Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

FGPP в Active Directory: свой пароль для каждой роли

Как мы разводим требования к паролям админов, сотрудников и сервисных учёток через PSO

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

В домене одна Default Domain Policy: требования к паролю и блокировке одинаковы для бухгалтера, администратора домена и сервисной учётки 1С или SQL. Планку опускают до самого неудобного — учётки с паролем, зашитым в конфиге. Админские аккаунты защищены как рядовые, а сотрудники живут с лишними блокировками. FGPP снимает компромисс: политика цепляется к группе, а не к домену.

Почему это важно бизнесу

- Пароль администратора домена по силе равен паролю менеджера: одна подобранная учётка открывает доступ ко всем серверам и файлам
- Сервисные учётки с вечным паролем годами живут в конфигах и скриптах — их утечка не оставляет следов и не истекает
- Единая жёсткая политика на всех даёт вал блокировок и заявок в поддержку: люди пишут пароли на стикерах
- 152-ФЗ и договоры с заказчиками требуют доказуемой парольной политики для привилегированного доступа
- Без разделения политик любое ужесточение упирается в одно легаси-приложение и не проходит вовсе

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

2012+

функциональный уровень домена для FGPP; плюс RSAT: ADAC или модуль ActiveDirectory

документация AD DS

10/30/50

шаг Precedence в нашем наборе: админы 10, сервисные 30, пользователи 50, базовый 500

стандарт ITfresh

14 симв.

MinPasswordLength в PSO-Admins при PasswordHistoryCount 24 и MinPasswordAge 1 день

стандарт ITfresh

5 баллов

порог приёма пароля в Entra Password Protection: вхождение банворда — 1 балл, прочий символ — 1

док. Entra Password Protection

60 мин

период, с которым DC-агент проверяет возраст политики в sysvol и запрашивает новую

док. Entra Password Protection

0x18

код в событии 4771 (Kerberos pre-auth failed): предъявлен неверный пароль — маркер подбора

документация аудита Windows

РЕАЛИЗАЦИЯ 1 ИЗ 3

Разносим домен на четыре PSO без простоя пользователей

Что настраиваем

Офис 40–70 рабочих мест, домен AD DS, один-два контроллера Windows Server 2019/2022

Как мы это делаем

1. Снимаем исходное: (Get-ADDomain).DomainMode, Default Domain Policy и ACL на CN=Password Settings Container,CN=System
2. Создаём PSO-Baseline (Precedence 500) с ТЕКУЩИМИ параметрами домена и вешаем на Domain Users — никто ничего не замечает
3. PSO-Admins (Precedence 10): длина 14, история 24, MaxPasswordAge 30 д, MinPasswordAge 1 д, Threshold 5, Window/Duration 15 мин
4. PSO-Service (30) и PSO-Users (50) цепляем Add-ADFineGrainedPasswordPolicySubject; у всех ProtectedFromAccidentalDeletion $true
5. Проверяем Get-ADUserResultantPasswordPolicy по каждой роли и ищем учётки с пустым msDS-ResultantPSO

РЕЗУЛЬТАТ

Домен переходит на ролевые требования без единого принудительного сброса: новые правила срабатывают у пользователя при очередной смене пароля. Привилегированные учётки получают жёсткий профиль, а рядовые сотрудники — более длинный срок жизни пароля и меньше блокировок.

КЛЮЧЕВОЙ НЮАНС

Первым всегда создаём PSO-Baseline — копию действующей политики. Он ловит всех, кто не попал ни в одну целевую группу, и делает переход обратимым: снял PSO — вернулся к Default Domain Policy.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Сервисные учётки: PSO как переходный режим, gMSA как цель

