



# Программный комплекс «Альт Домен»

[basealt.ru](http://basealt.ru)





# Уникальность «Альт Домен»



## Групповые политики в Linux как в Windows

Возможность одновременно применять групповые политики к компьютерам и пользователям доменов ОС «Альт» и Windows при переходе на импортонезависимое программное обеспечение



## Готовые сценарии миграции с Windows на Linux

Специально разработанные инструменты применения групповых политик и управления объектами домена. Типовые сценарии миграции опубликованы в документации



## Эффективное решение для перевода ИТ-инфраструктуры организаций с зарубежных аналогов на российское ПО

Возможность интеграции в инфраструктуру MS Active Directory без внесения в структуру домена каких-либо изменений



## Интуитивно понятный и удобный интерфейс

ИТ-администраторам не нужно дополнительно переучиваться, инструменты управления принципиально сделаны похожими на привычные



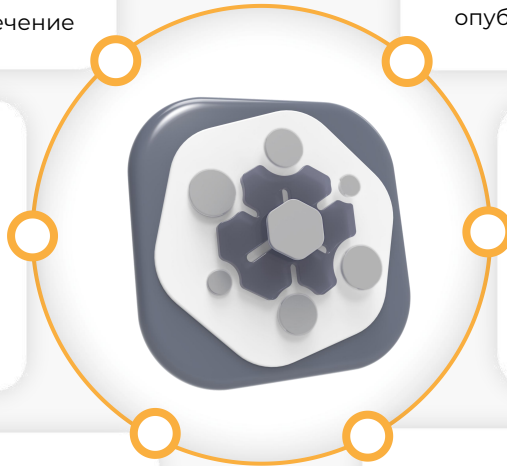
## Открытость решения

Доступны исходные коды, опубликованы шаблоны групповых политик. Можно адаптировать решение под нужды конкретной организации

**SAMBA**

## Основа решения — международный свободный проект Samba

Большие ресурсы разработки, постоянное развитие и обновление, самые актуальные доработки, признание организациями по всему миру, большой опыт использования





# О компании

**33%**

прирост  
за 2024 год

**8**

операционных  
систем

**8**

аппаратных  
платформ

**20+**

лет на рынке

**Собственная  
технологическая  
платформа**

**Своя инфраструктура  
на территории РФ**

**Офисы  
в 4 городах**

**Поставки лицензий**

**1 300 000+**

всего

**280 000+**

для образования

**Обучение**

**11 000+**

специалистов

Данные приведены с 2016 года



# Продукты «Альт»



**Альт**  
СП



**Альт**  
Сервер



**Альт**  
Виртуализация



**Альт**  
Рабочая станция



**Альт**  
Рабочая станция К



**Альт**  
Образование



**ALT**  
Mobile



**Альт**  
Домен



**Simply**  
Linux



**Альт**  
Платформа



# «Альт Домен»

Программный комплекс для централизованного управления компьютерами и пользователями в гетерогенной (смешанной) сети



**Служба каталогов, позволяющая централизованно управлять компьютерами и пользователями в корпоративной сети с операционными системами (ОС) на ядре Linux и Windows по единым правилам из единого центра**

Служит как для создания новой ИТ-инфраструктуры, так и для миграции с зарубежного ПО на отечественное (например, для замены службы каталогов Microsoft Active Directory).



# Проблемы, мешающие продолжать использовать Active Directory (AD)

- **Санкции:**
  - ✗ нельзя продлить лицензии,
  - ✗ невозможно получить техподдержку.

- **Требования безопасности**

- **Постановления правительства:**

Указы Президента РФ:

- № 166 от 30 марта 2022 г.
- № 250 от 01 мая 2022 г.
- изменения в № 1085 от 16 августа 2004 г.

от 8 ноября 2023 расширяет полномочия ФСТЭК РФ



# Что такое Microsoft AD?

- **Active Directory** (AD) — проприетарная реализация от компании Microsoft службы каталогов, позволяющее объединить различные объекты сети — компьютеры, серверы, принтеры, различные сервисы — в единую систему. В данном случае AD выступает в роли базы данных (каталога), в которой хранится информация о пользователях, ПК, серверах, сетевых и периферийных устройствах.  
(Аналоги **Apple Open Directory, Novell Directory Services**).
- **В качестве** такой **базы** выступает **LDAP** (Lightweight Directory Access Protocol) — облегчённый протокол доступа к каталогам, открытый стандартизированный протокол, применяемый для работы с различными реализациями служб каталогов, в том числе, но и не только, Active Directory.
- **Основной задачей** Active Directory является **хранение информации** обо всех объектах в сети и предоставление её внешним системам.  
В свою очередь, LDAP позволяет пользователям получить доступ к ресурсам в зависимости от прав, настроенных администратором службы каталогов.



# Возможности MS Active Directory

- Единая точка аутентификации
- Удобное управление политиками
- Безопасность
- Удобный обмен файлами
- Интеграция сервисов и оборудования

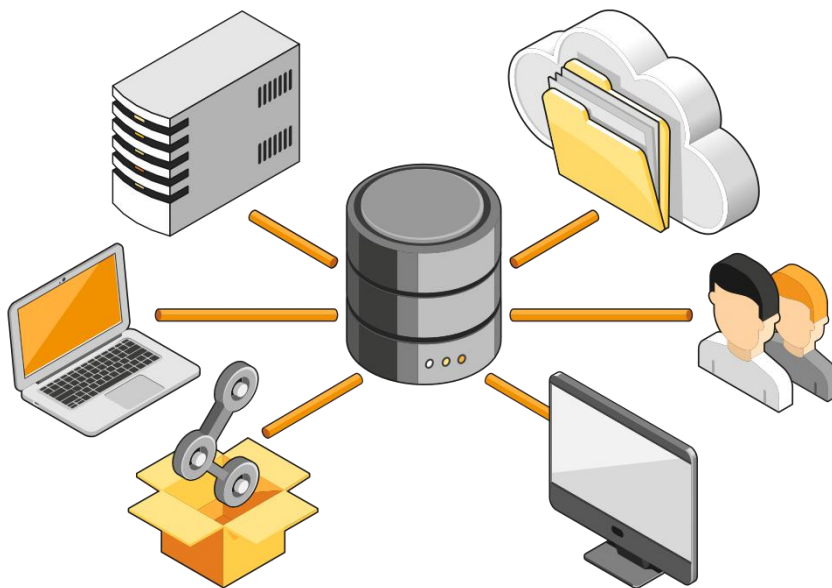


# Особенности MS Active Directory

**MS AD** — критическая точка в ИТ-структуре

Для повышения надёжности необходимо:

- наличие вторичных контроллеров;
- регулярный бэкап.



