



Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Перевод офиса на Linux: матрица ролей и смешанная инфраструктура

Как мы отбираем роли, вводим Linux-станции в AD и оставляем Windows-only ПО через RemoteApp

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

Суть проблемы

Заказчик хочет снять лицензионную нагрузку Windows/Office и закрыть требования по отечественному ПО, но у него один домен AD, общий файловый сервер, 1С, КriptoПро и парк принтеров. Перевод «всех подряд» ломает подпись у бухгалтера, СПС у юриста и Excel-макросы; без ролевой матрицы и единого управления парк превращается в две инфраструктуры с двойной стоимостью и откатом.

Почему это важно бизнесу

- Лицензии Windows Pro + Office на 30 РМ — сотни тысяч рублей единовременно и ежегодно; экономия реальна только на «зелёных» ролях
- Сорванная подпись отчётности в ФНС или банк-клиент у бухгалтера стоит дороже любой лицензии — красные роли не трогаем
- Две неуправляемые платформы = двойные регламенты, двойные ошибки; Linux обязан жить в том же AD, бэкапе и мониторинге
- Требования регуляторов к отечественному ПО закрываются Astra/Альт только при корректной интеграции, а не «поставили и забыли»
- Откат после неудачной миграции — это повторная оплата работ и простой сотрудников на 1–2 дня на каждое РМ



Ключевые параметры реализации

6.12 / 6.1

Ядра: Альт PC 11.2 — 6.12 LTS; Astra SE 1.8.3 — 6.1 LTS или 6.12 под новое железо

Альт 11.2 / Astra SE 1.8, политика ядер

≤5 мин

Допуск часов Kerberos (clockskew); chrony к DC ставим до realm join, иначе нет входа и шар

MIT krb5 clockskew / наш стандарт

enforcing

Дефолт ad_gpo_access_control в SSSD: GPO «Allow log on locally» уже действует на Linux-станции

man sssd-ad(5)

3.10-7.0

Ядра, поддерживаемые Veeam Agent for Linux 13.1; снапшоты blksnap только на Ext4/XFS/Btrfs

Veeam Agent for Linux 13.1, System Requirements

26.2

Ветка LibreOffice still 26.2 (поддержка до 30.11.2026) на станции; на fresh 26.8 — после 26.8.2

libreoffice.org, Release Notes

86400 с

dyndns_refresh_interval SSSD: станция сама обновляет A/PTR в DNS AD по GSS-TSIG раз в сутки

man sssd-ad(5)



Ролевая матрица и пилот: кто идёт на Linux, кто остаётся

Что настраиваем

Аудит 20-50 РМ: инвентаризация ПО и периферии по каждой роли, стенд-пилот на 2 недели, решение по цветам

Как мы это делаем

- 1 Снимаем инвентарь через наш Collector-GPO (реестр Uninstall, Get-Printer, USB-устройства, плагины браузера) в CSV — по каждому ПК, а не «по словам»
- 2 Красим роли: зелёные (браузерные CRM/ERP, почта, LibreOffice, клиент 1С без подписи), жёлтые (КонсультантПлюс, Контур, VBA), красные (КриптоПро+банк-клиент, ЧПУ)
- 3 Жёлтые закрываем RemoteApp на RDS: FreeRDP 3 (xfreerdp /app:program:... /dynamic-resolution +clipboard /drive:home,\$HOME) — приложение на Windows, окно у пользователя
- 4 Пилот: 2-3 станции на Ubuntu 24.04/26.04 LTS или Альт 11.2 (при требовании ФСТЭК — Astra SE 1.8), 2 недели, журнал обращений; критерий — 0 блокирующих кейсов
- 5 Фиксируем стандарт образа (дистрибутив, DE «как Windows», шпаргалка по горячим клавишам Calc/Excel) и план тиража партиями по 5 РМ

РЕЗУЛЬТАТ

Заказчик получает список «можно/нельзя» по фамилиям с обоснованием, а не общее «Linux подходит»; бухгалтерия и подпись остаются на Windows, зелёные роли уходят на Linux без откатов.

КЛЮЧЕВОЙ НЮАНС

Смотрим не на должность, а на бинарники и плагины: одна «Такском»-надстройка или GDI-принтер переводят роль в жёлтую зону; RemoteApp дешевле, чем эмуляция через Wine.