Что настраиваем

Инфраструктура с 1С, SQL Server, бэкапом и печатью на доменных сервисных учётках

Как мы это делаем

1. Инвентаризация: службы и задания планировщика с доменным LogonAccount, сверка с событиями 4624 типов 4 и 5
2. Группа SVC-Accounts (Global Security) и PSO-Service: длина 24, MaxPasswordAge 0, LockoutThreshold 10, Duration и Window по 60 мин
3. Компенсация вечного пароля: Deny log on locally и через RDS, ограничение LogonWorkstations, алерты по 4625 и 4771
4. Перевод на gMSA: New-ADServiceAccount с PrincipalsAllowedToRetrieveManagedPassword, на хосте — Install-ADServiceAccount
5. Ротацию берёт на себя AD: 30 дней по умолчанию, ManagedPasswordIntervalInDays задаётся только при создании учётки

РЕЗУЛЬТАТ

Пароль, который нельзя менять по техническим причинам, перестаёт быть дырой в политике всего домена: он длинный, ограничен по местам входа и находится под наблюдением. Каждая переведённая на gMSA служба навсегда уходит из ручного учёта паролей.

КЛЮЧЕВОЙ НЮАНС

MaxPasswordAge 0 допустим только в паре с компенсирующими мерами и планом миграции. PSO для сервисных учёток — это срок, а не режим навсегда: после переезда учётка уходит из SVC-Accounts и отключается.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Проверяем стойкость паролей и ловим подбор

Что настраиваем

Домен с историей 5–10 лет, где никто не знает, у скольких людей пароль вида Qwerty12!

Как мы это делаем

1. Офлайн-аудит: копия ntds.dit из теневой копии на изолированной ВМ, Test-PasswordQuality (DSInternals) — слабые, дубли, reversible
2. GPO на DC: Audit User Account Management, Audit Logon, Audit Kerberos Authentication Service; журнал Security 196608 КБ
3. Мониторим 4723, 4724, 4740, 4767 и 4771 с кодом 0x18; по 4740 шлём алерт с именем учётки и полем Caller Computer Name
4. При лицензиях Entra ID P1/P2 — DC-агент и прокси-служба Entra Password Protection: сначала audit mode, затем enforce на всех DC
5. Итог сводим в отчёт: кто без PSO, у кого пароль старше срока, какие учётки чаще всего блокируются и откуда

РЕЗУЛЬТАТ

Появляется фактическая картина вместо предположений: список учёток со слабыми и повторяющимися паролями, источник ложных блокировок (обычно забытая сессия RDP или мобильная почта) и понятная очередь работ. Подбор виден в первые часы, а не после инцидента.

КЛЮЧЕВОЙ НЮАНС

Аудит хешей делаем только на изолированной копии базы и по письменному согласованию с владельцем: сама выгрузка — чувствительная операция, её результат хранится зашифрованным и уничтожается после работ.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **PSO пытаются привязать к OU**
  PSO применяется только к глобальным группам безопасности и объектам user. Для OU нужна теневая группа и её синхронизация по расписанию.

- ✕ **Одинаковый Precedence у двух PSO**
  На дубле Precedence командлет New-ADFineGrainedPasswordPolicy падает с ошибкой, но через ADAC дубль пройдёт: выиграет PSO с меньшим GUID.

- ✕ **«Сработает самая строгая политика»**
  Нет: применяется ровно один PSO с наименьшим Precedence, остальные игнорируются целиком. Результат проверяем Get-ADUserResultantPasswordPolicy.

- ✕ **Теневая группа заполнена вручную**
  Новый сотрудник в OU появляется, в группе — нет, и он остаётся на базовой политике. Синхронизацию OU→группа ставим задачей раз в час.

- ✕ **LockoutObservationWindow больше Duration**
  LockoutDuration не меньше окна наблюдения, иначе объект не создастся. Window 0 — блокировки не будет никогда, Duration 0 — снимет только админ.

- ✕ **Забыли про локальные учётки**
  FGPP не управляет локальными администраторами на ПК и серверах и не трогает пароль DSRM. Для локальных — Windows LAPS, для DSRM — ntdsutil.

