Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

5 причин перейти на IT-аутсорсинг: инженерная кухня ITfresh

Bus-фактор, мониторинг 24/7, бэкапы и SLA: как мы строим контур на Vaultwarden, Zabbix и Veeam

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Компания до 50 рабочих мест зависит от одного штатного админа: пароли и знание инфраструктуры — в его голове, бэкапы годами не проверяются, ночного мониторинга нет, время реакции нигде не зафиксировано. Его отпуск, болезнь или увольнение превращаются в простой на дни и потерю данных на недели. Разбираем, каким технологическим контуром мы снимаем эти риски за 2–4 недели передач...

Почему это важно бизнесу

- Простой офиса на 1С/файлах/почте — это оплата всего штата за дни ожидания «единственного, кто знает пароль»
- Потеря даже недели данных бухгалтерии и юристов не компенсируется деньгами — только повторной работой людей
- Непредсказуемые IT-затраты (авралы, подрядчики, замены) ломают годовой бюджет; абонентка + SLA делают строку плоской
- Проверки контрагентов и регуляторов по ИБ проваливаются без документации, бэкап-протоколов и журналов доступа

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

7.0 LTS

Ветка Zabbix у всех наших клиентов: полная поддержка вендора до июня 2027, security-фиксы — до…

Zabbix Life Cycle & Release Policy

1 мин

Интервал опроса критичных метрик через Zabbix agent 2; SMART и RAID — раз в 10 мин

наш стандарт

15 мин

TTO по критичным инцидентам в GLPI: эскалация на второго дежурного за 5 мин до дедлайна

GLPI 10.0, Service Levels

3-2-1-1-0

3 копии, 2 носителя, 1 вне офиса, 1 immutable, 0 ошибок теста восстановления

Veeam B&R 12.3

30 сут

Период immutability на hardened-репозитории Veeam: файлы нельзя изменить или удалить до истече…

Veeam B&R 12.3, Hardened Repository

4+

Минимум инженеров с доступом к коллекции клиента в Vaultwarden — bus-фактор закрыт

наш стандарт

РЕАЛИЗАЦИЯ 1 ИЗ 3

Приём инфраструктуры: паспорт, секреты, доступы

Что настраиваем

Весь контур клиента до 50 PM: AD, гипервизор, 1С, сеть, бэкапы; срок полной передачи — 2–4 недели

Как мы это делаем

1. Инвентаризация: экспорт AD (Get-ADComputer/Get-ADUser), карта сети, версии ОС и конфигураций 1С; всё — в Git как «паспорт инфраструктуры» в Markdown
2. Секреты — в self-hosted Vaultwarden: отдельная организация на клиента, коллекции «Серверы/Сеть/Сервисы», доступ минимум у 4 инженеров по ролям
3. Локальные админ-пароли рабочих станций переводим на Windows LAPS: ротация каждые 30 дней, чтение пароля — только группе инженеров через ACL на атрибут в AD
4. Смена всех унаследованных паролей и ключей на 1-й неделе; сервисные запуски — на gMSA вместо личных учёток бывших админов
5. Runbook на каждый сервис: как перезапустить, где логи, кто владелец — второй инженер подхватывает объект за 30 минут

РЕЗУЛЬТАТ

Bus-фактор снят: любой дежурный входит на любой узел без «поиска пароля в переписке». Отпуск или увольнение конкретного инженера не влияет на непрерывность — документация и секреты живут в системе с аудит-логом, а не в голове человека.

