Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Онбординг и оффбординг: наш регламент доступов

Как мы заводим и отзываем сотрудника в AD, почте, VPN, 1С и BitLocker

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Заказчик до 50 мест живёт без IT-директора: приказ о приёме и увольнении ходит между HR и бухгалтерией, а мы узнаём постфактум. Итог — либо новичок первый день сидит без 1С и почты, либо уволенный неделями держит живую учётку, активные веб-сессии, VPN-сертификат и ключ BitLocker. Мы закрываем это регламентом: HR-триггер, единый чеклист, PowerShell и ежемесячная сверка.

Почему это важно бизнесу

- Доступ уволенного к CRM и 1С — это утечка клиентской базы и цен закупки
- Простой новичка без 1С и почты оплачивается компанией как рабочий день
- Права «как у коллеги» копят избыточный доступ и ломают разделение обязанностей
- Без акта приёма-передачи технику и токен ЭЦП юридически не вернуть
- Отсутствие журнала выдачи доступов делает проверку ИБ и аудит недоказуемыми

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

Т-1 день

заявка от HR на онбординг: ФИО, должность, отдел, дата выхода, список систем

Регламент ITfresh

4 часа

наш SLA на полный онбординг рабочего места до первого рабочего дня

SLA ITfresh

2 часа

SLA на блокировку всех учёток при плановом увольнении с момента заявки

SLA ITfresh

30 минут

SLA на аварийный оффбординг при конфликтном уходе: AD, почта, VPN, RDP

SLA ITfresh

90 дней

срок хранения архива почты и профиля уволенного до необратимого удаления

Регламент ITfresh

1 раз/мес

сверка Search-ADAccount -AccountDisabled и списка HR: спящие и осиротевшие учётки

Регламент ITfresh

РЕАЛИЗАЦИЯ 1 ИЗ 3

Плановый оффбординг менеджера с доступом в CRM и 1С

Что настраиваем

Наш клиент: торговая компания, 38 рабочих мест, домен на Windows Server 2019, почта в облаке, 1С:УТ на сервере предприятия

Как мы это делаем

1. Т-1: HR закрывает форму в тикет-системе, задача с чеклистом падает на дежурного инженера
2. День X, 10:00: Disable-ADAccount, Set-ADUser -Description с датой и номером заявки, Set-ADAccountPassword -Reset
3. 10:15: снятие из групп безопасности через Remove-ADGroupMember, перенос в OU Disabled, блок наследования
4. 10:30: Revoke-MgUserSignInSession — отзыв refresh-токенов и cookie; методы MFA снимаем отдельными командлетами
5. 17:00: приём техники по акту, отзыв VPN-сертификата в CRL, ящик конвертирован командой Set-Mailbox -Type Shared

РЕЗУЛЬТАТ

Refresh-токены и cookie отозваны к обеду, выданные access-токены доживают свой срок (до часа) — поэтому блокировка в AD идёт первой. Почта и файлы остались у руководителя через shared-ящик. Учётку не удаляли: отключённый объект в OU Disabled держит SID в ACL и нужен для аудита.

КЛЮЧЕВОЙ НЮАНС

Отключать, а не удалять. Удалённый объект AD рвёт связи SID в ACL и владельцах, и восстановление прав к общим папкам обходится дороже, чем хранение отключённой учётки три месяца.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Аварийный оффбординг: уход в конфликте за один рабочий день

Что настраиваем

Наш клиент: производственная компания, 24 рабочих места, терминальный сервер RDS, файловый сервер с BitLocker на ноутбуках

Как мы это делаем

1. 0:00: получаем сигнал от директора, стартуем аварийный сценарий вне очереди
2. 0:05: Disable-ADAccount и Revoke-MgUserSignInSession, завершение RDS-сессии командой logoff по её ID
3. 0:12: отзыв клиентского сертификата VPN и правка правил доступа на периметре
4. 0:25: блок пользователя в 1С через администрирование кластера, ротация общих паролей в менеджере паролей
5. 1:30: выгрузка журналов входов и почтового аудита за 30 дней в отдельное хранилище

РЕЗУЛЬТАТ

Полный отзыв доступа занял менее получаса, ещё час ушёл на сбор доказательной базы. Ключи восстановления BitLocker заранее выгружались в AD через Backup-BitLockerKeyProtector, поэтому ноутбук был расшифрован и переиспользован без обращения к бывшему сотруднику.

КЛЮЧЕВОЙ НЮАНС

Аварийный сценарий должен быть написан заранее и лежать отдельным скриптом. В момент конфликта нет времени вспоминать, где ещё жили учётки и кто знал общие пароли.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Онбординг по шаблону отдела вместо копирования коллеги

Что настраиваем

Наш клиент: сервисная компания, 45 рабочих мест, четыре отдела, единый файловый сервер и 1С:Бухгалтерия

Как мы это делаем

1. Разобрали фактические права: сняли Get-ADPrincipalGroupMembership по всем и свели матрицу доступа
2. Собрали ролевые группы безопасности на отдел и заменили прямые ACL на папках группами
3. Написали скрипт New-ADUser с параметрами по отделу и Add-ADGroupMember по списку ролей
4. Ящик, RDS-профиль и пользователь 1С заводятся тем же прогоном, лицензии проверяются заранее

РЕЗУЛЬТАТ

Заведение сотрудника вместо получаса ручной работы занимает несколько минут и даёт воспроизводимый набор прав. Копирование учётки коллеги мы запретили: именно оно годами тянуло за новичком лишние группы и доступ к чужим папкам.

