Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Hardening Active Directory: 12 шагов нашей методики

Как мы закрываем домен офиса до 50 PM: LAPS, krbtgt, AES-only, SMB/LDAP signing, аудит

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Домен в офисе на 30-50 мест разворачивали один раз и с тех пор не трогали: у пользователей права локального админа, пароль встроенного Administrator одинаков на всех ПК, сервисные учётки 1С и бэкапа лежат в Domain Admins, журнал Security перетирается за сутки. Компрометация одной станции превращается в захват домена за часы, а восстановление упирается в непроверенный бэкап.

Почему это важно бизнесу

- Шифровальщик с правами Domain Admin проходит все шары и базы 1С за часы: встаёт офис целиком, а не один отдел.
- Подъём домена из непроверенного бэкапа — это не четыре часа, а несколько суток простоя бухгалтерии и склада.
- Утечка базы 1С и кадровых данных — инцидент по 152-ФЗ с уведомлением регулятора в первые 24 часа.
- Без журналов и алертов взлом замечают по записке вымогателя: хронологию и объём ущерба восстановить уже нечем.
- После ухода админа его доступ живёт в сервисных учётках и в билетах Kerberos, пока ключи явно не переизданы.

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

0x18

DefaultDomainSupportedEncTypes на KDC: только AES128/AES256-SHA1, RC4 не выдаётся

по докам Kerberos KDC

20

PasswordLength в Windows LAPS: наш минимум против дефолтных 14 (потолок 64)

по докам Windows LAPS / наш стандарт

10 ч

минимальный интервал между двумя сбросами krbtgt — равен дефолтной жизни TGT

по докам AD Forest Recovery

3 / 15 мин

порог блокировки учётной записи и её длительность в базлайне Windows Server 2025

по базлайну Microsoft для Windows Server 2025

CBT = 2

LDAP server channel binding token requirements = Always плюс LDAP signing Require

по докам ADV190023 / KB4520412

24H2

с Windows 11 24H2 и Server 2025 подпись SMB обязательна по умолчанию, NTLMv1 удалён

по докам SMB security hardening

РЕАЛИЗАЦИЯ 1 ИЗ 3

Неделя 1: инвентаризация, OU-модель и Tier-0

Что настраиваем

Бухгалтерская компания, 42 рабочих места, 2 DC на Windows Server 2019, файловая роль и 1С живут на одном хосте с DC

Как мы это делаем

1. Снимаем Domain/Enterprise/Schema Admins, учётки с SPN и Search-ADAccount -AccountInactive -TimeSpan 90; список на чистку согласуем с директором.
2. Строим OU: Sotrudniki, Workstations, Servers, ServiceAccounts, PrivilegedAccounts и переводим доступы на модель AGDLP — только через группы SG_*.
3. Выносим файловый сервер и 1С с контроллера домена: на DC остаются AD DS, DNS и DHCP, остальное уезжает на отдельную виртуальную машину.
4. Разводим учётки администрирования: DA входит только на DC и jump-хост, станции обслуживаются через LAPS и отдельную учётку Tier-1.
5. Включаем AD Recycle Bin: Enable-ADOptionalFeature 'Recycle Bin Feature' (FFL 2008 R2+) — удалённый OU возвращается за минуту.

РЕЗУЛЬТАТ

Domain Admins сократили с 9 учёток до 2 — инженерная и break-glass в сейфе, 17 неактивных отключили. Файловую роль и 1С сняли с DC: компрометация шары больше не даёт доступ к NTDS.dit. Права выдаются только через группы SG_*, кадровое изменение — одна команда.