- ✕ **ReversibleEncryptionEnabled $true**
  Включают ради одного старого приложения — и пароли группы начинают храниться в обратимо шифрованном виде. Держим $false во всех PSO без исключений.

- ✕ **Работа с PSO через RODC**
  Командлеты PSO не работают ни с контроллером только для чтения (RODC), ни со снимком AD, ни с AD LDS. В -Server указываем записываемый DC с ролью PDC.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- PSO-Baseline на Domain Users, точно повторяющий текущую Default Domain Policy
- PSO-Admins на Domain/Enterprise/Schema Admins: MinPasswordLength от 14, история 24
- ProtectedFromAccidentalDeletion $true на каждом PSO и ограниченный ACL контейнера
- Контрольная проверка Get-ADUserResultantPasswordPolicy для админа и рядового юзера

НОРМАЛЬНО

- Четыре PSO: Baseline 500, Users 50, Service 30, Admins 10 — уникальный Precedence
- Теневые группы под OU и их синхронизация задачей планировщика раз в час
- MinPasswordAge 1 день против прокрутки истории, MaxPasswordAge 30 д для админов
- Аудит 4723/4724/4740/4767 и 4771 (0x18), журнал Security размером 196608 КБ

ХОРОШО

- gMSA вместо сервисных паролей: ротация 30 дней; dMSA — на DC Windows Server 2025
- Entra Password Protection на всех DC: audit mode, затем enforce, свой стоп-лист
- Protected Users для Tier 0, MFA на VPN и RD Gateway, Windows LAPS на ПК и серверах
- Ежеквартальный отчёт: учётки без msDS-ResultantPSO, просроченные и вечные пароли

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Функциональный уровень домена не ниже Windows Server 2012, установлены ADAC или модуль ActiveDirectory?
- [ ] Права на запись в CN=Password Settings Container,CN=System проверены и никому лишнему не делегированы?
- [ ] Есть PSO-Baseline на Domain Users, повторяющий текущие параметры Default Domain Policy?
- [ ] Precedence у всех PSO уникальны и заданы кратно 10, с запасом под будущие политики?
- [ ] Все PSO привязаны к глобальным группам безопасности, а не к OU или доменно-локальным группам?
- [ ] ReversibleEncryptionEnabled $false и ProtectedFromAccidentalDeletion $true во всех PSO?
- [ ] LockoutDuration не меньше LockoutObservationWindow, порог блокировки не равен нулю?
- [ ] Список сервисных учёток известен, у каждой есть владелец и план перевода на gMSA?
- [ ] Найдены пользователи с пустым msDS-ResultantPSO и разнесены по нужным группам?
- [ ] Включены Audit User Account Management и Audit Kerberos Authentication Service, алерт по 4740?

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 домена: Default Domain Policy, действующие PSO, учётки без политики и с вечными паролями
- Проектируем и разворачиваем набор PSO под ваши роли, с базовым PSO для обратимого отката
- Собираем теневые группы под OU и автоматическую синхронизацию, чтобы политика не разъезжалась
- Переводим сервисные учётки на gMSA, локальных админов — на Windows LAPS (msLAPS-Password)
- Ставим аудит и алерты по блокировкам и подбору, отдаём регламент и передаём штатному админу

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 Configure fine grained password policies for AD DS (learn.microsoft.com — 2025)

02 New-ADFineGrainedPasswordPolicy (ActiveDirectory) (learn.microsoft.com — 2026)

03 Get-ADUserResultantPasswordPolicy (ActiveDirectory) (learn.microsoft.com — 2026)

04 Microsoft Entra Password Protection для AD DS (learn.microsoft.com — 2025)

05 Audit Kerberos Authentication Service, событие 4771 (learn.microsoft.com — 2025)

06 Manage Group Managed Service Accounts (AD DS) (learn.microsoft.com — 2025)

07 Windows LAPS overview (learn.microsoft.com — 2025)

08 Шаблон ITfresh: набор PSO и чек-лист приёмки домена (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.