились менее суток и чаще всего заканчивались шифрованием файлов

Источник: «Лаборатория Касперского», отчёт за 2025 год

до 5 млн ₽

типичный первоначальный выкуп у малого бизнеса в России (нижняя граница — 100 тыс. руб.)

Источник: F6 (ex-F.A.C.C.T.), итоги 2024 года

24 дня

средний простой бизнеса после атаки шифровальщика

Источник: Coveware, отчёт за II квартал 2022

54%

компаний восстановили данные из бэкапов — минимум за шесть лет: копии тоже уничтожают

Источник: Sophos State of Ransomware 2025

до 3 млн ₽

штраф юрлицу за неуведомление Роскомнадзора об утечке персональных данных в срок

Источник: КоАП РФ ст. 13.11, с 30.05.2025

КЕЙС 1 ИЗ 3

СДЭК: 11 дней паралича доставки

Ситуация

СДЭК — крупный российский логистический оператор (май 2024)

Как развивались события

1. Вечер 26 мая 2024: сайт, приложение и внутренние системы перестают работать по всей сети
2. 27 мая: приём и выдача отправлений приостановлены по всей стране
3. 28 мая: группировка Head Mare заявляет об атаке шифровальщиком и утверждает, что уничтожила резервные копии
4. 29 мая: пункты начинают выдавать готовые к выдаче посылки, системы работают частично
5. Полное восстановление всех сервисов — только к 6 июня

ПОСЛЕДСТВИЯ

Около 11 дней до полного восстановления сервисов: простой тысяч пунктов выдачи, отток клиентов к конкурентам, репутационный ущерб. Точную сумму потерь компания не раскрывала.

ГЛАВНАЯ ОШИБКА / ВЫВОД

Даже крупная ИТ-зрелая компания восстанавливалась почти две недели: решают изолированные проверенные бэкапы и отработанный план восстановления, а не только защита периметра.

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

КЕЙС 2 ИЗ 3

Мираторг: под угрозой отгрузки по всей стране

Ситуация

Агрохолдинг «Мираторг» — один из крупнейших агрохолдингов России (март 2022)

Как развивались события

1. Троян-шифровальщик на базе BitLocker шифрует данные в системах хранения складских и учётных систем
2. Нарушена работа с государственной системой ВетИС — оформление электронных ветсертификатов останавливается
3. Без сертификатов продукция не может законно перемещаться — под угрозой поставки по всей стране
4. Россельхознадзор экстренно разрешает перевозку продукции без электронных ВСД до устранения последствий
5. Восстановление занимает несколько суток; пострадали 18 предприятий холдинга

ПОСЛЕДСТВИЯ

Несколько суток работы в аварийном режиме: оформление электронных ветсертификатов остановлено на 18 предприятиях, потребовалось экстренное послабление государственного регулятора, чтобы не встали поставки продукции.

ГЛАВНАЯ ОШИБКА / ВЫВОД

По данным Россельхознадзора, троян использовал уязвимость ОС Microsoft; учётные системы не были изолированы от общей сети — одна точка входа остановила ключевой бизнес-процесс.

Источник: Россельхознадзор (fsvps.gov.ru), CNews, SecurityLab — 2022

КЕЙС 3 ИЗ 3

Garmin: выкуп $10 млн за декриптор

Ситуация

Garmin — мировой производитель GPS-навигации и носимых устройств (июль 2020)

Как развивались события

1. 23 июля 2020: шифровальщик WastedLocker останавливает сервисы Garmin Connect, колл-центры и, по сообщениям СМИ, производственные линии
2. 4–5 дней глобального простоя: миллионы пользователей без сервисов, авиационный flyGarmin недоступен
3. Компания получает декриптор — по данным СМИ, после выплаты выкупа порядка $10 млн
4. Полное восстановление сервисов растягивается ещё на несколько дней

ПОСЛЕДСТВИЯ

Около 5 дней глобального простоя сервисов плюс выкуп порядка $10 млн (по данным СМИ). Оплата не отменила затрат на восстановление и репутационных потерь.

ГЛАВНАЯ ОШИБКА / ВЫВОД

Без гарантированно восстановимых бэкапов даже корпорация с миллиардной выручкой оказалась перед выбором «платить или потерять всё» — и заплатила преступникам.

Источник: BleepingComputer, Threatpost, CSHub — 2020

КАК ДЕЛАТЬ НЕ НАДО

Типовые ошибки

- **Открытый RDP в интернет**
  Один из главных векторов проникновения в России: подобранные или украденные пароли к удалённому рабочему столу открывают дверь в сеть.

