Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Обновления Windows под контролем: цена пропущенного патча

Инженерный разбор ITfresh: почему непропатченный офис — главная мишень шифровальщиков

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Обновления Windows в небольшом офисе живут своей жизнью: одни ПК обновляются и перезагружаются посреди рабочего дня, другие годами не получают патчей — «чтобы не мешали». Пока тихо, проблемы не видно. Но шифровальщики заходят через известные, давно закрытые уязвимости, а после атаки бизнес ждут недели простоя и потери, несопоставимые с ценой нормального процесса обновлений.

Почему это важно бизнесу

- Взлом через незакрытую уязвимость — это не «сбой у айтишников», а остановка касс, 1С и бухгалтерии на дни и недели
- Средний простой после шифровальщика измеряется неделями; компания на 20–50 рабочих мест такой паузы может не пережить
- Утечка персональных данных с 30.05.2025 грозит штрафом до 15 млн ₽, повторная — оборотным до 3% годовой выручки
- Обратная крайность — патчи сразу на все машины без пилота: одно кривое обновление кладёт весь офис разом

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

~20%

взломов начинаются с эксплуатации уязвимостей в ПО — один из главных векторов проникновения

~32%

атак шифровальщиков стартовали с непропатченной уязвимости

21 день

типичный простой бизнеса после атаки шифровальщика

500+

атак шифровальщиков на российские компании за год — рост в полтора раза год к году

8,5 млн

Windows-машин по миру разом легли из-за одного непротестированного обновления агента

15 млн ₽

максимальный штраф за первую крупную утечку персональных данных по 152-ФЗ с 30 мая 2025 года

РЕАЛИЗАЦИЯ 1 ИЗ 3

NotPetya: патч вышел за два месяца до атаки

Что настраиваем

Крупный контейнерный перевозчик и тысячи компаний меньшего размера

Как мы это делаем

1. Март 2017: Microsoft выпускает бюллетень MS17-010, закрывающий уязвимость SMBv1 (EternalBlue)
2. Май 2017: WannaCry поражает сотни тысяч непропатченных ПК по миру — первый громкий звонок
3. Июнь 2017: NotPetya через ту же уязвимость за часы парализует сети компаний в десятках стран
4. У пострадавшего перевозчика встаёт ИТ-инфраструктура в 130 странах: порты и терминалы останавливаются
5. 10 дней ручного восстановления: 4 000 серверов и 45 000 ПК переустановлены с нуля

РЕЗУЛЬТАТ

Убытки оценены примерно в 300 млн $. Атака не использовала неуловимый 0-day: заплатка существовала два месяца, у компаний просто не было процесса её установки.

КЛЮЧЕВОЙ НЮАНС

Регулярная установка критических патчей на все машины — базовая страховка. Уязвимость, уже закрытая производителем, не должна жить в вашей сети месяцами.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Служба доставки: три дня без приёма и выдачи посылок

Что настраиваем

Одна из крупнейших российских служб доставки

Как мы это делаем

1. Май 2024: атака на инфраструктуру с запуском шифровальщика
2. Сайт и приложение не работают, пункты выдачи по всей стране останавливаются на 3 дня
3. По заявлению атакующих, уничтожены и резервные копии; полное восстановление заняло около полутора недель

РЕЗУЛЬТАТ

Ущерб от простоя оценивался в сотни миллионов рублей без учёта упущенной выгоды и репутационных потерь. Российский бизнес после 2022 года — не менее частая мишень, чем западный.

КЛЮЧЕВОЙ НЮАНС

Гигиена инфраструктуры — своевременные патчи, сегментация, изолированные бэкапы — определяет, станет ли атака инцидентом на час или простоем на неделю.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Дефектное обновление агента, уложившее 8,5 млн ПК

Что настраиваем

Тысячи организаций по всему миру — от банков и авиакомпаний до клиник

Как мы это делаем

1. Июль 2024: поставщик защитного ПО рассылает дефектное обновление агента сразу всем клиентам
2. 8,5 млн Windows-машин уходят в «синий экран»; аэропорты, банки и медцентры встают
3. Крупная авиакомпания отменяет свыше 7 000 рейсов за 5 дней; каждую машину восстанавливают вручную
4. В отчёте о причинах поставщик обязуется внедрить поэтапный выпуск обновлений

РЕЗУЛЬТАТ

Потери одной только авиакомпании оценены примерно в 550 млн $. Урок для компании любого размера: обновление, уходящее сразу на все машины без пилотной группы, — такая же бомба, как пропущенный патч.