# Чем заменить AD?

Что есть в мире Linux?

- LDAP + Kerberos
- Samba  
(с 1992 г. v.4 2012 г.)
- FreeIPA (2008 г.)  
LDAP: 389-ds  
Mit Kerberos  
DogTag  
DNS: BIND  
DHCP

**Операционные системы «Альт»  
поддерживают все эти виды доменов**



# Чем заменить AD: FreeIPA vs SAMBA

## Поддержка связности узлов в сети предприятия

- Почта предприятия (**Exchange**) — **SOGGo/CommuniGate**
- **DNS** — решается сторонними проектами (или внутр. **Samba**)
- **DHCP** — решается сторонними проектами
- Внутренние сервисы (корпоративные порталы)
- **Файлообмен**  
Решается только с помощью **Samba**
- **Управление конфигурацией**  
Решается только с помощью **Samba**
- **Сквозная аутентификация**  
Предоставляется обоими проектами — **FreeIPA** и **Samba**
- **Организация удалённого доступа**  
Полноценно не решается ни одним из проектов

**ОС «Альт» поддерживают оба варианта: Samba DC и FreeIPA**



# Наш выбор — SAMBA + GPO = «Альт Домен»

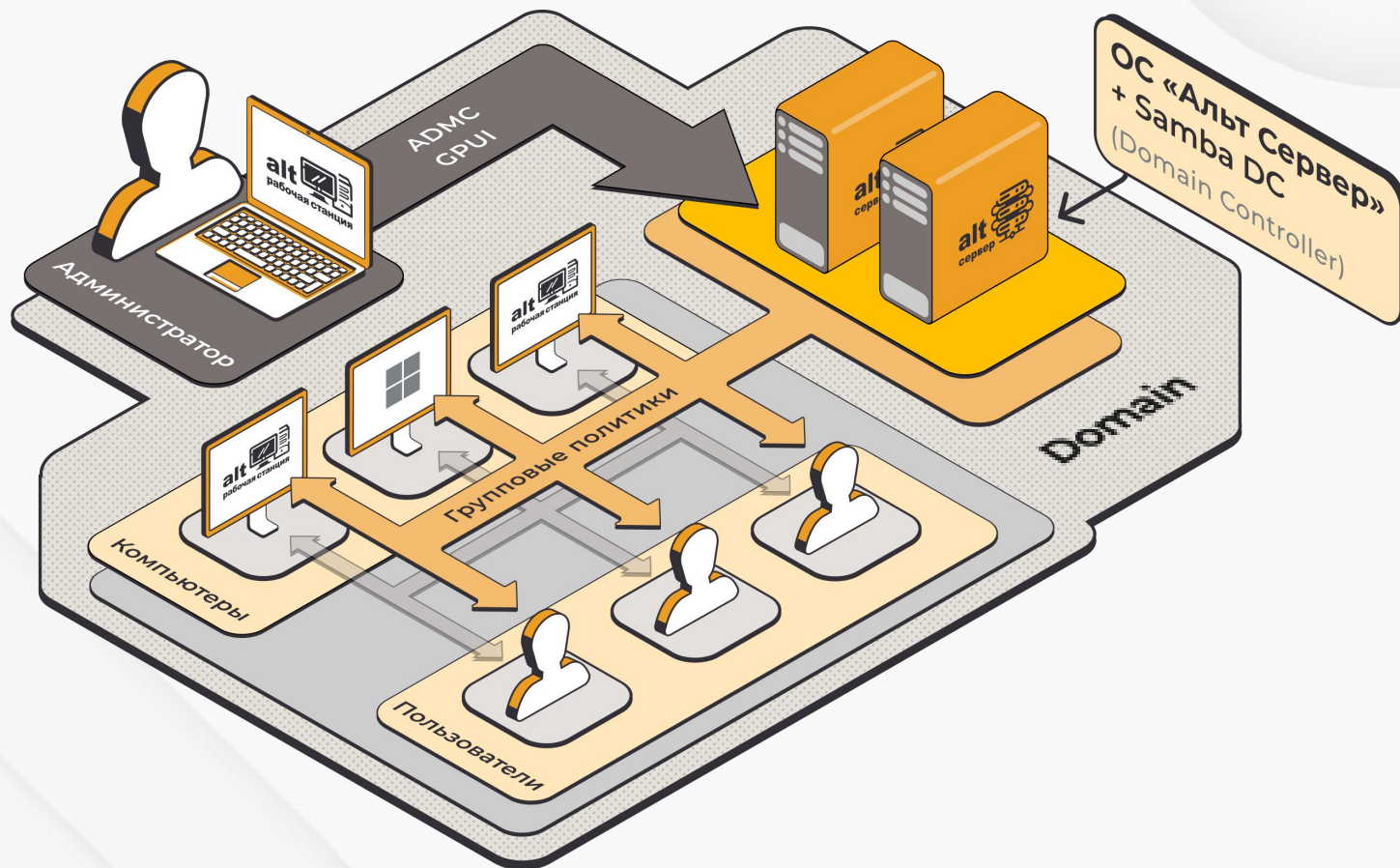
- Поддержка применения групповых политик в конкретных дистрибутивных решениях, в целом, не является частью проекта **Samba**
- Разработка ведется в рамках проекта **Samba** с известными ограничениями
- Политики разрабатываются для семейства ОС «Альт», перенос на другие «линуксы» возможен с ограничениями
- Инструменты управления разрабатывались по гранту РФРИТ (и продолжают развиваться)

