Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Ручное управление Active Directory: цена одной забытой учётки

Почему уволенные с «живым» доступом и «мёртвые» учётки стоят бизнесу миллионы

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

В компаниях до 50 рабочих мест учётками Active Directory управляют вручную и «по памяти»: сотрудник уволился, а его логин, VPN и почта живут ещё недели. «Мёртвые» учётки копятся годами, состав админ-групп никто не проверяет, GPO не бэкапятся. Каждая такая мелочь — открытая дверь для бывшего сотрудника или взломщика ко всей сети, 1С и данным клиентов.

Почему это важно бизнесу

- Уволенный с «живым» доступом может остановить бизнес: одной ночной сессии под неотозванной учёткой хватает, чтобы удалить серверы, почту и данны…
- AD — сердце сети: компрометация домена открывает атакующему путь ко всем ресурсам сразу, а падение контроллеров останавливает всех сотрудников.
- Утечка через забытую учётку — штраф по 152-ФЗ до 15 млн ₽, при повторной утечке — оборотный штраф до 3% годовой выручки.
- Ручная рутина съедает часы ИТ-специалиста и порождает ошибки: лишние права, опечатки, незаблокированные учётки.

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

90 дней

порог неактивности, по которому Search-ADAccount -AccountInactive -TimeSpan «90.00:00:00» выде…

Регламент аудита AD ITfresh, 2026

~14 дней

задержка репликации атрибута lastLogonTimestamp — для точного «последнего входа» опрашиваем la…

learn.microsoft.com, 2025

~10 часов

конвергенция KDS root key после Add-KdsRootKey, прежде чем удаётся создать gMSA через New-ADSe…

learn.microsoft.com, 2025

1 день

целевой SLA блокировки: Disable-ADAccount плюс отзыв VPN и почты по событию из HR в день ухода…

Регламент offboarding ITfresh, 2026

12

рабочих PowerShell-скриптов в нашем наборе автоматизации AD: onboarding, offboarding, аудит не…

Методология ITfresh, 2026

раз в неделю

минимальная частота Backup-GPO всех политик домена в версионируемый каталог плюс системный бэк…

Регламент бэкапа AD ITfresh, 2026

РЕАЛИЗАЦИЯ 1 ИЗ 3

Доступ не отозвали — под неотозванной учёткой удалили тестовую ферму

Что настраиваем

Обобщённый кейс: ИТ-подрядчик, тестовая среда

Как мы это делаем

1. Администратора тестовой среды увольняют, но его учётные данные и VPN никто не отзывает
2. Несколько месяцев бывший сотрудник удалённо заходит в сеть и отлаживает скрипт удаления
3. За одну ночь скрипт уничтожает почти две сотни виртуальных серверов тестового контура
4. Восстановление растягивается на месяцы; вход вычисляют по журналам и IP-адресу

РЕЗУЛЬТАТ

Причиной стал не «гениальный хакер», а отсутствие простой процедуры: учётные данные уволенного администратора оставались рабочими несколько месяцев.

КЛЮЧЕВОЙ НЮАНС

Блокировка учётки должна происходить в день увольнения автоматически — Disable-ADAccount по событию из HR, а не «когда админ вспомнит». Регулярный Search-ADAccount -AccountInactive ловит то, что пропустили.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Инсайдер массово удалил учётки в облачном каталоге

Что настраиваем

Обобщённый кейс: миграция в облачный каталог, внешний консультант

Как мы это делаем

1. Внешний консультант мигрирует компанию в облачный каталог; после конфликта его отстраняют, но доступ не отзывают
2. Спустя месяцы он входит в систему и удаляет большую часть учётных записей сотрудников
3. Два дня компания полностью стоит: не работают почта, календари, документы и телефония
4. Прямые убытки и недели устранения последствий

РЕЗУЛЬТАТ

Полная остановка бизнеса: сотрудники не могли войти в системы, клиенты не могли дозвониться, руководство не могло даже оценить масштаб.

КЛЮЧЕВОЙ НЮАНС

Доступ подрядчиков и консультантов — отдельная зона риска: выдавать на срок задачи через accountExpires с автоотзывом, а действия привилегированных учёток — журналировать и контролировать.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Уволенный инженер снёс виртуальные машины облачного сервиса

Что настраиваем

Обобщённый кейс: облачная инфраструктура, уволенный инженер

Как мы это делаем

1. Инженер увольняется, но его доступ к облачной инфраструктуре остаётся действующим
2. Через несколько месяцев он запускает код, удаляющий сотни виртуальных машин продакшн-сервиса
3. Тысячи корпоративных аккаунтов недоступны, восстановление занимает до двух недель
4. Прямые потери — миллионы, плюс компенсации клиентам

РЕЗУЛЬТАТ

Даже у крупного вендора процесс отзыва доступа дал сбой: облачные учётные данные уволенного никто не деактивировал несколько месяцев.