КЛЮЧЕВОЙ НЮАНС

Любые обновления — сначала на пилотную группу из 10–15 машин, через несколько дней — на остальные. Поэтапный выпуск встроен в WSUS и не требует дополнительных лицензий.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- **Обновления пущены на самотёк**
  Каждый ПК решает сам: часть перезагружается в разгар рабочего дня, часть откладывает патчи месяцами. Общей картины не видит никто.
- **Нет пилотной группы**
  Патчи уходят сразу на все машины. Один дефектный апдейт — и утром не работает весь офис, включая 1С и кассы.
- **Серверы обновляются как обычные ПК**
  Автоматическая перезагрузка сервера 1С или терминального сервера днём останавливает работу всех сотрудников разом.
- **Обновления отключены «чтобы не мешали»**
  После 2022 года — частая практика в РФ. Машина без патчей два-три года — открытая дверь для шифровальщика.
- **Дистрибутивы из случайных источников**
  Сборки с торрентов и «активаторы» нередко несут закладки. Обновления — только с серверов Microsoft или собственного WSUS.
- **Результат установки никто не проверяет**
  Одобрить патч — полдела. Без отчётов WSUS треть машин может месяцами висеть со статусом «ошибка установки» — и об этом никто не узнает.
- **В сети живут системы без поддержки**
  Windows 7, 8.1 и Server 2008/2012 обновлений больше не получают. Одна такая машина в сети обнуляет защиту всех остальных.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Включить установку критических обновлений на всех ПК политикой «Настройка автоматиче…
- Провести инвентаризацию: найти машины без патчей и системы без поддержки (Windows 7/…
- Назначить ответственного и фиксированный день месяца для контроля установки

НОРМАЛЬНО

- Развернуть роль WSUS: централизованное одобрение обновлений и отчёты по всему парку
- Задать клиентам GPO «Указать размещение службы обновлений Майкрософт в интрасети» (W…
- Разбить парк через «Включить клиентское назначение» (TargetGroup): пилот из 10–15 ПК…
- Серверам — отдельная группа и окно: ночь или выходные, согласованная перезагрузка

ХОРОШО

- Правила автоодобрения критических патчей плюс поэтапный выпуск по группам: пилот → о…
- SLA на критические патчи — 7 дней; регулярное обслуживание базы WSUS утилитой wsusut…
- Изолированные (offline) резервные копии и плановый тест восстановления
- Мониторинг: машина без обновлений более 30 дней и сбой синхронизации WSUS видны сразу

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Вы знаете, сколько компьютеров в компании не получали обновлений безопасности больше месяца?
- [ ] Обновления одобряет ответственный специалист, а не каждый ПК сам по себе?
- [ ] Есть ли пилотная группа, на которой патчи проверяются до массовой установки?
- [ ] Серверы 1С и терминальные серверы обновляются по отдельному расписанию с согласованной перезагрузкой?
- [ ] В сети не осталось Windows 7, 8.1 или Server 2008/2012, которые уже не получают патчей?
- [ ] Есть ли отчёт с долей машин, на которых обновления реально установились без ошибок?
- [ ] Дистрибутивы и патчи скачиваются только из доверенных источников, а не со сборок и торрентов?
- [ ] Есть ли изолированная резервная копия, которая переживёт атаку шифровальщика?

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 парка: инвентаризация всех Windows-машин, поиск непропатченных и систем без поддержки, отчёт с приоритетами
- Внедрение WSUS под ключ за 3–5 дней: сервер, роль WSUS, группы, GPO (WUServer, клиентское назначение), пилот, авто…
- Сопровождение цикла обновлений: ежемесячный контроль отчётов WSUS, разбор проблемных машин, патчи серверов ночью
- Резервное копирование и план восстановления: бэкапы, которые переживут шифровальщика, и тест отката
- WSUS остаётся в поставке Windows Server 2025 и поддерживается весь его жизненный цикл; при желании поможем перейти…

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

ДОКУМЕНТАЦИЯ И НАШ СТЕК

Техническая база

01 Deploy updates using Windows Server Update Services (WSUS) (learn.microsoft.com — 2025)

02 Настройка групповых политик для автоматических обновлений (WUServer, «Наст… (learn.microsoft.com — 2025)

03 Управление клиентами и группами WSUS (клиентское назначение, TargetGroup) (learn.microsoft.com — 2025)

04 Removed and deprecated features in Windows Server (статус WSUS, deprecatio… (learn.microsoft.com — 2024)

05 Регламент ITfresh: цикл обновлений, пилотные группы и окна для серверов (itfresh.ru — 2025)

06 Шаблон аудита парка Windows и внедрения WSUS (ITfresh) (itfresh.ru — 2025)

Основано на официальной документации продуктов и нашей практике внедрения.