КЛЮЧЕВОЙ НЮАНС

Пока в домене нет карты «кто и где админ», любой hardening остаётся косметикой. Сначала инвентаризация и согласованный список привилегий, только потом GPO.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Неделя 2: Windows LAPS и сервисные учётные записи

Что настраиваем

Тот же офис плюс 6 серверов — 1С, файловый, RDS, СУБД, бэкап, шлюз; парк ПК на Windows 10 22H2 и Windows 11 24H2

Как мы это делаем

1. Update-LapsADSchema, затем Set-LapsADComputerSelfPermission на OU=Workstations и OU=Servers; чтение — Set-LapsADReadPasswordPermission на SG_LAPS_Readers.
2. GPO «LAPS»: BackupDirectory=2, PasswordLength=20, PasswordComplexity=4, PasswordAgeDays=30, PostAuthenticationActions=3, PostAuthenticationResetDelay=8.
3. ADPasswordEncryptionEnabled активен только при DFL 2016+; ADPasswordEncryptionPrincipal=SG_LAPS_Readers, ADEncryptedPasswordHistorySize=6 (потолок 12).
4. Сервисные учётки 1С, SQL и агентов переводим на gMSA: New-ADServiceAccount, ManagedPasswordIntervalInDays 30; KDS-ключ создаём заранее, конвергенция 10 ч.
5. dMSA держим в плане: Start-/Complete-ADServiceAccountMigration требуют DC и хост на Windows Server 2025 — до апгрейда работаем на gMSA.

РЕЗУЛЬТАТ

Пароль локального администратора уникален на каждом хосте и ротируется раз в 30 дней — боковое перемещение по одному хешу закрыто. Учётки с SPN и статичными паролями переведены на gMSA: офлайн-подбор по сервисным билетам теряет смысл, ручные смены паролей служб исчезают как класс.

КЛЮЧЕВОЙ НЮАНС

LAPS без ADPasswordEncryptionPrincipal и делегирования чтения — это пароль в атрибуте каталога: при DFL ниже 2016 шифрование не применяется и атрибут читает любой, кому дали право.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Неделя 3: протоколы, krbtgt и наблюдаемость

Что настраиваем

Тот же домен: 2 DC, 6 серверов, 42 ПК; в сети остаются МФУ и NAS, которые умеют только NTLMv2 и SMB2

Как мы это делаем

1. GPO AD-Hardening-Baseline: LmCompatibilityLevel 5 (только NTLMv2), 128-bit session security, отключение LLMNR и NetBIOS, Hardened UNC Paths на SYSVOL и NETLOGON.
2. SMB: Set-SmbServerConfiguration и -SmbClientConfiguration -RequireSecuritySignature $true, снос роли FS-SMB1, -Smb2DialectMin SMB311 на хостах WS2025.
3. LDAP: две недели читаем события 2889 на DC, затем LDAPServerIntegrity=2 и LdapEnforceChannelBinding=2; МФУ и NAS переводим на LDAPS 636.
4. Kerberos: аудит 4768/4769 по типам шифрования, чистка msDS-SupportedEncryptionTypes, затем DefaultDomainSupportedEncTypes=0x18; krbtgt дважды с паузой 10-24 ч.
5. Advanced Audit Policy с Force subcategory, журнал Security 1 ГБ, WEF-подписка на коллектор, алерты на 4625, 4740, 4768/4769 RC4, 4688, 4104, 1102.

РЕЗУЛЬТАТ

NTLM-relay и перехват через LLMNR закрыты на уровне домена, биндинги без подписи видны заранее по событию 2889 и не роняют печать и сканирование. События с DC и станций уезжают на коллектор вне домена — при инциденте есть на чём строить хронологию.

КЛЮЧЕВОЙ НЮАНС

Любой запрет протокола сначала включаем в режиме аудита на две недели: исключения в малом офисе есть всегда — МФУ, сканер, NAS или старый сервис 1С.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Passphrase в LAPS на старых ОС**
  Значения PasswordComplexity 5-8 и PassphraseLength поддерживают только 24H2 и Server 2025; Windows 10 молча откатывает политику к дефолту 4.

- ✕ **LAPS-шифрование молчит ниже DFL 2016**
  ADPasswordEncryptionEnabled включён по умолчанию, но при уровне домена ниже 2016 не применяется — пароль ложится в AD открытым атрибутом.

- ✕ **Один сброс krbtgt вместо двух**
  История паролей krbtgt равна 2: после одного сброса старый ключ ещё принимается. Второй сброс делаем не раньше чем через 10 часов.

- ✕ **RC4 выключили без аудита**
  Перед DefaultDomainSupportedEncTypes=0x18 две недели смотрим 4768/4769 и msDS-SupportedEncryptionTypes служб, иначе встают агенты 1С и МФУ.