КЛЮЧЕВОЙ НЮАНС

Ключевое — смена унаследованных секретов до начала боевого дежурства: пока жив пароль бывшего админа, ответственность размыта. По доке Microsoft сверяем политику ротации Windows LAPS и права на атрибут msLAPS-…

РЕАЛИЗАЦИЯ 2 ИЗ 3

Мониторинг 24/7 на Zabbix 7.0 LTS

Что настраиваем

Все серверы и сетевые узлы клиента: Windows/Linux, гипервизор, 1С/SQL, RAID и SMART, сертификаты, бэкап-джобы

Как мы это делаем

1. Ставим Zabbix agent 2, вешаем штатные шаблоны «Windows by Zabbix agent» и «Linux by Zabbix agent»; ключевые item — с интервалом 1m
2. Диски — шаблон «SMART by Zabbix agent 2»: LLD сам находит HDD/SSD/NVMe, требуется smartmontools 7.1+ и sudo-права agent 2 на smartctl
3. Триггеры: свободное место <15% (warning) и <5% (high), CPU >90% за 5 мин, служба 1С/SQL остановлена; пороги задаём макросами {$...} на уровне хоста
4. Алерты — штатный media type Telegram (webhook): step 1 дежурному, через 10 мин без ack — step 2 старшему инженеру
5. SSL-сертификаты — item web.certificate.get в agent 2, триггер за 14 дней до истечения

РЕЗУЛЬТАТ

Инциденты класса «диск сыпется», «бэкап не прошёл», «место кончается» ловим за дни и недели до отказа. Дежурный получает алерт в Telegram через 1–2 минуты после срабатывания триггера — ночью и в выходные тоже, без участия клиента.

КЛЮЧЕВОЙ НЮАНС

Порог — не догма: 15% свободного места на файловом сервере — норма, а на диске журналов SQL — уже поздно. Поэтому пороги выносим в пользовательские макросы хоста и не правим сам шаблон — иначе ломается апгрейд.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Контур бэкапов и SLA: Veeam 12.3 + GLPI 10.0

Что настраиваем

Резервное копирование всех ВМ и физических серверов + сервис-деск с измеримым SLA, зашитым в договор

Как мы это делаем

1. Veeam B&R 12.3: джобы по схеме 3-2-1-1-0, GFS-ретенция (14 дней + 4 недели + 12 месяцев), окно бэкапа ночью — вне регламентных заданий 1С
2. Offsite-копия — на Linux hardened repository (XFS + fast clone): immutability 30 суток, подключение под непривилегированной учёткой по single-use credentials (root…
3. SureBackup: еженедельный автозапуск ВМ из бэкапа в изолированной сети с heartbeat- и ping-тестами и проверкой служб — восстановимость доказана протоколом, а не пред…
4. Заявки — GLPI 10.0: SLA с TTO/TTR по 4 категориям, уровень эскалации срабатывает за 30 мин до дедлайна (переназначение + приоритет High)

РЕЗУЛЬТАТ

Клиент получает не обещание, а измеримый контур: отчёт Veeam по каждой джобе, протокол SureBackup и статистику SLA из GLPI ежемесячно. Нарушили TTR по критичному инциденту — минус 10% абонентки автоматически из следующего счёта.

КЛЮЧЕВОЙ НЮАНС

Период immutability считаем от цикла полного бэкапа с запасом, а не «на глаз». И проверяем, что репозиторий вне домена и недоступен по SMB — иначе шифровальщик с правами домен-админа дотянется и до него.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Пароли в голове одного админа**
  Классический bus-фактор. Обходим: коллекции Vaultwarden с доступом 4+ инженеров и аудит-логом обращений к каждой записи.

- ✕ **Бэкап есть, восстановления нет**
  Джоба «зелёная», а restore не проверяли годами. SureBackup еженедельно поднимает ВМ из бэкапа в изолированной сети и пишет протокол.

- ✕ **Репозиторий бэкапов в домене**
  Шифровальщик с правами домен-админа доедает и бэкапы. Держим hardened-репозиторий вне AD, SSH после развёртывания отключаем, консоль — только локальн…

- ✕ **Мониторинг без эскалации**
  Алерт улетел в общий чат и утонул. В Zabbix — операции по шагам: 0–10 мин дежурный, дальше старший инженер, затем руководитель.

- ✕ **Обновления сразу на прод**
  Апдейт платформы 1С или гипервизора без стенда. Сначала тестовый стенд и сверка release notes, потом прод в согласованное окно.

