Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Инвентаризация IT-активов: техника, лицензии и доступы

Как мы разворачиваем GLPI, SNMP-инвентарь сети и защищённое хранилище доступов

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Заказчик не знает, что у него в IT: парк докупался стихийно, лицензии и ключи разбросаны, а доступы к домену, роутерам и облачным сервисам держит в голове один приходящий айтишник. Пока всё работает — кажется, что под контролем. Но поломка вне гарантии, проверка лицензий или уход сотрудника с паролями превращаются в простой и незапланированные расходы.

Почему это важно бизнесу

- Техника вне учёта: упускаем гарантию и продлеваем платно то, что чинится бесплатно
- Лицензии на несколько миллионов теряются вместе с ключами и чеками — платим дважды
- Просроченный КриптоПро останавливает сдачу отчётности в ФНС в день дедлайна
- Уход айтишника с паролями = простой домена, роутера и ЛК провайдера на сутки
- Нелегальное ПО при внешней проверке — штраф по ст. 7.12 КоАП и иск правообладателя

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

10.0.x

Версия GLPI: нативная инвентаризация без плагина, включаем в Setup → General → Inventory

по докам GLPI

1.17

GLPI Agent — преемник FusionInventory; ставим на все PC и серверы через GPO-MSI

по докам glpi-agent

24 ч

Частота PROLOG-инвентаризации, задаём на стороне сервера GLPI

наш стандарт

SNMPv3

Сетевое железо: auth SHA + priv AES вместо открытой community v2c

по докам GLPI

30 дн

Порог алерта до истечения лицензий и сертификатов КриптоПро

наш стандарт

2

Минимум держателей мастер-ключа хранилища паролей: не только ИТ

наш стандарт

РЕАЛИЗАЦИЯ 1 ИЗ 3

GLPI + GLPI Agent: авто-учёт железа и ПО

Что настраиваем

Сервер GLPI 10.0.x на выделенной VM/LXC, агенты на всех рабочих станциях и серверах домена AD

Как мы это делаем

1. Ставим GLPI 10.0.x (PHP 8.2, MariaDB), включаем нативную инвентаризацию в Setup → General → Inventory, точка приёма — /front/inventory.php
2. Разворачиваем GLPI Agent 1.17 на PC и серверах через GPO-MSI с ключами server= и tag=; частота PROLOG 24 ч
3. Агент снимает модель, S/N, CPU/RAM/диски и список ПО из Uninstall-веток реестра — без медленного WMI Win32_Product
4. Бизнес-правила автосоздания активов связывают записи по серийнику, проставляют статус, локацию и ответственного
5. Заявки техподдержки ведём в том же GLPI Helpdesk и привязываем тикет к конкретному активу

РЕЗУЛЬТАТ

Единый реестр всего парка обновляется сам: по каждой единице видно возраст, гарантию, установленное ПО и владельца. Поломка или закупка сразу отражается в базе, списание и продление гарантии идут по факту, а не по памяти сотрудника.

КЛЮЧЕВОЙ НЮАНС

В инвентаре не используем WMI-класс Win32_Product: обращение к нему запускает reconfigure всех MSI и тормозит PC. GLPI Agent читает Uninstall-ветки реестра — быстро и без побочных эффектов.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Сетевое железо и МФУ через SNMP-инвентарь GLPI

Что настраиваем

Коммутаторы, маршрутизаторы и принтеры в LAN; задачи netdiscovery + netinventory на GLPI Agent в роли сборщика

Как мы это делаем

1. Заводим SNMP-креды: для v3 — user + auth SHA + priv AES (для v2c только community); ставим perl-модуль Crypt::Rijndael для AES/v3
2. Network discovery по IP-диапазону: агент перебирает креды по порядку, поэтому держим минимальный набор и снижаем SNMP timeout
3. Network inventory снимает модель, версию прошивки, порты, MAC-таблицы и уровни тонера у известных устройств
4. Конфиги свитчей MikroTik/Cisco выгружаем (export/tftp) и версионируем в git-хранилище

РЕЗУЛЬТАТ

Сеть восстанавливается после гибели свитча за минуты — по сохранённому конфигу, а не сборкой с нуля. Прошивки и занятость портов видны централизованно, устаревшее железо попадает в план замены заранее.

КЛЮЧЕВОЙ НЮАНС

GLPI Agent ждёт SNMP timeout на каждый неподходящий cred в списке — при десятке кредов discovery диапазона /24 растягивается на часы. Привязываем к диапазону только релевантные креды.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Реестр доступов: AD, менеджер паролей, КриптоПро

Что настраиваем

Учётки домена AD, пароли к оборудованию и облачным ЛК, лицензии и сертификаты; self-hosted менеджер паролей

Как мы это делаем

1. Инвентаризация AD: Get-ADComputer и Get-ADUser -Filter {Enabled -eq $false} — отключённые и уволенные чистим, доступ отзываем
2. Пароли переносим в self-hosted Vaultwarden 1.37 (или KeePassXC 2.7, база KDBX4 на Argon2) — коллекции по сервисам
3. Подключаем OIDC-SSO к домену; мастер-коллекция доступна минимум двум держателям — директору и доверенному сотруднику
4. Мониторим срок лицензий и сертификатов КриптоПро (cpconfig -license -view), порог алерта 30 дней до истечения
5. При аудите меняем стандартные и застарелые пароли на роутерах и свитчах, фиксируем в хранилище

РЕЗУЛЬТАТ

Доступы больше не живут в голове одного айтишника: увольнение или болезнь не блокирует бизнес. Отчётность в ФНС не встаёт из-за просроченного КриптоПро, а чужие учётки не остаются активными месяцами.