Ввод Linux-станций в AD: realmd/SSSD, GPO, шары, печать

Что настраиваем

Каждая Linux-станция в том же домене corp.<клиент>.ru, что и Windows: SSO, DNS, доменные шары и принтеры без второй учётной записи

Как мы это делаем

- 1 Готовим узел: hostname ≤15 символов, DNS на DC, chrony к DC; Ubuntu — realmd sssd adcli oddjob-mkhomedir; Astra — astra-ad-sssd-client; Альт — task-auth-ad-sssd
- 2 `realm join -U <svc-join> corp.example.ru`; `sssd.conf`: `access_provider = ad`, `dyndns_update = true`, `fallback_homedir = /home/%u@%d`, `use_fully_qualified_names = false`
- 3 GPO: на пилоте `ad_gpo_access_control = permissive` и читаем `/var/log/sssd`, потом `enforcing`; на Альт ставим `gupdate` + `ADMX admx-basealt` в `SYSVOL\PolicyDefinitions`
- 4 Шары: `cifs-utils` + `pam_mount` с `sec=krb5,multiuser` к DFS-пути; браузеры — политики JSON в `/etc/opt/chrome/policies/managed` (`AuthServerAllowlist`, `HomepageLocation`)
- 5 Печать: CUPS 2.4, `lpadmin -m everywhere` на IPP-принтеры (HP/Kyocera/Canon); Zebra/TSC — raw-очередь ZPL; GDI-модели помечаем к замене

РЕЗУЛЬТАТ

Пользователь входит доменным логином, получает домашнюю папку, сетевые диски и принтеры автоматически; блокировка учётки в AD мгновенно закрывает доступ и на Linux; DNS-записи станций ведёт сам SSSD.

КЛЮЧЕВОЙ НЮАНС

GPO на Linux — это только права входа и то, что умеет `gupdate` Альт; остальное (браузер, офис, обновления) раскладываем Ansible-ролями, а не ждём «как в Windows».



Стандарт рабочего места: офис, шрифты, бэкап, мониторинг

Что настраиваем

Единый образ Linux-станции и ноутбука: LibreOffice, шрифты, шифрование, обновления, Veeam и Zabbix в общей консоли с Windows

Как мы это делаем

- 1 LibreOffice 26.2 (still): дефолт Load/Save = Office Open XML через .xcd в /etc/libreoffice/registry; словари hunspell-ru/hyphen-ru; автосохранение 5 мин
- 2 Шрифты metric-compatible: Liberation (Times/Arial), Carlito (Calibri), Caladea (Cambria), PT Astra Serif/Sans на Astra — вёрстка договоров не «плывёт»
- 3 Ноутбуки: LUKS2 на корень при установке, TPM/Secure Boot через shim; станции — unattended-upgrades только security-origin, окно ребута ночью
- 4 Veeam Agent for Linux 13.1 в protection group VBR: blksnap на Ext4/XFS; Astra/Альт вне списка — nosnap-агент (LVM/Btrfs-снимок), файловый бэкап /home
- 5 Zabbix agent 2 (7.0 LTS) с шаблоном Linux by Zabbix agent; KESL 12.5 с политикой из общей консоли KSC; sudo только группе AD «Linux-Admins»

РЕЗУЛЬТАТ

Один регламент на весь парк: бэкап-джоб и триггеры Zabbix одинаковы для Windows и Linux, ноутбук с LUKS можно потерять без утечки, обновления не ломают интерфейс между релизами LTS.

КЛЮЧЕВОЙ НЮАНС

Ветка still LibreOffice и LTS-дистрибутив важнее «свежести»: пользователи привыкают к интерфейсу один раз, а мы не переобучаем их каждые полгода.



Подводные камни

✗ Часы разъехались с DC

Kerberos терпит ≤ 5 мин; при большем realm join и вход падают с KRB5KRB_AP_ERR_SKEW. chrony к DC ставим первым шагом образа.

✗ Имя хоста длиннее 15 символов

sAMAccountName компьютера режется, join проходит, а тикеты — нет. Именованые станции по стандарту клиента, ≤ 15 знаков, без кириллицы.

✗ GPO молча запрещает вход

enforcing по умолчанию: без «Allow log on locally» для группы пользователь получает отказ. На пилоте permissive + журнал sssd_<домен>.log.

✗ LibreOffice сохраняет в ODF

Контрагент не открывает .odt/.ods. Дефолт фильтра ставим OOXML через xcd-политику и оставляем ODF только для внутреннего архива.

✗ Excel-макросы VBA

LibreOffice Basic не совместим с VBA бухгалтерии/аналитики. Роль с макросами — жёлтая: RemoteApp Excel на RDS, а не переписывание макросов.

✗ GDI-принтер без IPP

Host-based модели не отвечают на get-printer-attributes — CUPS не поднимет очередь. Проверяем driverless/ippool до миграции, GDI меняем на PCL/PS.

✗ КриптоПро и плагин в браузере

CSP 5.0 R3 (ветка 4.0 без сертификата с 15.01.2026); ставим cprocsp-rdr-gui-gtk, не cprocsp-rdr-gui; pcsd для Рутокен. Подпись — на Windows/RDS.