- ✕ **SLA без измерения**
  Цифры в договоре есть, считать нечем. TTO/TTR фиксирует GLPI автоматически с момента регистрации заявки — спорить не о чем.

- ✕ **Общий пароль локального админа**
  Один пароль на все PC — готовое горизонтальное перемещение атакующего. Windows LAPS: уникальный пароль на машину, ротация 30 дней.

- ✕ **Правка шаблонов Zabbix «в лоб»**
  Изменённый штатный шаблон ломается при апгрейде сервера. Пороги задаём только макросами {$…} на уровне хоста или группы.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Все секреты — в менеджер паролей с доступом минимум двух человек
- Zabbix agent 2 на все серверы, алерты в Telegram дежурному
- Ежедневный бэкап с копией вне офиса и ежемесячным тестом восстановления

НОРМАЛЬНО

- Vaultwarden self-hosted + Git-паспорт инфраструктуры по каждому клиенту
- Zabbix 7.0 LTS: SMART, RAID, службы 1С/SQL, сертификаты; эскалация по шагам
- Veeam 12.3: GFS-ретенция + offsite-копия, ежедневный отчёт по джобам
- GLPI с SLA (TTO/TTR) и автоэскалацией за 30 мин до дедлайна

ХОРОШО

- Hardened repository с immutability 30 суток, узел вне домена
- SureBackup: автоматическая верификация восстановимости еженедельно
- Windows LAPS + gMSA, tier-модель административного доступа
- Тестовый стенд под обновления 1С и гипервизора перед каждым прод-апдейтом

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Сможет ли второй специалист войти на любой ваш сервер, если основной админ недоступен сутки?
- [ ] Хранятся ли пароли в менеджере с аудитом доступа, а не в Excel-файле или переписке?
- [ ] Есть ли актуальная схема инфраструктуры, обновлявшаяся за последние 3 месяца?
- [ ] Проверялось ли восстановление из бэкапа за последний месяц — с протоколом, а не «на словах»?
- [ ] Есть ли копия бэкапов, которую нельзя удалить даже с правами администратора домена?
- [ ] Узнаете ли вы об умирающем диске или упавшем бэкапе в субботу ночью — и кто получит алерт?
- [ ] Зафиксированы ли в договоре время реакции и решения по категориям с финансовой ответственностью?
- [ ] Ротируются ли локальные админ-пароли рабочих станций автоматически (LAPS)?
- [ ] Обновляются ли 1С и гипервизор через тестовый стенд, а не сразу в прод?

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 и приём инфраструктуры за 2–4 недели: паспорт в Git, секреты в Vaultwarden, смена унаследованных паролей
- Разворачиваем мониторинг Zabbix 7.0 LTS с дежурной сменой 24/7 и эскалацией алертов в Telegram
- Строим контур бэкапов Veeam 3-2-1-1-0 с hardened-репозиторием и еженедельным SureBackup
- Подключаем сервис-деск с SLA и финансовой ответственностью: TTO 15 мин по критичным инцидентам
- Гибридная схема со штатным админом: он — хелпдеск на месте, мы — серверы, безопасность и проекты

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 Zabbix 7.0 LTS Documentation + Life Cycle & Release Policy (zabbix.com — 7.0 LTS)

02 Шаблон «SMART by Zabbix agent 2» (smartmontools 7.1+) (zabbix.com — 7.0)

03 Veeam B&R User Guide — Hardened Repository (helpcenter.veeam.com — 12.3)

04 GLPI Documentation — Service Levels (SLA/OLA, эскалации) (glpi-project.org — 10.0)

05 Windows LAPS Overview (политики ротации, ACL атрибутов) (learn.microsoft.com — 2025)

06 Bitwarden — Organizations & Collections (bitwarden.com — 2026)

07 Наш шаблон «Паспорт инфраструктуры клиента» (Git, Markdown) (itfresh.ru — v3)

Основано на официальной документации продуктов и нашей практике внедрения.