**Samba DC + групповые политики (GPO) для бесшовной миграции с Windows на Linux — решение «Альт Домен» (ALT Domain)**

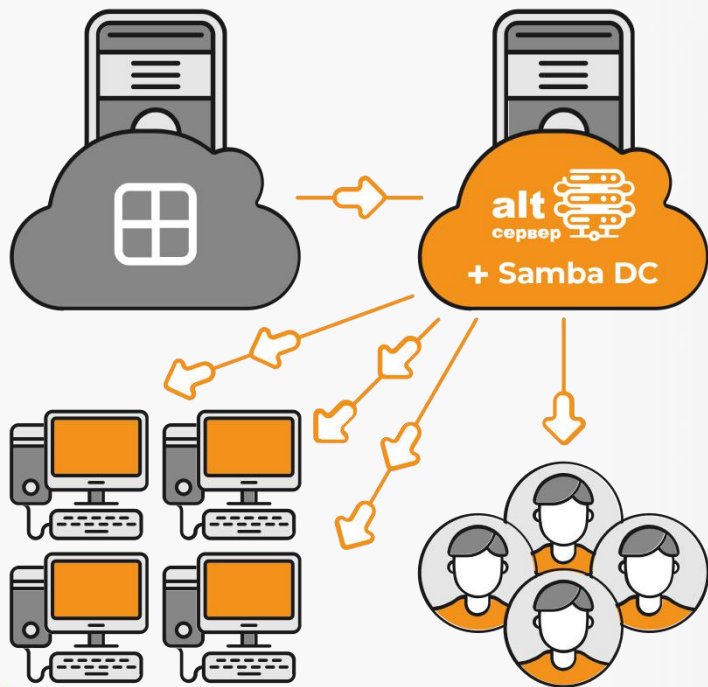


# Групповые политики (ГПО)

Схема управления и работы ГПО



# Особенности реализации групповых политик в ОС «Альт»



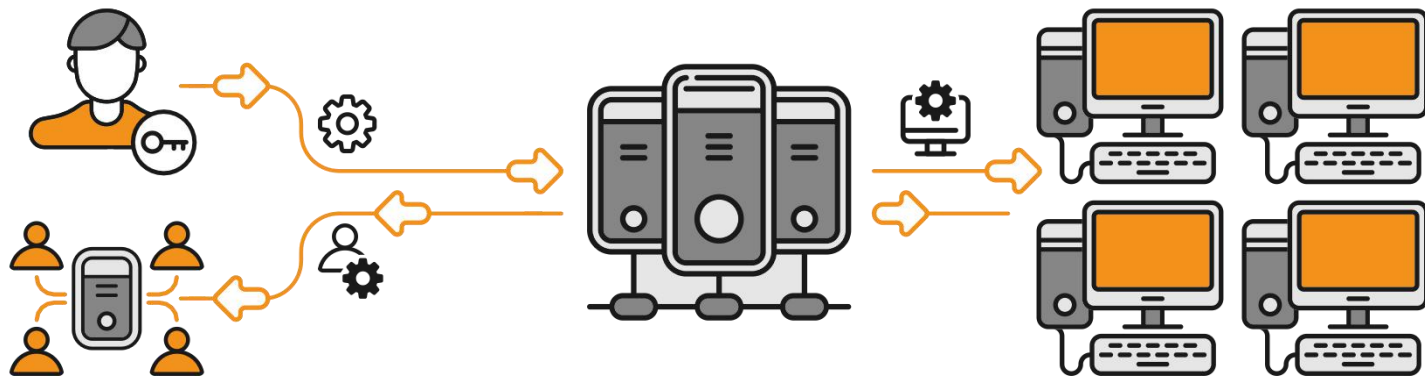
Групповые политики, как механизм, отличаются от стандартных инструментов управления конфигурациями (таких как, например, Puppet, Ansible и др.) тремя ключевыми особенностями:

- интеграцией в инфраструктуру Active Directory;
- соответствием декларативной части настроек конфигураций конкретным дистрибутивным решениям;
- наличием не только управления конфигурациями компьютеров, но и конфигурациями пользователей.

**Управление политиками происходит или через знакомый всем администраторам Windows комплект приложений RSAT или посредством ADMS/GPUI**

# «Альт Домен» — SAMBA + GPO

- Групповая политика — это набор правил, в соответствии с которыми производится настройка рабочей среды относительно локальных политик, по умолчанию.
- Групповые политики применяются к компьютерам и пользователям.
- Групповые политики работают в рамках домена, где их создают системные администраторы.



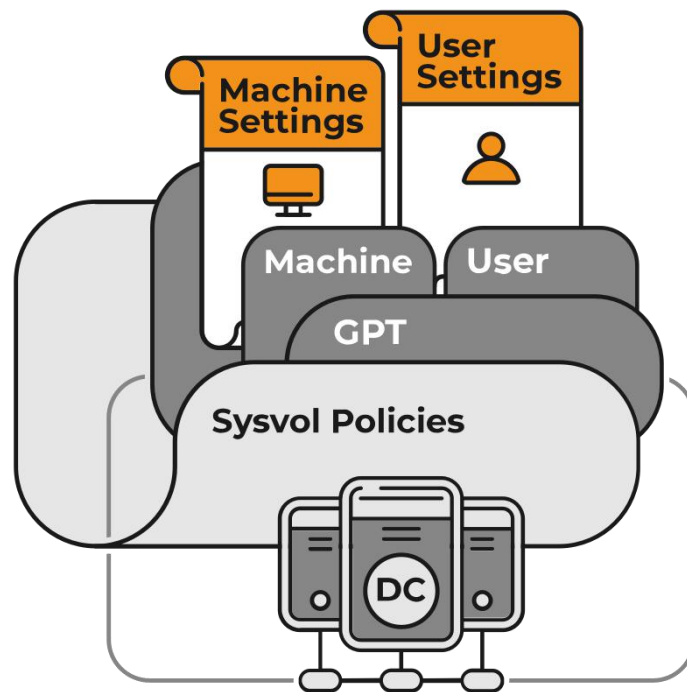
# Групповые политики в «Альт Домен»



## Групповые политики

### «Альт Домен» —

это комплексное решение, которое включает хранение политик и шаблонов в каталоге **Sysvol** на контроллере домена, инструменты управления политиками, и механизмы применения настроек для компьютеров и пользователей