КЛЮЧЕВОЙ НЮАНС

Отзыв доступа — это не только AD: облака, VPN, SaaS и API-ключи должны отключаться единым offboarding-процессом по чек-листу. Что не автоматизировано — рано или поздно будет забыто.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Увольнение без отзыва доступа**
  Учётку блокируют «когда вспомнят»: логин, VPN и почта уволенного живут днями и неделями — готовое окно для мести или взлома.

- ✕ **«Мёртвые» учётки копятся годами**
  Аккаунты давно ушедших сотрудников остаются активными; злоумышленник входит через них незаметно — жаловаться на взлом некому.

- ✕ **Никто не следит за админ-группами**
  Состав Domain Admins разрастается «временными» правами, которые не забирают. Каждый лишний админ — вектор захвата всего домена.

- ✕ **Задачи от имени Domain Admin**
  Скрипты и сервисы работают под доменным админом с вечным паролем вместо gMSA — утечка одного пароля отдаёт весь домен.

- ✕ **GPO без резервных копий**
  Ошибочное изменение групповой политики кладёт работу всего офиса, а откатиться некуда: без Backup-GPO восстановление растягивается на дни.

- ✕ **Скрипты падают молча**
  Автоматизация без логов и уведомлений неделями не работает, а узнают об этом по последствиям: нет бэкапа, уволенный не отключён.

- ✕ **Ручное заведение пользователей**
  Учётки создают копированием «как у коллеги» — новичок сразу получает лишние права, а опечатки ломают почту и доступ к 1С.

- ✕ **Подрядчики с бессрочным доступом**
  Внешним специалистам выдают учётки без accountExpires и не отключают после проекта — так и случаются самые крупные инсайдерские инциденты.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Чек-лист увольнения: Disable-ADAccount и сброс сессий, отзыв VPN, почты и SaaS в ден…
- Ежеквартальный аудит: Search-ADAccount -AccountInactive -TimeSpan «90.00:00:00» и Ge…
- Backup-GPO всех политик и системный бэкап состояния AD минимум раз в неделю

НОРМАЛЬНО

- Скрипты on/offboarding по заявке из HR (New-ADUser / Disable-ADAccount) — без ручных…
- Запуск задач под gMSA (New-ADServiceAccount) с автосменой пароля, а не под Domain Ad…
- Автоотчёты: неактивные учётки, привилегированные группы, репликация DC (Get-ADReplic…
- Логи и алерты (почта/Telegram) на каждый автоматический скрипт

ХОРОШО

- Полный IAM-процесс: права по ролям, доступ подрядчикам через accountExpires со сроко…
- Мониторинг изменений AD с алертами на критичные группы (Domain Admins, Enterprise Ad…
- Регулярные учения по восстановлению AD и GPO (Restore-GPO) из резервной копии
- Tiering-модель: отдельные админ-учётки Tier 0/1/2 для задач разного уровня

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Учётки уволенных блокируются в день увольнения через Disable-ADAccount, а не «по памяти» админа?
- [ ] Вы знаете точный состав Domain Admins и других привилегированных групп на сегодня (Get-ADGroupMember)?
- [ ] В домене нет активных учёток без входа более 90 дней (Search-ADAccount -AccountInactive)?
- [ ] Доступ подрядчиков ограничен через accountExpires и отключается после проекта?
- [ ] Групповые политики резервируются через Backup-GPO, и вы проверяли Restore-GPO из копии?
- [ ] Автоматические задачи работают под gMSA, а не под учёткой доменного администратора?
- [ ] Вы получите уведомление, если ночной скрипт или бэкап не отработал?
- [ ] Отзыв доступа покрывает всё: AD, VPN, облака, 1С и SaaS — по единому чек-листу?

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).

- Бесплатный аудит домена AD: «мёртвые» учётки, лишние админы, состояние репликации и бэкапов
- Внедрение автоматизации onboarding/offboarding, аудита и Backup-GPO за 5–10 рабочих дней
- Настройка мониторинга: отчёты и алерты в почту и Telegram о сбоях и изменениях в домене
- Сопровождение: регулярный аудит прав, привилегированных групп и парольных политик

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 Search-ADAccount (ActiveDirectory) — поиск неактивных и отключённых учёток… (learn.microsoft.com — 2025)

02 Disable-ADAccount и Enable-ADAccount (ActiveDirectory) — блокировка/разбло… (learn.microsoft.com — 2025)

03 Backup-GPO и Restore-GPO (GroupPolicy) — резервное копирование и откат гру… (learn.microsoft.com — 2025)

04 Групповые управляемые сервисные учётные записи (gMSA): Add-KdsRootKey, New… (learn.microsoft.com — 2025)

05 Get-ADGroupMember (ActiveDirectory) — контроль состава привилегированных г… (learn.microsoft.com — 2025)

06 Get-ADReplicationPartnerMetadata (ActiveDirectory) — контроль репликации м… (learn.microsoft.com — 2025)

07 Регламент offboarding и аудита AD ITfresh — набор из 12 рабочих PowerShell… (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.