- ✕ **Protected Users для служб**
  Учётки служб и компьютеров в этой группе не работают: входящая аутентификация падает. Для них — Authentication Policy Silos.

- ✕ **Channel binding сразу в Always**
  Сначала собираем события 2889 на DC и переводим МФУ, NAS и сканеры на LDAPS, иначе сканирование в папку и печать умирают в один день.

- ✕ **Бэкап-сервер в домене**
  Хранилище копий с доменной учёткой шифруется вместе с доменом. Держим его вне AD, с локальными учётками и без обратного доступа в сеть.

- ✕ **AppLocker без службы AppIDSvc**
  Правила не применяются, пока Application Identity не переведена в автозапуск через GPO; проверяем это до включения enforcement.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Убрать пользователей из локальных администраторов и из Domain Admins
- Windows LAPS на все ПК и серверы: PasswordLength 20, PasswordAgeDays 30
- SMB signing Required, SMB1 удалён, LLMNR и NetBIOS выключены через GPO
- System State всех DC ежесуточно на хранилище вне домена

НОРМАЛЬНО

- Advanced Audit Policy, журнал Security 1 ГБ, алерты на 4625/4740/1102
- Двойной сброс krbtgt раз в 180 дней и сразу после ухода администратора
- LDAP signing Require и channel binding Always после двух недель аудита
- Сервисные учётки на gMSA с ротацией пароля раз в 30 дней

ХОРОШО

- AES-only: DefaultDomainSupportedEncTypes 0x18 после аудита 4768/4769
- Protected Users и Authentication Policy Silos для учёток Tier-0
- WEF-коллектор вне домена, ежеквартальный аудит привилегий и SPN
- Ежеквартальное восстановление DC из бэкапа в изолированной сети

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Domain/Enterprise/Schema Admins — две учётки: инженерная и break-glass с паролем в сейфе
- [ ] Учётки с SPN переведены на gMSA либо имеют пароль длиной от 25 символов
- [ ] GPO LAPS применяется на все OU с компьютерами; выборочный Get-LapsADPassword по 5 хостам
- [ ] На DC только AD DS, DNS и DHCP; RDP к DC — с jump-хоста и только для инженерной группы
- [ ] SMB1 удалён, подпись SMB обязательна на клиенте и сервере, минимальный диалект SMB 3.1.1
- [ ] На DC нет событий 2889 за последние 14 суток — LDAP-биндингов без подписи не осталось
- [ ] krbtgt сброшен дважды за последние 180 дней, интервал между сбросами больше 10 часов
- [ ] События 4625, 4740, 4768/4769, 4688, 4104 и 1102 доходят до коллектора вне домена
- [ ] System State DC восстанавливался в изолированной сети за 90 дней, домен встал за 4 часа
- [ ] AppLocker в enforcement на ПК бухгалтерии, служба AppIDSvc в автозапуске через GPO

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).

- Проводим аудит домена и отдаём карту привилегий, SPN, устаревших учёток и путей эскалации.
- Разворачиваем Windows LAPS, gMSA и OU-модель AGDLP за 25-40 часов, без остановки офиса.
- Собираем GPO AD-Hardening-Baseline и включаем запреты протоколов поэтапно, через режим аудита.
- Ставим сбор событий на коллектор вне домена и алерты на 4625/4740/4769/1102 в Telegram.
- Ежеквартально проверяем восстановление DC из бэкапа и повторяем аудит привилегий домена.

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 Windows LAPS: Configure policy settings (learn.microsoft.com — 2025)

02 AD Forest Recovery: Reset the krbtgt password (learn.microsoft.com — 2025)

03 Detect and remediate RC4 usage in Kerberos (learn.microsoft.com — 2026)

04 SMB security hardening in Windows Server and Windows Client (learn.microsoft.com — 2025)

05 LDAP channel binding and LDAP signing requirements (KB4520412) (support.microsoft.com — 2024)

06 Protected Users, Authentication Policy Silos, gMSA и dMSA (learn.microsoft.com — 2025)

07 Audit Policy Recommendations и Security Baseline для WS2025 (learn.microsoft.com — 2025)

08 Шаблон ITfresh: GPO AD-Hardening-Baseline и чек-лист Tier-0 (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.