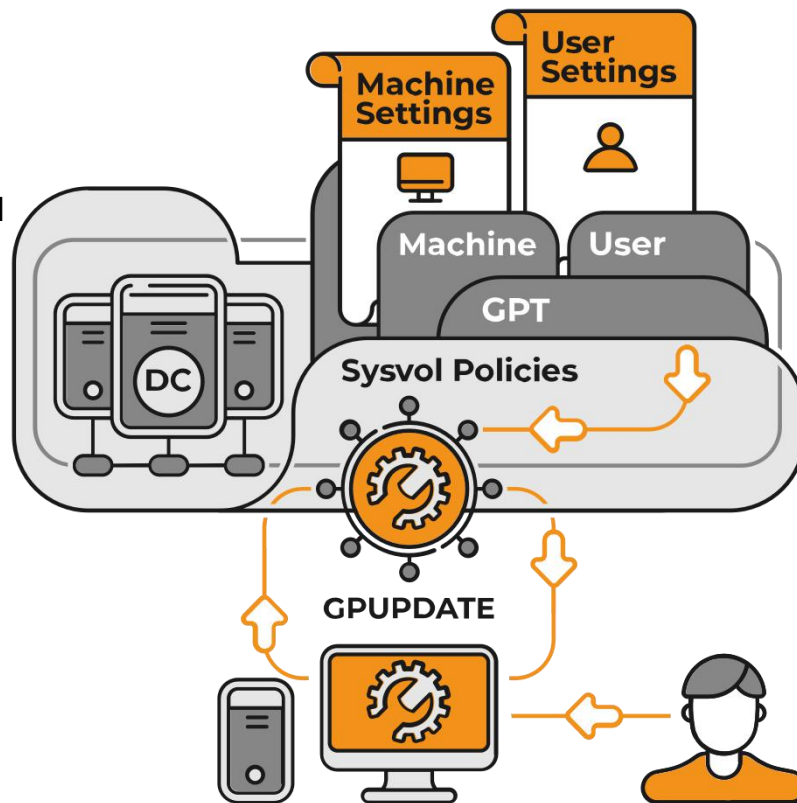


[Подробнее про групповые политики](#)



# Групповые политики в «Альт Домен»

Централизованное  
управление  
и настройка парка машин  
с ОС «Альт» производится  
через инструмент  
**GRUPDATE**



# Групповые политики в «Альт Домен»

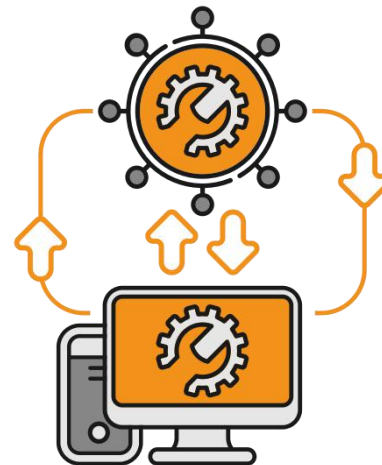
## Стабильные\*:

- Включение или выключение различных служб (сервисов systemd)
- Управление control framework
- Управление Gsettings
- Генерация ярлычков запуска программ
- Запрет на подключение внешних носителей данных
- Управление настройками браузеров: Firefox, Chromium, Яндекс-браузер
- Создание директорий

Machine

User

GPT



\* Работают по умолчанию

# Групповые политики в «Альт Домен»

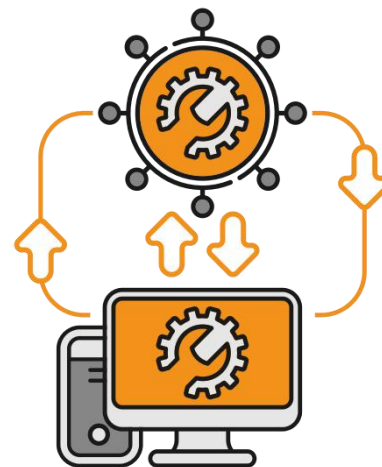
## Экспериментальные\*:

- Управление файлами (создание/удаление/ пересоздание)
- Управление logon-скриптами
- Подключение сетевых дисков
- Управление INI-файлами
- Управление настройками KDE Plasma
- Установка программного обеспечения
- Управление общими каталогами

Machine

User

GPT



\* Требуют специального включения

# Групповые политики в «Альт Домен»

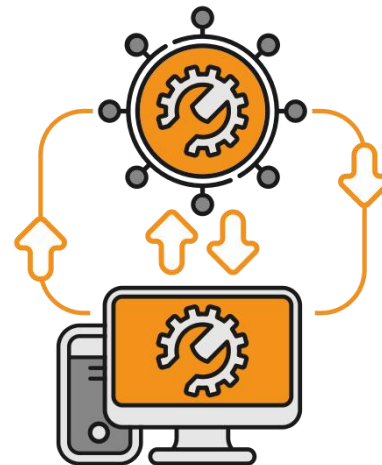
## Разрабатываемые:

- Управление графической средой KDE
- Политика паролей
- Установка пароля для локального пользователя root
- Подключение принтеров
- Синхронизация времени по NTP
- Информация о применении политик
- ...
- ? (Что могут предложить пользователи?)

Machine

User

GPT





# Групповые политики. Шаблоны



admx.help/?Category=ALTLinux

Microsoft >

Citrix >

Lenovo >

Google >

VMware >

Cjwdev >

Tracker Software >

Adobe >

Login Consultants Nederland B.V. >

Bentley >

Collabora >

Binary Fortress Software >

## ALT Linux

Active Directory Administrative Template for BaseALT distributions

Download

### Administrative Templates (Computers)

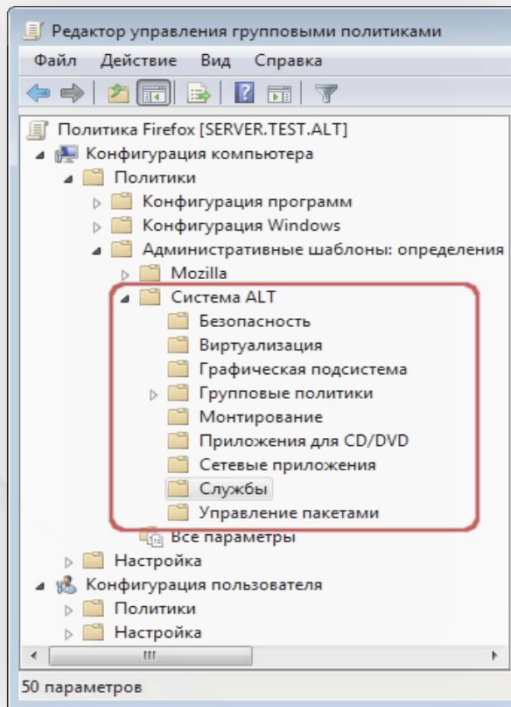
- ▼ ALT System
  - ▼ CD/DVD Applications
    - Permission to use /usr/bin/dvd+rw-booktype
    - Permission to use /usr/bin/dvd+rw-format
    - Permission to use /usr/bin/dvd+rw-mediainfo
    - Permission to use /usr/bin/dvd-ram-control
    - Permission to use /usr/bin/growisofs
  - ▼ Graphics
    - Function for saving the list of user directories
    - Permissions for Xorg
    - Show or hide the list of known users in the greeter (LightDM)
  - ▼ Group Policies
    - ▼ GUpdate Mechanisms
      - Chromium browser
      - Control system facilities
      - Firefox browser
      - Firewall configuration support
      - GSettings configuration



[ADMX шаблоны на международном ресурсе](https://admx.help/?Category=ALTLinux)



# Поддержка ОС «Альт» групповых политик MS AD и инструменты управления ими



## Реализованные политики:

- подключение разделяемых ресурсов;
- ограничение доступа к носителям, включая мобильные устройства;
- управление службами;
- управление каталогами;
- управление ярлыками на рабочем столе;
- управление доступом к виртуальным машинам и виртуализации;
- установка и удаление пакетов;
- управление внешним видом браузеров;
- управление оформлением рабочего стола;
- и др.

