Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Групповые политики Windows: 10 GPO-настроек безопасности офиса

Наш типовой контур: пароли, LAPS, AppLocker, RDP/NLA, аудит и обновления по baseline Microsoft

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Типовой офис до 50 РМ живёт на дефолтных настройках Windows: пароли по 7 символов, флешки без контроля, RDP наружу, журналы не пишутся. Один подобранный пароль или заражённая флешка — и это шифровальщик, простой на неделю и восстановление из устаревших бэкапов. Мы закрываем эти векторы штатными GPO за один рабочий день, без покупки стороннего ПО.

Почему это важно бизнесу

- Перебор пароля RDP — самый частый вектор шифровальщика: простой 3–7 дней и восстановление обходятся дороже любых лицензий
- Без журналов аудита не доказать в суде увод клиентской базы сотрудником — логи должны писаться ДО инцидента
- GPO — штатный механизм Windows Pro/AD: закрытие типовых дыр не требует закупок, только день работы инженера
- Взломы идут через давно закрытые уязвимости: автообновления по расписанию убирают целый класс рисков
- Уникальные пароли локальных админов (LAPS) не дают одной заражённой машине положить всю сеть

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

14

Минимальная длина пароля — по baseline Microsoft вместо дефолтных 7; история — 24 пароля

Security baseline, SCT

10/15 мин

Порог блокировки учётной записи и её длительность: стопорит перебор, не создавая DoS-лавину

наш стандарт по SCT

30 дн

PasswordAgeDays в Windows LAPS: авторотация пароля локального админа с бэкапом в AD

по докам Windows LAPS

7–14 дн

Обкатка AppLocker в режиме «Только аудит» до включения принудительного применения

наш стандарт

30 мин

Лимит бездействующей RDP-сессии (Session Time Limits): гасим брошенные подключения

наш стандарт

192 МБ

Максимальный размер журнала Security (196608 КБ) — чтобы события аудита не затирались за сутки

Security baseline, SCT

РЕАЛИЗАЦИЯ 1 ИЗ 3

Домен: политика паролей, блокировка и Windows LAPS

Что настраиваем

Контур учётных записей: GPMC на контроллере домена, отдельные GPO на OU рабочих станций и серверов, охват — все машины домена

Как мы это делаем

1. Политика паролей в Default Domain Policy: длина 14, сложность включена, история 24 пароля, максимальный срок — по регламенту клиента
2. Политика блокировки: порог 10 попыток, длительность 15 мин, сброс счётчика 15 мин; включаем «Разрешить блокировку учётной записи администратора»
3. Windows LAPS (встроен с обновлений 04.2023): Update-LapsADSchema, Set-LapsADComputerSelfPermission на OU; в GPO — бэкап в AD, длина 24, ротация 30 дней
4. Проверка: gpresult /h на клиенте и Get-LapsADPassword -Identity <ПК> -AsPlainText под админом — пароль читается и ротируется

РЕЗУЛЬТАТ

Перебор паролей по RDP/SMB перестаёт быть рабочим вектором: 10 попыток — и учётка молчит 15 минут. Пароли локальных админов уникальны на каждой машине и меняются сами — компрометация одной PC не даёт горизонтального перемещения по сети.

КЛЮЧЕВОЙ НЮАНС

Legacy-LAPS (MSI) и встроенный Windows LAPS — разные ADMX и ключи, смешивать нельзя. Порог блокировки ставим 10, а не 3–5: при опубликованном наружу сервисе атакующий иначе устроит DoS, намеренно блокируя учёт…

РЕАЛИЗАЦИЯ 2 ИЗ 3

Контроль запуска: AppLocker вместо устаревшего SRP

Что настраиваем

PC пользователей и RDS-хосты на Windows 10/11 Pro/Enterprise и Server 2019+; SRP оставляем только на legacy-машинах

Как мы это делаем

1. Службу Application Identity (AppIDSvc) переводим в «Автоматически» через GPO: без неё правила AppLocker молча не применяются
2. Генерируем правила по умолчанию (Exe, MSI, Script) + publisher-правила на подписанный софт клиента: 1С, банк-клиенты, КриптоПро
3. Режим «Только аудит» на 7–14 дней: разбираем журнал Microsoft-Windows-AppLocker/EXE and DLL, сводим через Get-AppLockerFileInformation -EventLog
4. Переводим в Enforce: запуск из %TEMP%, %APPDATA% и Downloads запрещён по умолчанию — сценарий «скачал-запустил» умирает на старте

РЕЗУЛЬТАТ

Исполняемые файлы стартуют только из C:\Windows и C:\Program Files либо по подписи вендора. Основной канал заражения — запуск из профиля пользователя — закрыт политикой, а не антивирусной эвристикой.

КЛЮЧЕВОЙ НЮАНС

SRP объявлены deprecated и на Windows 11 22H2+ не обслуживаются — новые внедрения делаем только на AppLocker/WDAC. DLL-коллекцию включаем отдельно и осознанно: без обкатки она кладёт часть прикладного софта.

