Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Групповые политики Active Directory: порядок, который спасает

Почему неуправляемый домен Windows — главный риск для офиса и что настроить в первую очередь

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Домен Active Directory есть почти в каждом офисе, но годами живёт «как установили»: безымянные политики, слабые пароли, ноутбуки без шифрования, любой софт запускается откуда угодно. Пока всё работает, проблемы не видно. Но домен — единый пульт управления всеми ПК компании: захватив его, атакующий за минуты раздаёт шифровальщик на весь парк, и бизнес встаёт на недели.

Почему это важно бизнесу

- Захват домена = захват всего: атакующий разом получает все компьютеры, серверы, файлы и учётные записи компании
- Простой после шифровальщика измеряется неделями: стоят продажи, бухгалтерия, почта и 1С, клиенты уходят к конкурентам
- Потерянный ноутбук без шифрования — утечка персональных данных: с 2025 года штрафы по 152-ФЗ выросли до десятков миллионов рублей
- Хаос в политиках — скрытый налог: каждая диагностика «почему не работает» съедает дни работы администратора

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

1 GPO

одной вредоносной групповой политики с захваченного контроллера хватает, чтобы отключить антив…

14

символов — минимальная длина пароля в нашем базовом наборе GPO; совпадает с рекомендацией Micr…

10

неверных вводов — порог блокировки учётной записи по базовому шаблону Microsoft; без него паро…

192 МБ

рекомендованный размер журнала «Безопасность» (196608 КБ); стандартные 20 МБ затираются за сут…

20

групповых политик в нашем базовом наборе для офиса: пароли, BitLocker, AppLocker, аудит, отклю…

2–3 дня

занимает аудит AD и GPO по нашей методологии — от инвентаризации политик до готового плана раб…

РЕАЛИЗАЦИЯ 1 ИЗ 3

Шифровальщик через одну групповую политику

Что настраиваем

Домен Active Directory офиса на 30–50 рабочих мест, один-два контроллера

Как мы это делаем

1. Атакующий получает права администратора домена через слабый пароль или устаревший протокол аутентификации
2. С контроллера создаётся одна GPO: она отключает Microsoft Defender и заводит задание в планировщике
3. При очередном применении политик задание запускает шифровальщик сразу на всех ПК домена
4. Весь парк зашифрован за минуты — без ручного обхода машин и без единого клика оператора

РЕЗУЛЬТАТ

Механизм централизованного управления, созданный для защиты, доставляет вредонос на каждый компьютер быстрее, чем администратор успевает среагировать. Без изолированного бэкапа AD и данных восстановление — недели.

КЛЮЧЕВОЙ НЮАНС

Контролируйте изменения GPO и права на контроллерах: новая политика должна появляться редко, осознанно и с оповещением ответственных. Аудит создания и изменения GPO включается штатной политикой аудита.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Потерянный ноутбук без BitLocker = готовая утечка

Что настраиваем

Рабочий ноутбук сотрудника с доступом к 1С, почте и клиентской базе

Как мы это делаем

1. Ноутбук теряется или его крадут — пароль входа в Windows атакующему не нужен
2. Диск вынимается и подключается к другому компьютеру как обычный накопитель
3. Без шифрования тома все файлы, кэш почты и локальные базы читаются напрямую
4. Персональные данные и коммерческая информация утекают целиком

РЕЗУЛЬТАТ

Пароль входа в Windows защищает только от входа в систему, но не от чтения диска на другом компьютере. Без BitLocker утерянный ноутбук — это выданная наружу клиентская база и штраф по 152-ФЗ.

КЛЮЧЕВОЙ НЮАНС

BitLocker на всех ноутбуках доменной политикой, ключи восстановления — в AD DS (GPO «Store BitLocker recovery information in AD DS»), чтобы не потерять доступ к собственным дискам.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Default Domain Policy как свалка настроек

Что настраиваем

Домен, который годами вёлся «как установили», без инвентаризации GPO

Как мы это делаем

1. Все настройки складываются в одну Default Domain Policy без документации
2. Рядом копятся политики «test», «новая», «не удалять!» без владельцев
3. Любое изменение бьёт по всему домену непредсказуемо
4. Диагностика «почему не работает» растягивается на дни ручного разбора

РЕЗУЛЬТАТ

Неуправляемый набор GPO — скрытый налог на каждую задачу администратора и слепая зона для безопасности: в этом шуме вредоносную политику никто не замечает.