Управление политиками происходит через знакомый всем администраторам Windows комплект приложений RSAT. Нужен компьютер с Windows.

# ADMC как инструмент управления групповыми политиками MS AD



Инструмент **ADMC** создан как ответ на потребность в нативном инструменте для работы с доменом Active Directory и групповыми политиками.

**ADMC предназначен** для управления:

- объектами в домене (пользователями, группами, компьютерами, подразделениями);
- групповыми политиками.



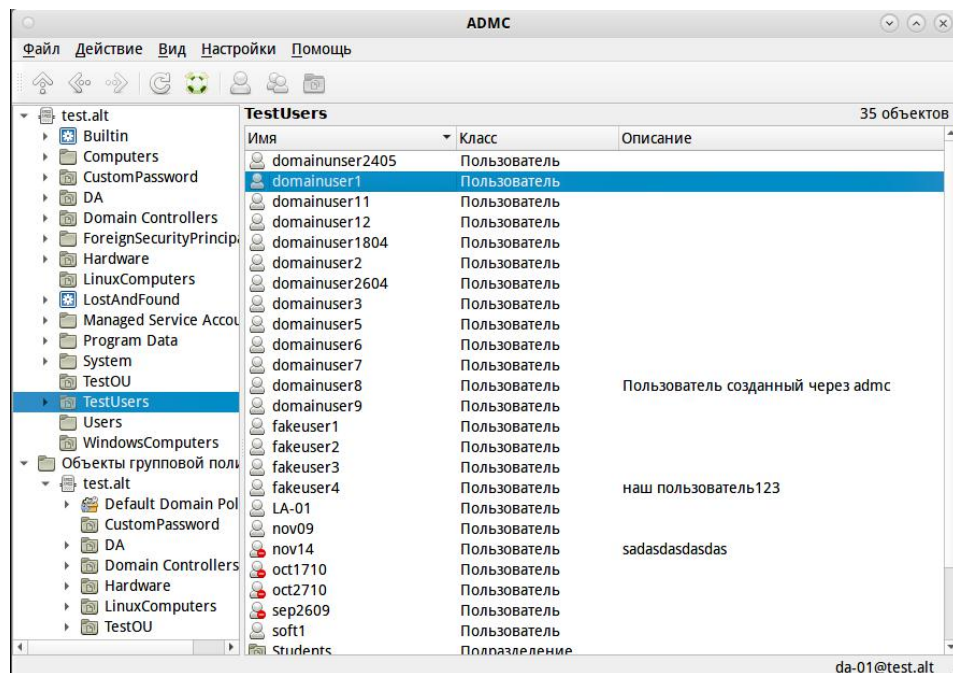
[Подробнее про ADCM на нашей WIKI](#)



# ADMC — альтернатива ADUC

**Простой  
графический  
инструмент  
для работы  
с доменом AD  
(Samba DC)**

**Переосмысливает  
пользовательский  
опыт работы  
с RSAT**

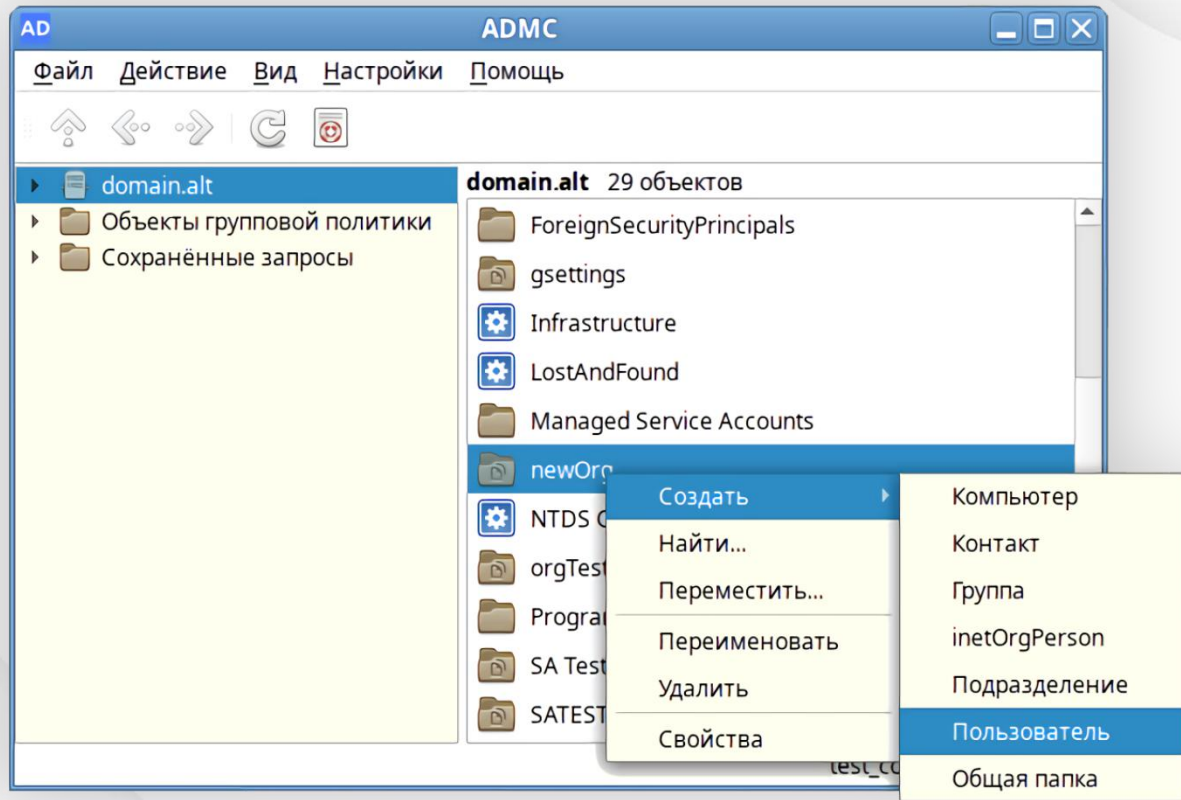


**Проект развития групповых политик и графического инструмента управления продолжается совместно с мейнстримом проекта Samba**