- **Бэкап-сервер в домене**
  Шифровальщик с правами администратора домена первым делом находит и уничтожает резервные копии — восстанавливаться оказывается не с чего.

- **Бэкапы без тестового восстановления**
  Что копия нерабочая, выясняется в день атаки. Без регулярной проверки восстановления бэкапа у вас фактически нет.

- **Пользователи с правами админа**
  Одно фишинговое письмо — и вредонос получает полные права на ПК, а дальше двигается по сети до серверов и баз 1С.

- **Надежда только на антивирус**
  Классический сигнатурный антивирус часто не распознаёт современных шифровальщиков: их выявляют по поведению — нужен EDR.

- **Плоская сеть без сегментации**
  Из гостевого Wi-Fi или с ПК менеджера напрямую виден сервер 1С — заражение одной машины охватывает всю инфраструктуру.

- **Почта без фильтрации вложений**
  Макросы и исполняемые вложения доходят до бухгалтера; фишинг остаётся одним из главных способов первичного заражения.

- **Нет плана реагирования**
  Первые часы уходят на панику: никто не изолирует заражённые ПК и не блокирует учётки — шифрование расползается на всю сеть.

РЕКОМЕНДАЦИИ И ПРАКТИКИ

Как правильно

МИНИМУМ

- Закрыть RDP и SMB из интернета, удалённый доступ — только через VPN
- Ежедневный бэкап на устройство вне домена + копия в облако с защитой от удаления
- Забрать у сотрудников права локального администратора
- Заблокировать макросы Office из интернета и опасные вложения в почте

НОРМАЛЬНО

- Двухфакторная аутентификация на VPN, почте и всех внешних доступах
- Тестовое восстановление из бэкапа минимум раз в квартал
- EDR с поведенческим анализом на все рабочие станции и серверы
- Сегментация сети: пользователи, серверы, Wi-Fi и камеры — в разных VLAN

ХОРОШО

- Централизованный сбор логов и алерты на массовое изменение файлов
- Регулярные фишинговые тренировки и обучение сотрудников
- Письменный план реагирования на инцидент, отработанный на учениях
- Неизменяемые копии бэкапов, LAPS, контроль запуска программ, tier-модель админов

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Вы уверены, что порт удалённого рабочего стола (RDP) вашего офиса не доступен из интернета?
- [ ] Есть ли копия бэкапа вне офиса и вне домена — там, где её не удалит даже администратор?
- [ ] Проверяли ли вы за последние три месяца, что база 1С реально восстанавливается из бэкапа?
- [ ] Работают ли сотрудники без прав локального администратора на своих компьютерах?
- [ ] Включена ли двухфакторная аутентификация на VPN, почте и удалённых доступах?
- [ ] Заблокированы ли макросы Office и исполняемые вложения в корпоративной почте?
- [ ] Стоит ли на компьютерах защита с поведенческим анализом (EDR), а не только антивирус?
- [ ] Знает ли ваша команда, кто и что делает в первые 30 минут после обнаружения шифровальщика?
- [ ] Успеете ли вы уведомить Роскомнадзор за 24 часа, если утекут персональные данные?
- [ ] Остались ли в сети Windows 7 или Server 2012, которые больше не получают обновлений?

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 защищённости офиса: периметр, бэкапы, права, почта — отчёт с приоритетами за первую неделю
- Внедрение базовой защиты за две недели: бэкап 3-2-1, VPN с MFA, снятие админ-прав, EDR
- Сопровождение: мониторинг, обновления, регулярная проверка восстановления бэкапов
- План реагирования на инциденты и фишинговые тренировки для сотрудников

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 F6 (ex-F.A.C.C.T.) — годовой отчёт о киберпреступности в России и СНГ (f6.ru — 2025)

02 «Лаборатория Касперского» — отчёт по инцидентам за 2025 год (kaspersky.ru, cnews.ru — 2026)

03 Sophos — The State of Ransomware 2025 (sophos.com — 2025)

04 Coveware — квартальная аналитика по ransomware-инцидентам (coveware.com — 2022)

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

06 Хроника сбоя СДЭК: атака Head Mare и восстановление сервисов (lenta.ru, habr.com — 2024)

07 Сообщения об атаке шифровальщика на «Мираторг» и работе ВетИС (fsvps.gov.ru — 2022)

08 «Хакеры заблокировали данные огромного российского агрохолдинга» (cnews.ru — 2022)

09 Garmin получил декриптор WastedLocker (выкуп ~$10 млн) (bleepingcomputer.com — 2020)

10 Новые штрафы за утечки персональных данных с 30.05.2025 (consultant.ru — 2025)

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