Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Интегратор исчез: как мы перехватываем проект клиента

Пошаговый перехват контроля над AD, доступами и мониторингом за 9 инженерных дней

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

К нам обращается компания, чей подрядчик пропал: пароль Domain Admin утерян, VPN и доступы подрядчика ещё живы, бэкап не проверен, домен и облака оформлены на чужое ИП, а сертификат кассы истекает через считанные дни. Пока контроль не вернули, любой сбой единственного DC или истёкший сертификат останавливает работу офиса, а бывший инженер сохраняет вход в инфраструктуру.

Почему это важно бизнесу

- Отказ единственного контроллера домена парализует вход всех сотрудников в офис на сутки и дольше
- Истёкший сертификат кассы останавливает отправку чеков в ОФД — торговля встаёт
- Живые доступы ушедшего подрядчика — прямой риск утечки данных и саботажа
- Непроверенный бэкап при аварии означает потерю данных и недели простоя
- Домен и облачный tenant на чужом юрлице можно потерять безвозвратно при конфликте

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

2 DC

Минимум контроллеров домена: отказ одного не должен останавливать вход в офис

наш стандарт

24 ч

Окно заморозки периметра и полной инвентаризации активов в день звонка

наш стандарт

x2

Двойной сброс пароля KRBTGT с паузой на репликацию — отзыв всех Kerberos-билетов

по докам Microsoft

14 дн

Порог {$CERT.EXPIRY.WARN} до истечения сертификата, алерт уходит в Telegram

Zabbix 7.0

7.0 LTS

Версия Zabbix: agent2 с плагином WebCertificate, ключ web.certificate.get

по докам Zabbix

false

SIGNUPS_ALLOWED в Vaultwarden: публичная регистрация закрыта на сервере клиента

по докам Vaultwarden

РЕАЛИЗАЦИЯ 1 ИЗ 3

Возврат контроля над Active Directory

Что настраиваем

Один DC на Windows Server 2019 под Hyper-V, пароль Domain Admin утерян, офис 25-50 PM

Как мы это делаем

1. Сброс локального админа гипервизора с PE-носителя SystemRescue: монтируем том, chntpw правит SAM Hyper-V-хоста
2. На гостевом DC офлайн-подменяем Utilman.exe на cmd.exe; при загрузке Win+U даёт консоль LocalSystem, net user сбрасывает пароль доменного администратора
3. Через восстановленный Domain Admin поднимаем второй DC: Install-ADDSDomainController, роли AD DS + DNS
4. Проверяем сходимость репликации: repadmin /replsummary и repadmin /showrepl, при нужде переносим FSMO через ntdsutil roles
5. Двойной сброс KRBTGT с паузой ≥10 ч на репликацию — отзываем все ранее выпущенные Kerberos-билеты

РЕЗУЛЬТАТ

Контроль над каталогом возвращается за смену: доменные пароли под нами, второй DC исключает простой офиса при отказе единственного контроллера, а двойная ротация KRBTGT закрывает возможность входа по ранее выпущенным Kerberos-билетам подрядчика.

КЛЮЧЕВОЙ НЮАНС

Если офлайн-подмену Utilman блокирует BitLocker или Secure Boot, план B — вход в DSRM (bcdedit /set safeboot dsrepair) с офлайн-сброшенным DSRM-паролем и восстановление доменного админа стартовым скриптом от L...

РЕАЛИЗАЦИЯ 2 ИЗ 3

Инвентаризация учёток и точек владения

Что настраиваем

Доменные, локальные и сервисные аккаунты + внешний контур: регистратор, почта, облака, эквайринг

Как мы это делаем

1. Выгрузка учёток: Get-ADUser -Filter * -Properties LastLogonDate,PasswordLastSet,Enabled в CSV
2. Сервисные ищем фильтром PasswordNeverExpires -eq $true, локальных админов — Invoke-Command + Get-LocalGroupMember
3. Отключаем мёртвые души с last logon >90 дней, ротируем пароли всех привилегированных и сервисных учёток
4. Строим карту владения: регистратор домена, tenant M365, Яндекс 360, эквайринг — на чьём юрлице/ИП
5. Переносим tenant и аккаунты на юрлицо заказчика по уставным документам, включаем 2FA везде

РЕЗУЛЬТАТ

Появляется полная карта: кто чем реально владеет и где остался доступ подрядчика. Привилегированные и сервисные пароли ротированы, неактивные учётки закрыты, облачные сервисы и регистратор домена переоформлены на заказчика — точка невозврата для бывшего инженера пройдена.

КЛЮЧЕВОЙ НЮАНС

Сервисные аккаунты с PasswordNeverExpires — типовая мина: смена пароля вслепую роняет службу. Сначала находим, где учётка используется (задачи, службы), готовим план смены, только потом ротируем — иначе положи...

РЕАЛИЗАЦИЯ 3 ИЗ 3

Мониторинг сертификатов и Vaultwarden у клиента

Что настраиваем

Zabbix 7.0 LTS и Vaultwarden в Docker на узле заказчика, алерты в Telegram директору и инженеру

Как мы это делаем

1. Zabbix 7.0 LTS + agent2 с плагином WebCertificate, ключ web.certificate.get по доменам и сертификату ОФД-кассы
2. Порог {$CERT.EXPIRY.WARN}=14 дн, триггер 'SSL certificate expires soon' → media type Telegram
3. Триггеры на отказ DC, незавершённый ночной бэкап и заполнение тома NAS свыше 85%
4. Vaultwarden в Docker: SIGNUPS_ALLOWED=false, ADMIN_TOKEN в виде Argon2-хеша, порт слушает 127.0.0.1
5. Перед контейнером nginx + Let's Encrypt, /admin открыт только с офисных IP; владелец хранилища — клиент

РЕЗУЛЬТАТ

Инфраструктура перестаёт быть чёрным ящиком: истечение сертификатов, падение DC и сбои бэкапа видны заранее и приходят в Telegram директору и инженеру. Пароли живут в хранилище на сервере клиента — при смене подрядчика все ключи остаются у заказчика.