# ADMC. Создание пользователя





# ADMC. Внесение данных пользователя

The image shows a screenshot of the ADCM (Active Directory Configuration Manager) interface. The main window is titled 'ADCM' and has a menu bar with 'Файл', 'Действие', 'Вид', 'Настройки', and 'Помощь'. Below the menu bar is a toolbar with icons for home, back, forward, refresh, and a warning icon. The left pane shows a tree view of the domain 'domain.alt' with various folders like 'Allow Login', 'Allow/Deny Login', 'Builtin', 'com1', 'Computers', 'Deny Login', 'desktop', 'Domain Controllers', 'Enterprise-AAV', 'ForeignSecurityPrincipals', 'gsettings', 'LostAndFound', 'Managed Service Accounts', 'newOrg' (selected), 'orgTest', 'Program Data', and 'SA Test Department'. The right pane is titled 'Создать пользователя — ADCM' and contains the following fields and options:

- Имя:
- Фамилия:
- Полное имя:
- Инициалы:
- Имя для входа:  - Имя для входа (до Windows 2000):
- Пароль:
- Подтвердите пароль:
- ☐ Показывать пароль
- Параметры учётной записи:
  - ☒ Пользователь должен сменить пароль при следующем входе в систему
  - ☐ Пользователь не может изменить пароль
  - ☐ Пароль не истекает
  - ☐ Учётная запись отключена

At the bottom right of the dialog are two buttons: 'Отмена' (Cancel) and 'ОК' (OK).



# ADMC. Просмотр свойств пользователя

AD

ТестФ Тести — свойства — ADCM

Общее

Объект

Атрибуты

Адрес

Организация

Телефоны

Учётная запись

Группы

Делегирование

Безопасность

| Имя             | Значение        | Тип                   |
|-----------------|-----------------|-----------------------|
| USNIntersite    | <без значени... | Целое число           |
| aCSPolicyN...   | <без значени... | Юникод                |
| accountExp...   | (никогда)       | Большое целое число   |
| accountNa...    | <без значени... | Юникод                |
| adminCount      | <без значени... | Целое число           |
| adminDesc...    | <без значени... | Юникод                |
| adminDispl...   | <без значени... | Юникод                |
| allowedAttr...  | <без значени... | Идентификатор объекта |
| allowedAttr...  | <без значени... | Идентификатор объекта |
| allowedChil...  | <без значени... | Идентификатор объекта |
| allowedChil...  | <без значени... | Идентификатор объекта |
| altSecurityI... | <без значени... | Юникод                |
| assistant       | <без значени... | Различающееся имя     |
| attributeCe...  | <без значени... | Октет                 |
| audio           | <без значени... | Октет                 |
| badPasswo...    | (никогда)       | Большое целое число   |
| badPwdCo...     | 0               | Целое число           |
| bridgehead...   | <без значени... | Различающееся имя     |
| businessCa...   | <без значени... | Юникод                |
| c               | <без значени... | Юникод                |
| canonicalN...   | <без значени... | Юникод                |
| carLicense      | <без значени... | Юникод                |
| cn              | ТестФ Тести     | Юникод                |
| co              | <без значени... | Юникод                |
| codePage        | 0               | Целое число           |
| comment         | <без значени... | Юникод                |
| company         | <без значени... | Юникод                |

Изменить...