✗ Astra/Альт вне списка Veeam

Официально — Debian/Ubuntu/RHEL/SLES-семейство; на отечественных сборках используем posnap-агент и файловый режим, иначе задание молча падает.

Как правильно

МИНИМУМ

- Инвентарь ПО/периферии по каждому ПК и ролевая матрица зелёные/жёлтые/красные
- Пилот 2–3 станции на LTS-дистрибутиве, 2 недели, журнал обращений
- Станции в AD через realmd/SSSD, chrony к DC, dyndns_update = true
- LibreOffice still с дефолтом OOXML и metric-compatible шрифтами

НОРМАЛЬНО

- RemoteApp на RDS для жёлтых ролей (СПС, Контур, Excel с VBA) через FreeRDP 3
- GPO-контроль входа enforcing + gpupdate/ADMX на Альт, политики браузера JSON
- Veeam Agent for Linux 13.1 в общей protection group, Zabbix agent 2 на каждой станции
- Ansible-роли для образа: шары ram_mount, CUPS-очереди, unattended-upgrades

ХОРОШО

- Astra SE 1.8 / Альт 11.2 при требованиях ФСТЭК, единый локальный apt-репозиторий
- LUKS2 + Secure Boot на ноутбуках, sudo только AD-группе, KESL 12.5 с общей политикой
- Регламент тиража по 5 РМ с откатным образом Windows и чек-листом приёмки роли
- Ежегодный пересмотр матрицы: веб-версии СПС/Контур переводят роли из жёлтых в зелёные



Чек-лист самопроверки

- | | |
|--|--|
| ☐ Есть ли инвентарь установленного ПО и принтеров по каждому ПК, а не только по должностям? | ☐ Задан ли режим <code>ad_gpo_access_control</code> и проверен ли вход пользователей после <code>enforcing</code> ? |
| ☐ Все бухгалтерские и подписывающие роли (КриптоПро, банк-клиент, Контур) оставлены на Windows или RDS? | ☐ Выставлен ли в LibreOffice дефолт сохранения OOOXML и установлены ли шрифты Liberation/Carlito/Caladea? |
| ☐ Проверены ли принтеры на IPP Everywhere (<code>driverless/ipptool</code>) и есть ли план замены GDI-моделей? | ☐ Попадают ли Linux-станции в общий бэкап Veeam и в Zabbix с теми же триггерами, что Windows? |
| ☐ Введены ли Linux-станции в тот же домен AD (<code>realm list</code> показывает <code>configured: kerberos-member</code>)? | ☐ Зашифрованы ли Linux-ноутбуки LUKS2 и ограничен ли <code>sudo</code> доменной группой администраторов? |
| ☐ Синхронизировано ли время станций с DC и укладывается ли <code>hostname</code> в 15 символов? | ☐ Есть ли шпаргалка по горячим клавишам Calc/Writer и ответственный «сосед» на первые 2 недели? |

Если хотя бы на два вопроса ответ «нет» или «не знаю» — тема требует внимания.



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 рабочих мест и ролевая матрица «Linux / Windows / RemoteApp» с расчётом реальной экономии
- Пилот и тираж Linux-станций (Ubuntu LTS, Альт 11.2, Astra SE 1.8) с вводом в существующий AD
- RDS с RemoteApp для КонсультантПлюс, Контур и 1С с подписью — без переезда бухгалтерии
- Единый образ: LibreOffice, шрифты, CUPS-печать, LUKS, обновления, Ansible-роли
- Подключение Linux-парка к Veeam и Zabbix ITfresh и сопровождение смешанной инфраструктуры

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** sssd-ad(5): AD provider, GPO access control, dynamic DNS (sssd.io — 2.13)
- 02** Astra Linux SE 1.8: ввод в домен AD (astra-ad-sssd-client), политика ядер (wiki.astralinux.ru — SE 1.8.3)
- 03** Альт Рабочая станция 11.2: ввод в домен AD, групповые политики, gupdate (docs.altlinux.org — 11.2)
- 04** Chrome Enterprise: политики Linux в /etc/opt/chrome/policies/managed (chromeenterprise.google — 2026)
- 05** Veeam Agent for Linux — System Requirements, blksnap, nosnap (helpcenter.veeam.com — 13.1)
- 06** LibreOffice Release Notes и план выпусков (still/fresh) (libreoffice.org — 26.2/26.8)
- 07** КриптоПро CSP 5.0 R3 и ЭЦП Browser plug-in для Linux (cryptopro.ru — 5.0 R3)
- 08** OpenPrinting CUPS 2.4: IPP Everywhere / driverless (openprinting.github.io — 2.4)

Основано на официальной документации продуктов и нашей практике внедрения.