КЛЮЧЕВОЙ НЮАНС

Vaultwarden держим на узле заказчика, а не в общем облаке подрядчика — это ключевой архитектурный принцип. ADMIN_TOKEN хранится как Argon2-хеш, а не открытым текстом, иначе секрет утекает в переменные окружени…

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Смена пароля сервисной учётки вслепую**
  Аккаунт с PasswordNeverExpires держит службу бэкапа или 1С; ротация без разбора роняет сервис. Сначала находим зависимости, потом меняем.

- ✕ **Единственный контроллер домена**
  Отказ одного DC парализует вход в офис на сутки. Поднимаем второй DC на отдельной ВМ и проверяем репликацию через repadmin.

- ✕ **Не отозваны Kerberos-билеты**
  После смены пароля админа старые TGT ещё живут. Нужен двойной сброс KRBTGT с паузой на репликацию, иначе вход по билету сохраняется.

- ✕ **Бэкап есть, но не проверен**
  Резервная копия без test-restore — не бэкап. Проверяем восстановление реального файла и БД, замеряем RTO до внесения в регламент.

- ✕ **Tenant и домен на ИП подрядчика**
  M365 и регистратор оформлены на чужое юрлицо — при уходе доступ 'зависает'. Переносим на заказчика по уставным документам заранее.

- ✕ **Пароли в общем хранилище подрядчика**
  Секреты в облаке интегратора — заложник при расставании. Разворачиваем Vaultwarden у клиента, наша учётка ограничена секциями.

- ✕ **VPN и remote-правила не вычищены**
  Старые L2TP/IKEv2-учётки и allow-правила с IP подрядчика остаются входом. Отключаем сертификаты, закрываем Winbox/SSH из интернета.

- ✕ **Мониторинг без канала доставки**
  Zabbix ставят, но алерты никто не видит. Настраиваем media type Telegram в группу директора и инженера и тестируем доставку.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Сменить все привилегированные пароли и отозвать VPN-учётки подрядчика в первые 24 ч
- Поднять второй контроллер домена, проверить репликацию repadmin /replsummary
- Проверить бэкап test-restore хотя бы за прошлые сутки
- Перевести регистратор домена и облачные tenant на юрлицо заказчика

НОРМАЛЬНО

- Zabbix 7.0 с алертами в Telegram: сертификаты, отказ DC, бэкап, заполнение NAS
- Двойной сброс KRBTGT, отключение неактивных учёток старше 90 дней
- Vaultwarden у клиента: SIGNUPS_ALLOWED=false, nginx + Let's Encrypt, /admin по IP
- Включить 2FA на почте, CRM, эквайринге и панели регистратора домена

ХОРОШО

- Wiki в BookStack: сетевая схема, реестр доступов, регламенты и SLA
- Порог {$CERT.EXPIRY.WARN}=14 дн и plan of action на типовые аварии
- Пункт договора о передаче дел за 30 рабочих дней с ежемесячной сверкой паролей
- Ротация секретов и API-токенов сторонних сервисов строго с нуля

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Сменены пароли Domain Admin и всех учёток с правами уровня администратора домена?
- [ ] Отозваны VPN-сертификаты и L2TP/IKEv2-учётки подрядчика, закрыты Winbox/SSH из интернета?
- [ ] В домене минимум два контроллера, репликация сходится по repadmin /replsummary?
- [ ] Выполнен двойной сброс KRBTGT с паузой на репликацию между сбросами?
- [ ] Бэкап проверен test-restore, известен RTO восстановления файла и БД?
- [ ] Регистратор домена и облачные tenant оформлены на юрлицо заказчика?
- [ ] Развёрнут Vaultwarden на сервере клиента, регистрация закрыта, /admin по офисным IP?
- [ ] Настроен Zabbix с алертами в Telegram на сертификаты, отказ DC и сбой бэкапа?
- [ ] Отключены неактивные учётки и разобраны сервисные аккаунты с PasswordNeverExpires?
- [ ] Есть актуальная Wiki с сетевой схемой, реестром доступов и регламентами?

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).

- Выезжаем в день звонка: заморозка периметра, инвентаризация активов и карта владения за 24 ч
- Возвращаем контроль над AD: офлайн-сброс доменного админа, второй DC, ротация KRBTGT и привилегированных учёток
- Переоформляем домен, tenant M365 и облака на заказчика, ротируем API-токены сторонних сервисов
- Разворачиваем Vaultwarden и Zabbix с Telegram-алертами на узле клиента
- Пишем Wiki, регламенты и SLA, закрепляем передачу дел отдельным пунктом договора

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 Reset the Directory Services Restore Mode admin password (ntdsutil) (learn.microsoft.com — 2025)

02 AD Forest Recovery: сброс пароля учётной записи krbtgt (learn.microsoft.com — 2025)

03 Install-ADDSDomainController и мониторинг репликации repadmin (learn.microsoft.com — 2025)

04 Monitor website certificates with Zabbix agent 2 (WebCertificate) (zabbix.com — 7.0)

05 Zabbix media type Telegram и настройка оповещений (zabbix.com — 7.0)

06 Vaultwarden configuration: ADMIN_TOKEN, SIGNUPS_ALLOWED (github.com — 1.x)

07 Шаблон приёма дел и реестра доступов ITfresh (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.