Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Сисадмин на офис до 50 ПК: наш чек-лист 2026

Требования к инженеру: AD/GPO и LAPS, Veeam 13, Zabbix 7.4, RouterOS 7.23

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Заказчик платит за «сисадмина», а получает переустановку Windows и замену картриджей: домен без политик, бэкап без единой проверки восстановления, сеть без схемы и мониторинга. На аудитах мы видим одно и то же — инфраструктура держится на памяти одного человека. Наш чек-лист переводит эту зону риска в измеримые пункты: что настроено, каким параметром и как проверяется.

Почему это важно бизнесу

- Простой 30 рабочих мест на день — это остановленная бухгалтерия и сорванные платежи, а не «неудобство для айтишников»
- Шифровальщик на сервере 1С без проверенного бэкапа означает потерю базы: восстанавливать нечего, документы вводят заново
- Уход единственного админа без документации — 2-3 недели паралича: пароли, схема сети и лицензии уходят вместе с человеком
- Без центральной консоли антивируса и триггеров мониторинга инцидент виден, когда встали все, а не в момент первого срабатывания
- Уволенный сотрудник с активной учётной записью и доступом к файловому серверу — утечка, за которую отвечает директор

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

7.4.x

версия Zabbix, на которой строим мониторинг: LTS-ветка 7.0, 8.0 LTS — Q3 2026

zabbix.com, life cycle policy

13.0.3

Veeam Agent для Windows в связке с VBR 13.0.2 — наша базовая схема копий

helpcenter.veeam.com, KB2683

3-2-1-1-0

схема копий: 3 копии, 2 носителя, 1 вне офиса, 1 неизменяемая, 0 ошибок проверки

наш стандарт

14 / 30

PasswordLength и PasswordAgeDays в Windows LAPS при PasswordComplexity=4

learn.microsoft.com, LAPS

900 с

SpecialPollInterval на PDC-эмуляторе при NtpServer с флагом 0x9 (0x1+0x8)

learn.microsoft.com, W32Time

60 мин

наш целевой RTO на подъём сервера 1С из последней копии на чистую систему

наш стандарт (SLA)

РЕАЛИЗАЦИЯ 1 ИЗ 3

Домен, учётные записи и рабочие места: AD DS + GPO

Что настраиваем

1-2 DC на Windows Server 2025, уровень домена и леса 2025 (DomainLevel 10), 20-50 PM, OU по подразделениям

Как мы это делаем

1. Строим OU-дерево и переносим учётки скриптом: Get-ADUser -Filter * -SearchBase ... | Move-ADObject -TargetPath ...; ручной ADUC оставляем только на исключения
2. Включаем корзину AD (Enable-ADOptionalFeature «Recycle Bin Feature»), парольную политику MinPwdLen=12, lockout 5 попыток / 15 минут
3. Windows LAPS на ПК и серверы: BackupDirectory=2, PasswordLength=14, PasswordAgeDays=30, PasswordComplexity=4, ADPasswordEncryptionEnabled=1 (нужен DFL 2016+)
4. GPO на OU бухгалтерии: Computer Configuration > System > Removable Storage Access > «All Removable Storage classes: Deny all access» + аудит доступа к шарам
5. Defender ASR в Block: 9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2 (кража кредов из LSASS) и d4f940ab-401b-4efc-aadc-ad5f3c50688a (Office не создаёт дочерние процессы)

РЕЗУЛЬТАТ

Учётки создаются и блокируются по регламенту в течение 24 часов, локальный админ на каждой машине имеет уникальный пароль с ротацией раз в 30 дней, а флешки в бухгалтерии перестают быть каналом заражения. Новый инженер разбирается в правах по структуре OU за один день.