РЕАЛИЗАЦИЯ 3 ИЗ 3

RDP, съёмные носители, аудит и обновления на всём парке

Что настраиваем

Периметр и рабочие места: RDS-хост, машины бухгалтерии и директора; журналирование — на всех узлах домена

Как мы это делаем

1. RDP: требуем NLA («Require user authentication… by using NLA»), security layer SSL/TLS, лимит бездействующей сессии 30 мин; 3389 наружу закрываем, доступ через VPN
2. Носители: «Removable Disks: Deny write access» на группах риска; автозапуск — «Turn off AutoPlay» для всех дисков + Default behavior for AutoRun = Do not execute
3. Advanced Audit Policy: Logon/Logoff, Account Management, Object Access (успех+отказ), флаг SCENoApplyLegacyAuditPolicy; журнал Security — 196608 КБ
4. Обновления: Configure Automatic Updates = 4, расписание — ночь пятницы; при 30+ машинах — WSUS с тестовым кольцом из 1–2 PC
5. Контроль применения: gpupdate /force, gpresult /h report.html, auditpol /get /category:* — сверяем фактические значения с эталоном

РЕЗУЛЬТАТ

RDP перестаёт отвечать неаутентифицированным клиентам, флешка перестаёт быть каналом выноса данных, а каждый вход, создание учётки и доступ к папкам с договорами ложатся в журнал — инцидент восстанавливается по минутам.

КЛЮЧЕВОЙ НЮАНС

Legacy-политика аудита и Advanced Audit Policy конфликтуют: без «Force audit policy subcategory settings» тонкие подкатегории затираются. Фактическое состояние проверяем только через auditpol, а не по оснастке.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **SRP на Windows 11 22H2+**
  Механизм deprecated и не обслуживается: правила «вроде есть», но не применяются. Новые контуры строим на AppLocker или WDAC.

- ✕ **AppLocker без службы AppIDSvc**
  При остановленной Application Identity правила не работают вовсе. Автозапуск службы фиксируем той же GPO и мониторим её состояние.

- ✕ **Enforce без периода аудита**
  Сразу включённый белый список кладёт обновления 1С и банк-клиенты. Держим «Только аудит» 7–14 дней и разбираем журнал AppLocker.

- ✕ **Порог блокировки 3 попытки**
  При опубликованном RDP перебор чужих логинов блокирует реальных пользователей — управляемый DoS. Ставим 10/15 мин по baseline.

- ✕ **Два механизма аудита сразу**
  Legacy-категории затирают Advanced Audit Policy. Включаем SCENoApplyLegacyAuditPolicy и проверяем факт через auditpol /get.

- ✕ **GPO «не применилась»**
  Причина почти всегда — security filtering без чтения для Authenticated Users, WMI-фильтр или наследование. Диагноз — gpresult /h, не правка вслепую.

- ✕ **Забытый loopback на RDS**
  Пользовательские политики на терминальнике берутся из OU юзера, а не сервера. Включаем Loopback processing (Merge/Replace) на OU RDS-хостов.

- ✕ **Локальные админ-права у всех**
  Пользователь-админ отключит любую GPO. Забираем права, а локального администратора отдаём под Windows LAPS с ротацией.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Пароли 12–14 символов + сложность, блокировка 10/15 мин на всех машинах
- NLA на RDP включён, порт 3389 из интернета закрыт (VPN/шлюз)
- Автозапуск носителей отключён, автообновления по расписанию включены

НОРМАЛЬНО

- Домен AD: политики через GPMC по OU, контроль применения gpresult
- Windows LAPS: уникальные пароли локальных админов, ротация 30 дней
- Запрет записи на съёмные диски + аудит входов и учёток (успех/отказ)
- AppLocker в режиме «Только аудит» на пилотной группе машин

ХОРОШО

- AppLocker в Enforce: запуск только из системных папок и по подписи
- Advanced Audit Policy + централизованный сбор событий (WEF/Wazuh)
- WSUS с тестовым кольцом и отложенной раскаткой обновлений
- Security baseline (SCT + LGPO.exe) как эталон, сверка раз в квартал

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Минимальная длина пароля не меньше 12 символов и включены требования сложности?
- [ ] Учётная запись блокируется после 10 неудачных попыток входа?
- [ ] Порт 3389 недоступен из интернета, а NLA на RDP включён?
- [ ] Пароли локальных администраторов уникальны на каждой машине и ротируются (LAPS)?
- [ ] Запуск exe из папок Downloads и %TEMP% заблокирован политикой?
- [ ] Запись на флешки запрещена там, где обрабатываются базы и персональные данные?
- [ ] Журнал Security увеличен и пишет входы и изменения учёток — успех и отказ?
- [ ] Обновления ставятся автоматически по расписанию, а не «когда-нибудь»?
- [ ] Рядовые сотрудники работают без прав локального администратора?
- [ ] Применение GPO проверяется отчётом gpresult, а не «на глаз»?

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 текущих политик: срезы gpresult/auditpol со всех машин, карта расхождений с baseline Microsoft
- Внедрение пакета из 10 GPO за рабочий день — в домене через GPMC или на отдельных PC через LGPO.exe
- Развёртывание Windows LAPS и AppLocker с обкаткой в аудит-режиме без остановки работы офиса
- WSUS и контур обновлений с тестовым кольцом для парков от 30 машин
- Сопровождение: ежеквартальная сверка политик с эталоном и разбор журналов безопасности

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 Security policy settings — Account Policies (learn.microsoft.com — Win 10/11)

02 Windows LAPS — policy settings и deployment (learn.microsoft.com — 2025)

03 AppLocker deployment guide (learn.microsoft.com — Win 11)

04 Advanced security audit policy settings (learn.microsoft.com — Win 11)

05 RDS Session Time Limits / Security (ADMX) (learn.microsoft.com — 2024)

06 Security Compliance Toolkit + LGPO.exe (microsoft.com — SCT 1.0)

07 Шаблон ITfresh «GPO-бейзлайн офиса до 50 PM» (itfresh.ru — v3)

Основано на официальной документации продуктов и нашей практике внедрения.