КЛЮЧЕВОЙ НЮАНС

Инвентаризация: у каждой GPO — понятное имя, назначение и владелец. В Default Domain Policy — только парольная политика и Kerberos, остальное — в отдельные адресные политики на OU.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Всё свалено в Default Domain Policy**
  Сотни настроек в одной политике без документации: любое изменение непредсказуемо, диагностика растягивается на дни

- ✕ **GPO без понятных имён и владельцев**
  Политики «test», «новая», «не удалять!» копятся годами; никто не помнит, что они делают, и боится их трогать

- ✕ **Нет блокировки учётных записей**
  Пароль можно перебирать бесконечно; без порога блокировки один слабый пароль сдаёт весь домен

- ✕ **Ноутбуки без шифрования диска**
  Утерянный или украденный ноутбук читается простым снятием диска — готовая утечка персональных данных и клиентской базы

- ✕ **Запуск любого софта откуда угодно**
  Без AppLocker/WDAC шифровальщик стартует из временных папок и AppData — именно так начинается большинство заражений

- ✕ **Аудит выключен, логи затираются**
  Журнал «Безопасность» стандартного размера (20 МБ) перезаписывается за сутки: после инцидента нечем восстановить картину атаки

- ✕ **Нет резервной копии AD и GPO**
  Без отдельного бэкапа AD, SYSVOL и GPO восстановление домена после атаки — недели ручной работы с нуля

- ✕ **Устаревшие протоколы не отключены**
  SMBv1, NTLMv1 и LLMNR — стандартные точки входа атакующего внутри сети; отключаются доменной политикой

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Инвентаризация GPO: у каждой политики — имя, назначение и владелец; Default Domain P…
- Блокировка учётной записи после 10 неверных попыток (базовый шаблон Microsoft), мини…
- Отключите SMBv1, NTLMv1 и LLMNR доменной политикой (ADMX «MS Security Guide», LAN Ma…
- Ежедневный автоматический бэкап GPO и системного состояния контроллеров домена

НОРМАЛЬНО

- BitLocker на всех ноутбуках, ключи восстановления — централизованно в AD DS
- AppLocker или WDAC: запуск программ только из Program Files и папки Windows
- Аудит входов и изменений AD, журнал «Безопасность» — от 192 МБ и выгрузка в отдельно…
- Отдельные учётные записи и более строгая парольная политика для администраторов

ХОРОШО

- Централизованный сбор логов (SIEM) с алертами на создание и изменение GPO
- Мониторинг активности на контроллерах домена и изменения прав в AD
- Регулярный внешний аудит AD и тест восстановления домена из бэкапа
- Ярусная модель админ-доступа (tiering) и Windows Defender Credential Guard

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Вы знаете, сколько групповых политик действует в вашем домене и за что отвечает каждая?
- [ ] Все ноутбуки сотрудников зашифрованы, а ключи восстановления хранятся централизованно в AD?
- [ ] Учётная запись блокируется после нескольких неверных попыток ввода пароля?
- [ ] Сотрудник НЕ может запустить на рабочем ПК произвольную скачанную программу?
- [ ] У администраторов отдельные учётные записи с более строгими требованиями, чем у пользователей?
- [ ] Есть ежедневный бэкап Active Directory, и вы проверяли восстановление из него?
- [ ] Вы узнаете в тот же день о появлении новой групповой политики или изменении прав в домене?
- [ ] Запись на USB-носители ограничена там, где обрабатываются персональные данные и финансы?
- [ ] Устаревшие протоколы (SMBv1, NTLMv1, LLMNR) в вашей сети отключены?

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 Active Directory и GPO за 2–3 дня: отчёт об уязвимостях и план работ; новым клиентам — бесплатно
- Внедрение базового набора из 20 политик: пароли, BitLocker, AppLocker, аудит, файрвол — без остановки работы
- Сопровождение домена: контроль изменений GPO, ежедневные бэкапы AD, мониторинг и реагирование
- Регулярные тесты восстановления AD из бэкапа и план действий на случай атаки шифровальщика

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

Техническая база

01 Password Policy и Account Lockout Policy — параметры безопасности Windows (learn.microsoft.com — 2024)

02 Account lockout threshold — рекомендованное значение (10) (learn.microsoft.com — 2024)

03 Disabling SMBv1 through Group Policy (ADMX «MS Security Guide») (learn.microsoft.com — 2024)

04 Network security: LAN Manager authentication level (отключение NTLMv1) (learn.microsoft.com — 2024)

05 Turn off Multicast Name Resolution (DNS Client) — отключение LLMNR (learn.microsoft.com — 2024)

06 BitLocker Group Policy settings — хранение ключей восстановления в AD DS (learn.microsoft.com — 2024)

07 AppLocker и Application Control Policies (WDAC) (learn.microsoft.com — 2024)

08 Advanced security audit policy settings — рекомендации по аудиту (learn.microsoft.com — 2024)

09 AD Forest Recovery — резервное копирование и восстановление контроллеров д… (learn.microsoft.com — 2024)

10 Windows security baselines и Security Compliance Toolkit (learn.microsoft.com — 2025)

11 Базовый набор из 20 GPO для офиса — внутренний шаблон ITfresh (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.