Фильтр

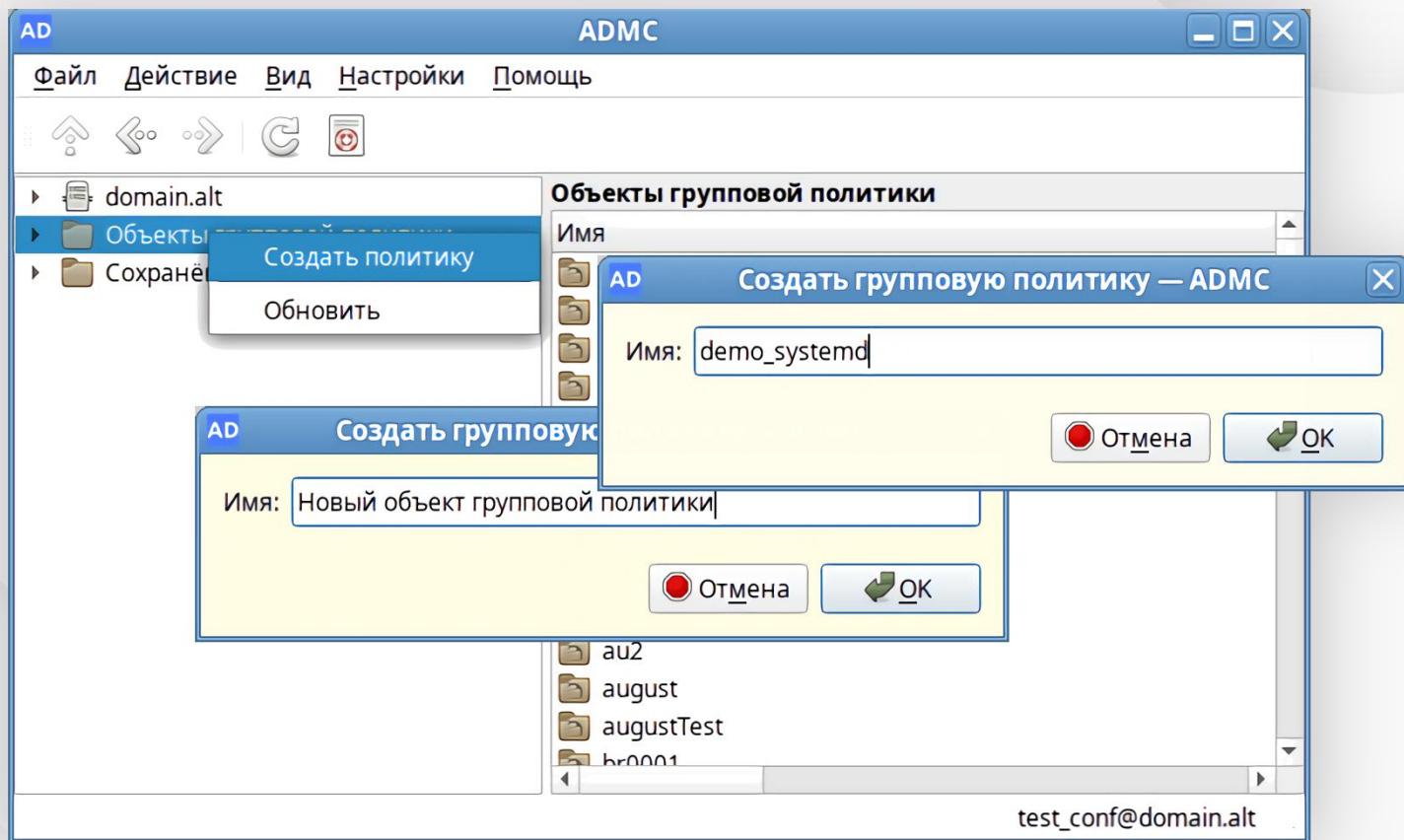
Сбросить

Применить

Отмена

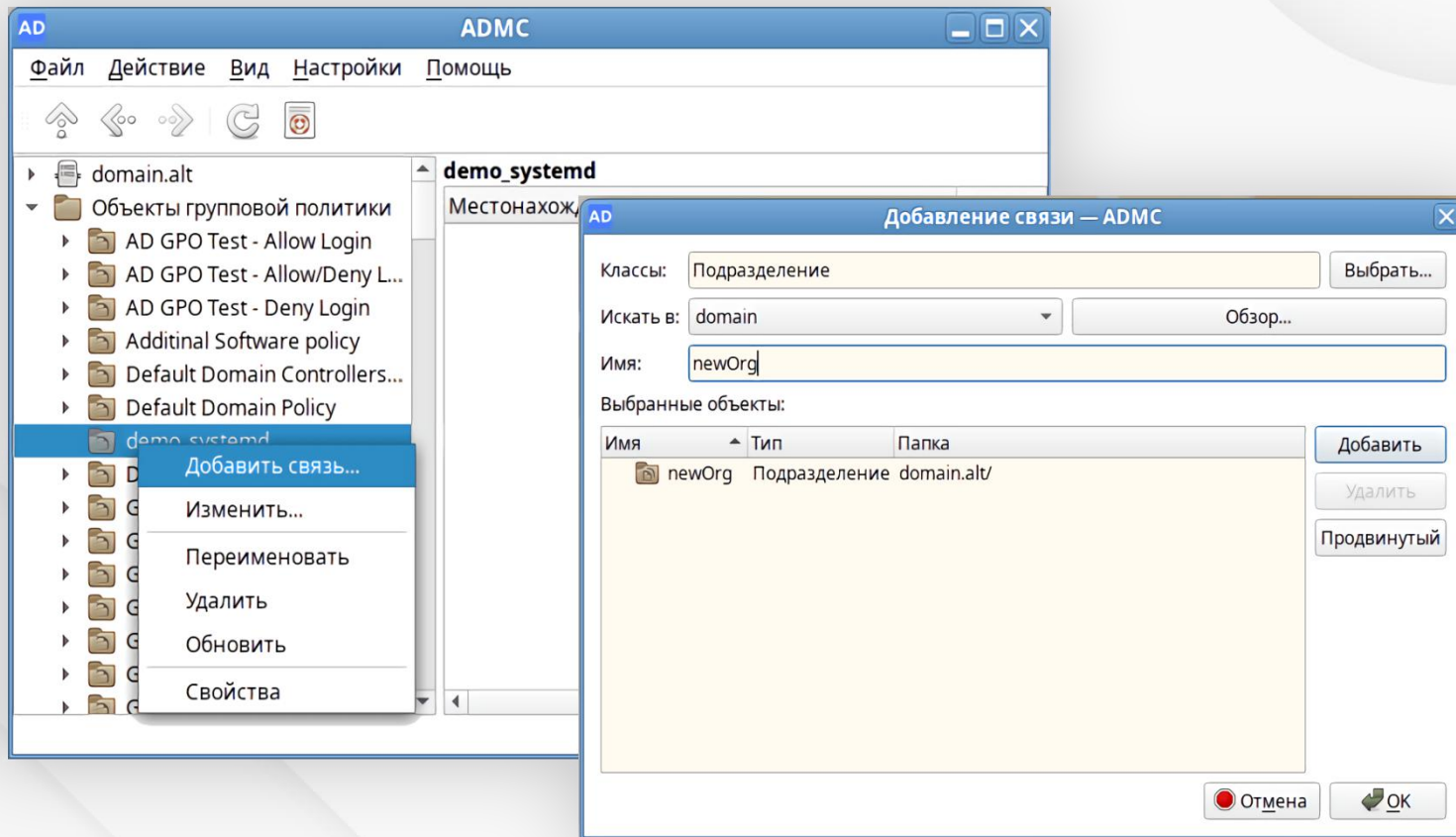
OK

# ADMC. Создание политики



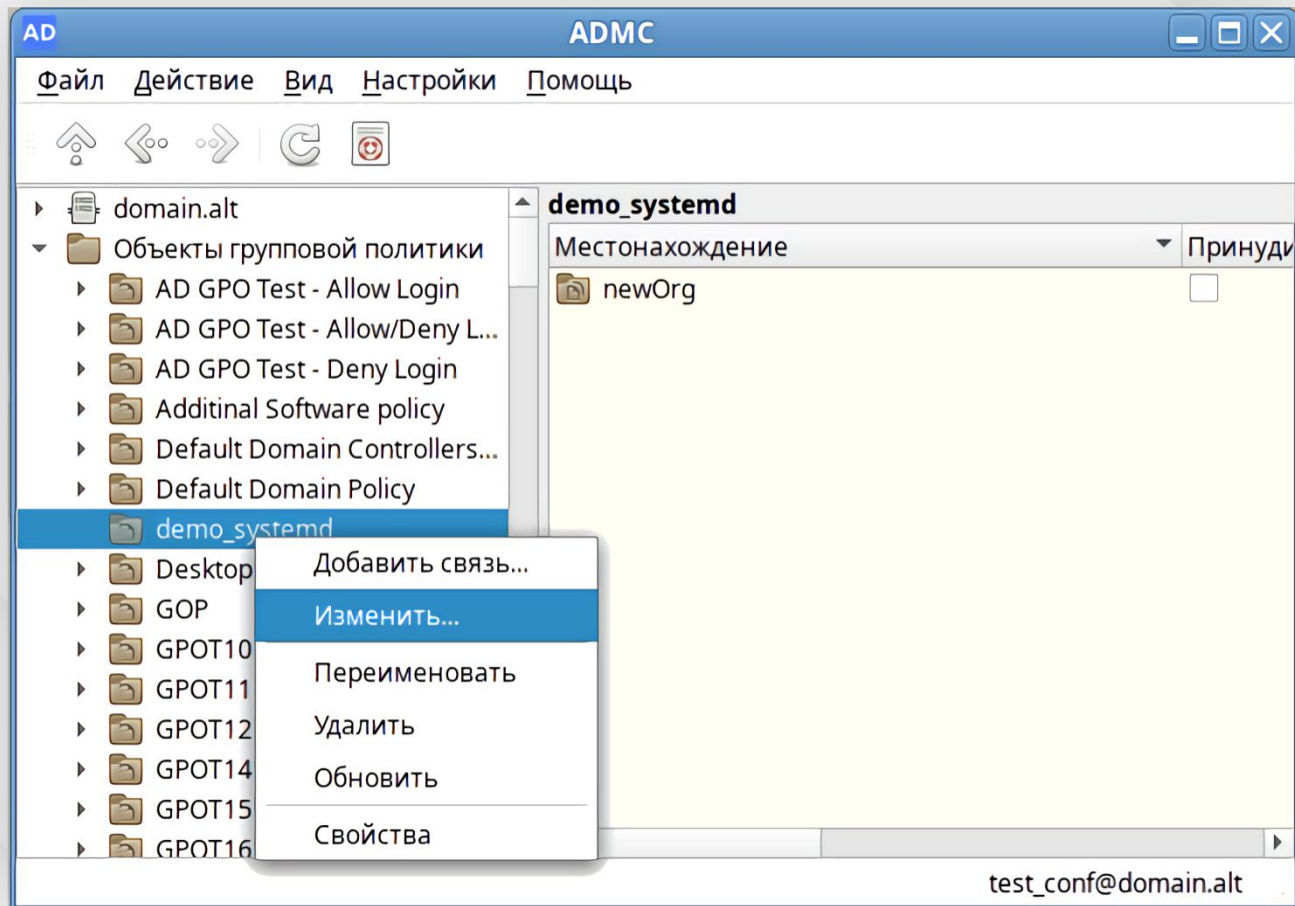