КЛЮЧЕВОЙ НЮАНС

Всё, что сделано мышкой в ADUC, через полгода не воспроизвести. Мы фиксируем состояние домена в скриптах PowerShell и в бэкапах политик (Backup-GPO), чтобы любое изменение можно было откатить.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Резервное копирование с обязательной проверкой восстановления

Что настраиваем

Veeam Backup & Replication 13.0.2 + Veeam Agent 13.0.3, Hardened Repository на Linux

Как мы это делаем

1. VBR 13 ставим отдельным хостом — Windows-установка или Veeam Software Appliance (ISO/OVA), но не на контроллер домена; агенты 13.0.3 на физику и ПК руководителей
2. Схема 3-2-1-1-0: ночной инкремент, недельный full, копия на NAS и вторая вне офиса, Hardened Repository с immutability на 14 дней
3. Учётка задания — сервисный аккаунт без прав администратора домена; Linux-репозиторий вне домена, доступ по single-use credentials
4. Раз в месяц health check файлов копий и прогон SureBackup, раз в квартал — ручное восстановление базы 1С на тестовый стенд с замером времени
5. Результат пишем в журнал восстановлений: дата, что поднимали, время до запуска, кто проверял, какие расхождения нашли

РЕЗУЛЬТАТ

На реальном инциденте мы поднимаем сервер 1С из ночной копии за 40-60 минут, а не выясняем в этот момент, читается ли архив. Копии живут отдельно от домена, поэтому даже при захвате контроллера остаётся из чего восстанавливаться.

КЛЮЧЕВОЙ НЮАНС

Бэкап, который никто не восстанавливал, — это гипотеза, а не защита. Мы считаем задание рабочим только после успешного восстановления с замером времени и записью в журнале.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Мониторинг, сеть и единое время

Что настраиваем

Zabbix 7.4 на Debian/Ubuntu, MikroTik RouterOS 7.23.x stable (long-term 7.21.x), W32Time

Как мы это делаем

1. Zabbix server 7.4 + agent 2 в режиме active checks; шаблоны «Windows by Zabbix agent active» на серверы и «Mikrotik by SNMP» (SNMPv3) на роутер
2. Пороги, которые действительно звонят: свободно менее 10% на данных и 15% на C:, задержка диска, службы 1С и SQL down, UPS на батарее — в Telegram
3. Сеть: VLAN под серверы, ПК, гостей и камеры; L2TP/IPsec или WireGuard для удалённых; ежедневный /export и /system backup save с выгрузкой на файловый сервер
4. Время: на PDC-эмуляторе w32tm /config /manualpeerlist:«ntp,0x9» /syncfromflags:manual /update, SpecialPollInterval=900; остальные — DOMHIER, расхождение до 5 с
5. Учёт и документация: GLPI 11.0.x с GLPI Agent 1.18 для инвентаризации, BookStack — карта сети, IP-план, регламенты и контакты поставщиков

РЕЗУЛЬТАТ

Мы узнаём о заполненном диске или упавшей службе 1С за часы до жалоб пользователей, а конфигурация роутера восстанавливается из вчерашнего экспорта за 10 минут. Расхождение времени перестаёт ломать вход по Kerberos и сопоставление журналов.

КЛЮЧЕВОЙ НЮАНС

Мониторинг без адресата бесполезен. У каждого триггера должен быть получатель, действие и порог, выверенный на боевых данных, иначе алерты быстро перестают читать.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Бэкап без теста восстановления**
  Задание зелёное, а база не поднимается: без квартального restore-теста и health check вы узнаёте об этом в день аварии.

- ✕ **Один пароль локального админа на всех ПК**
  Скомпрометировали одну машину — получили все. Лечится Windows LAPS: уникальный пароль на устройство и ротация раз в 30 дней.

- ✕ **Запрет USB только в User Configuration**
  Политика не покрывает сервисные сеансы и обходится вторым профилем. Ставим запрет в Computer Configuration и проверяем gpresult /h.

- ✕ **Ставка на WSUS как на вечный сервис**
  WSUS в статусе deprecated: новых функций не будет. Роль в Windows Server 2025 работает, но план перехода на Intune/Autopatch готовим заранее.

- ✕ **DC совмещён с файлами и 1С**
  Одна ВМ держит домен, шары и SQL: обновление или шифровальщик роняют всё сразу. Роли разносим минимум на две машины.

- ✕ **Мониторинг без порогов и адресата**
  Zabbix стоит, триггеры дефолтные, алерты идут в никуда. Пороги, эскалацию и Telegram-канал настраиваем под конкретную инфраструктуру.