КЛЮЧЕВОЙ НЮАНС

Права выдаются только через группы безопасности. Прямой ACL на пользователя невозможно ни проверить одним запросом, ни корректно снять при увольнении.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Удаление учётки вместо отключения**
  SID пропадает из ACL и владельцев файлов, права на общие папки и почтовый архив приходится восстанавливать вручную.
- ✕ **Новичок создаётся копированием коллеги**
  Вместе с шаблоном переносятся лишние группы и доступы, аудит перестаёт показывать, кому и за что выдан доступ.
- ✕ **Права выданы прямым ACL на пользователя**
  Такие разрешения не видны в членстве групп и остаются жить на папках после блокировки учётной записи.
- ✕ **Блокировка без отзыва веб-сессий**
  Revoke-MgUserSignInSession гасит refresh-токены и cookie, но выданный access-токен живёт до истечения срока — обычно около часа.
- ✕ **MFA считают отозванной вместе с сессией**
  Телефон и Authenticator остаются привязаны: методы удаляются отдельно, командлетами Remove-MgUserAuthentication*Method.
- ✕ **Забытые VPN-сертификаты и RDP**
  Сертификат работает независимо от пароля домена, пока не попал в список отозванных на шлюзе.
- ✕ **Общие пароли не ротируются**
  Учётные записи банк-клиента, регистратора доменов и соцсетей знал человек лично — их надо менять в день ухода.
- ✕ **Ключи BitLocker только на устройстве**
  Без Backup-BitLockerKeyProtector в AD DS или BackupToAAD- в облаке зашифрованный ноутбук после ухода — кирпич.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Единый чеклист онбординга и оффбординга в тикет-системе или таблице
- Заявка от HR за сутки до выхода и в день подписания приказа об увольнении
- Disable-ADAccount, Set-ADAccountPassword -Reset и отзыв веб-сессий в день ухода
- Акт приёма-передачи техники с серийными номерами и токеном ЭЦП

НОРМАЛЬНО

- Ролевые группы безопасности на отдел, прямые ACL на пользователя запрещены
- Заведение через скрипт New-ADUser по шаблону отдела и Add-ADGroupMember
- Корпоративный менеджер паролей, ротация общих секретов при каждом уходе
- Set-Mailbox -Type Shared, forwarding руководителю, архив и профиль 90 дней

ХОРОШО

- HR-система как триггер: заявка автоматически порождает задачу и скрипт
- Ежемесячный отчёт Search-ADAccount и сверка с кадровым списком
- Backup-BitLockerKeyProtector в AD DS, отзыв VPN-сертификатов в CRL
- Аварийный сценарий оффбординга одним прогоном плюс выгрузка журналов входа

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Заявка HR за сутки: ФИО, должность, отдел, дата выхода, перечень систем и лицензий
- [ ] Создание учётки: New-ADUser по шаблону отдела, Add-ADGroupMember по ролевым группам
- [ ] Рабочее место: образ ОС, антивирус, BitLocker с Backup-BitLockerKeyProtector, принтеры через GPO
- [ ] Почта, RDS-профиль, пользователь 1С и роли в базе, VPN-сертификат под конкретное лицо
- [ ] Первый день: акт на технику и токен ЭЦП, NDA, регламент использования инфраструктуры
- [ ] Уход: Disable-ADAccount, Set-ADAccountPassword -Reset, перенос в OU Disabled, Remove-ADGroupMember
- [ ] Сессии: Revoke-MgUserSignInSession, снятие методов MFA отдельно, logoff RDS-сессий
- [ ] Почта: Set-Mailbox -Type Shared, forwarding руководителю, срок хранения архива 90 дней
- [ ] Периметр: отзыв VPN-сертификата в CRL, блок в 1С и CRM, ротация общих паролей
- [ ] Финал: приём техники по акту, бэкап профиля, отчёт по журналам входов за 30 дней

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).

- Опишем матрицу доступа по отделам и заменим прямые ACL ролевыми группами AD
- Соберём скрипты онбординга и оффбординга под вашу инфраструктуру и HR-процесс
- Настроим escrow ключей BitLocker, отзыв VPN-сертификатов и менеджер паролей
- Возьмём выполнение чеклистов на себя с SLA 4 часа и аварийным сценарием 30 минут
- Проведём аудит учёток и вычистим осиротевшие доступы к почте, 1С и файловым ресурсам

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 AD PowerShell: New-ADUser, Disable-ADAccount, Search-ADAccount (learn.microsoft.com — 2026)

02 AD PowerShell: Set-ADAccountPassword, Add-/Remove-ADGroupMember (learn.microsoft.com — 2026)

03 Microsoft Graph PowerShell: Revoke-MgUserSignInSession (learn.microsoft.com — 2026)

04 Microsoft Graph: методы аутентификации и удаление методов MFA (learn.microsoft.com — 2026)

05 Exchange Online: Set-Mailbox -Type Shared и правила forwarding (learn.microsoft.com — 2026)

06 BitLocker: Backup-BitLockerKeyProtector и хранение ключей в AD DS (learn.microsoft.com — 2026)

07 Администрирование пользователей и ролей информационной базы 1С (its.1c.ru — 2026)

08 Внутренний регламент онбординга и оффбординга ITfresh (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.