КЛЮЧЕВОЙ НЮАНС

Единственный держатель пароля — точка отказа: уход сотрудника = потеря доступа к домену, роутеру и ЛК провайдера. Всегда закладываем второго держателя мастер-ключа, не только ИТ.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Win32_Product в скрипте инвентаризации**
  Обращение к WMI-классу запускает reconfigure каждого MSI и вешает PC. Собираем ПО из Uninstall-веток реестра штатным GLPI Agent.

- ✕ **Пароли знает только один человек**
  Уход или болезнь айтишника блокирует домен, роутер и ЛК провайдера. Кладём в хранилище с минимум двумя держателями мастер-ключа.

- ✕ **Пароли в txt на рабочем столе**
  Файл не шифрован и копируется куда угодно. Переносим в Vaultwarden или KeePassXC с базой KDBX4 на Argon2.

- ✕ **SNMP v2c с community public наружу**
  Строка читается в открытую и торчит в сеть. Переходим на SNMPv3 (auth SHA, priv AES) и закрываем ACL по управляющей подсети.

- ✕ **Нет бэкапа конфигов свитчей**
  Гибель коммутатора без сохранённого конфига — это сутки без сети. Выгружаем export/tftp и версионируем в git.

- ✕ **Активные учётки уволенных в AD**
  Чужой доступ к домену и файлам месяцами. Регулярно Get-ADUser по Enabled/lastLogon, отключаем и переносим в архивную OU.

- ✕ **КриптоПро без контроля срока**
  Лицензия или сертификат истекает — отчётность встаёт утром сдачи. cpconfig -license -view плюс алерт за 30 дней до конца.

- ✕ **Дубли активов в GLPI**
  Без tag и связки по серийнику один ПК плодит записи при каждой переустановке. Бизнес-правила матчат по S/N и обновляют актив.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Реестр в Excel/облаке: 3 листа — Железо, Лицензии, Доступы, файл не на локальной PC
- Полная ревизия раз в год плюс реакция на увольнение, закупку, истечение лицензии
- Менеджер паролей вместо txt, мастер-ключ минимум у двух человек
- Чистка учёток уволенных в AD и возврат техники в день ухода

НОРМАЛЬНО

- GLPI 10.0.x + GLPI Agent 1.17 по GPO, автоинвентарь железа и ПО
- SNMP-инвентарь сети (v3, SHA/AES) и бэкап конфигов свитчей
- Self-hosted Vaultwarden/KeePassXC KDBX4, коллекции по сервисам
- Мониторинг срока лицензий и КриптоПро, порог 30 дней

ХОРОШО

- GLPI как CMDB + Helpdesk: тикеты привязаны к активам, история изменений
- Бизнес-правила автосоздания активов, версионирование конфигов в git
- Bitwarden Business: OIDC-SSO и SCIM-провижининг учёток из AD
- Пороги истечения и доступность железа заведены в Zabbix

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Все PC и серверы отдают инвентарь в GLPI Agent с частотой PROLOG не более 24 ч?
- [ ] Нативная инвентаризация включена в GLPI 10 (Setup → Inventory), точка приёма /front/inventory.php?
- [ ] Сетевое железо снято по SNMP (v3 SHA/AES), конфиги свитчей забэкаплены в git?
- [ ] Реестр лицензий: ключ/ЛК/дата окончания по Windows, Office, 1С и КриптоПро?
- [ ] Срок лицензии и сертификатов КриптоПро под мониторингом с порогом 30 дней?
- [ ] Пароли лежат в менеджере (Vaultwarden/KeePassXC KDBX4), а не в txt на столе?
- [ ] Мастер-ключ хранилища есть минимум у двух человек, не только у ИТ-специалиста?
- [ ] Учётки уволенных отключены в AD, техника возвращена и переучтена?
- [ ] Стандартные и застарелые пароли на роутерах и свитчах сменены?
- [ ] Полная ревизия раз в год плюс реакция на события (увольнение, закупка, лицензия)?

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).

- Разворачиваем GLPI 10.0.x + Agent 1.17 по GPO: единый реестр железа и ПО за 1-3 дня
- Настраиваем SNMP-инвентарь сети (v3) и бэкап конфигов свитчей MikroTik/Cisco в git
- Ведём реестр лицензий и мониторинг срока КриптоПро/сертификатов с алертом за 30 дней
- Внедряем менеджер паролей (Vaultwarden/KeePassXC) с двумя держателями и OIDC-SSO
- Чистим AD от уволенных, ротируем пароли оборудования, отдаём шаблон реестра активов

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 GLPI 10.0 — Inventory (нативная инвентаризация) (glpi-project.org — 10.0)

02 GLPI Agent documentation (установка, PROLOG) (glpi-agent.readthedocs.io — 1.17)

03 Network discovery / SNMP Credentials (help.glpi-project.org — 10.0)

04 Vaultwarden Wiki: self-hosting, OIDC SSO (github.com — 1.37)

05 Bitwarden Business: SSO и SCIM 2.0 provisioning (bitwarden.com — 2026)

06 KeePassXC User Guide: KDBX4, Argon2 (keepassxc.org — 2.7)

07 Active Directory PowerShell: Get-ADUser/Get-ADComputer (learn.microsoft.com — 2026)

08 КриптоПро CSP: управление лицензией (cpconfig) (cryptopro.ru — CSP 5.0)

Основано на официальной документации продуктов и нашей практике внедрения.