- ✕ **Конфигурация роутера нигде не сохранена**
  После сброса или неудачного апгрейда сеть собирают по памяти сутки. /export и /system backup save по расписанию снимают проблему.

- ✕ **Время в домене не синхронизировано**
  Расхождение больше 5 минут ломает вход по Kerberos (KRB_AP_ERR_SKEW) и делает журналы 1С и Windows несопоставимыми при разборе.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- AD + базовый набор GPO, MinPwdLen=12, lockout 5 попыток / 15 минут
- Veeam Agent на серверы, копии на отдельный носитель, тест-restore раз в месяц
- Антивирус с одной центральной консолью вместо разных free-агентов
- Схема сети, IP-план и список доступов в документе, доступном двоим

НОРМАЛЬНО

- VBR 13.0.2 и Hardened Repository с immutability, схема 3-2-1-1-0, журнал restore
- Zabbix 7.4 с алертами в Telegram и порогами по дискам, службам, UPS
- Windows LAPS, MFA на внешние сервисы, RustDesk self-hosted для удалёнки
- VLAN-сегментация, бэкап конфига MikroTik, VPN на L2TP/IPsec или WireGuard

ХОРОШО

- GLPI 11 и BookStack: учёт техники, лицензий и регламентов с ревизией
- Defender ASR в режиме Block и обновления кольцами: тест, потом все
- Квартальный restore-тест 1С на тестовом стенде с замером RTO
- Дежурство 2+ инженеров: отпуск и болезнь не превращаются в простой

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Учётки лежат в OU по подразделениям, а массовые операции делаются скриптами PowerShell, а не мышкой?
- [ ] Уволенный сотрудник блокируется в AD и в почте в течение 24 часов, и это записано в регламенте?
- [ ] Пароль локального администратора уникален на каждой машине и ротируется через Windows LAPS?
- [ ] Восстановление из бэкапа проверялось на реальных данных за последние 90 дней, с замером времени?
- [ ] Есть копия вне офиса и хотя бы одна неизменяемая (immutable) копия с заданным сроком хранения?
- [ ] Мониторинг покрывает диски, службы 1С и SQL, UPS и роутер, а алерты приходят конкретному инженеру?
- [ ] Конфигурация MikroTik выгружается по расписанию (/export) и хранится вне самого роутера?
- [ ] Время на всех серверах синхронизировано с PDC-эмулятором, расхождение меньше 5 секунд?
- [ ] Схема сети, IP-план и журнал доступов актуальны и доступны минимум двум людям в компании?
- [ ] Есть письменный порядок действий при шифровальщике, отказе UPS и утечке пароля?

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 за 2-3 дня: домен, GPO, бэкапы, сеть, регламенты — письменный отчёт со списком пробелов
- Разворачиваем базу под ключ: AD/GPO, LAPS, Veeam 13, Zabbix 7.4, VLAN на MikroTik
- Пишем регламенты и карту сети в BookStack, ставим GLPI 11 для учёта техники и лицензий
- Берём серверы и безопасность на себя, штатный инженер закрывает пользователей: гибридная модель
- Дежурная смена подменяет вашего админа в отпуске и на больничном без простоя бизнеса

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 DS Functional Levels: Windows Server 2025 = DomainLevel 10 (learn.microsoft.com — 2025)

02 Configure policy settings for Windows LAPS: значения и defaults (learn.microsoft.com — 2026)

03 Attack surface reduction (ASR) rules reference: GUID правил (learn.microsoft.com — 2026)

04 Windows Time Service Tools and Settings: NtpServer, SpecialPollInterval (learn.microsoft.com — 2026)

05 Features no longer developed in Windows Server: WSUS deprecated (learn.microsoft.com — 2025)

06 Zabbix Life cycle and release policy + Templates out of the box (zabbix.com — 7.4)

07 Veeam B&R 13 release notes + KB2683 (Agent for Windows 13.0.3) (helpcenter.veeam.com — 13.0)

08 RouterOS changelogs: stable 7.23.2, long-term 7.21.4 (mikrotik.com — 7.23)

09 GLPI 11.0.x и GLPI Agent 1.18: документация по установке (glpi-project.org — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.