# ADMC. Создание политики. Добавление связи

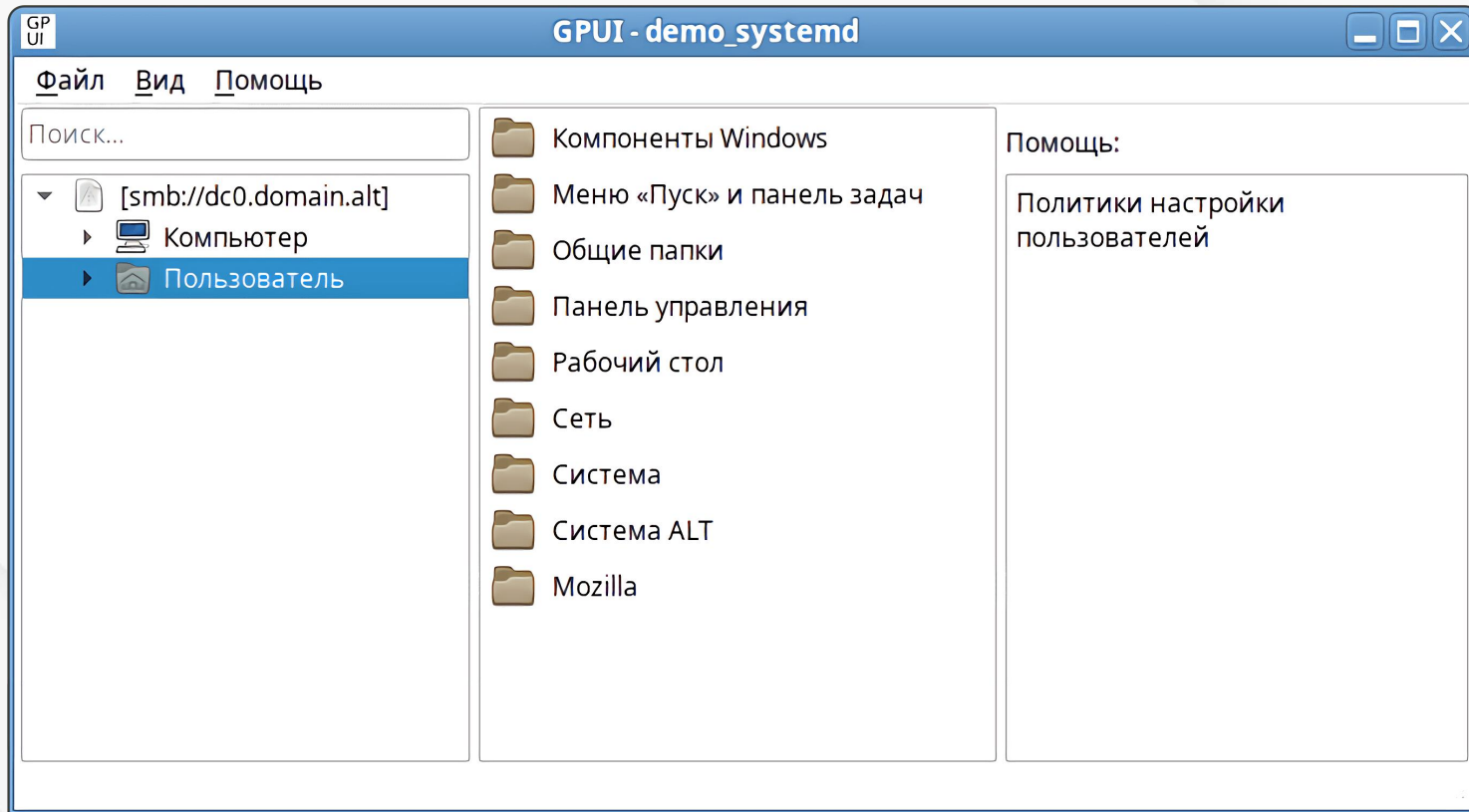




# ADMC. Создание политики. Изменение



# GPU! — редактор политик

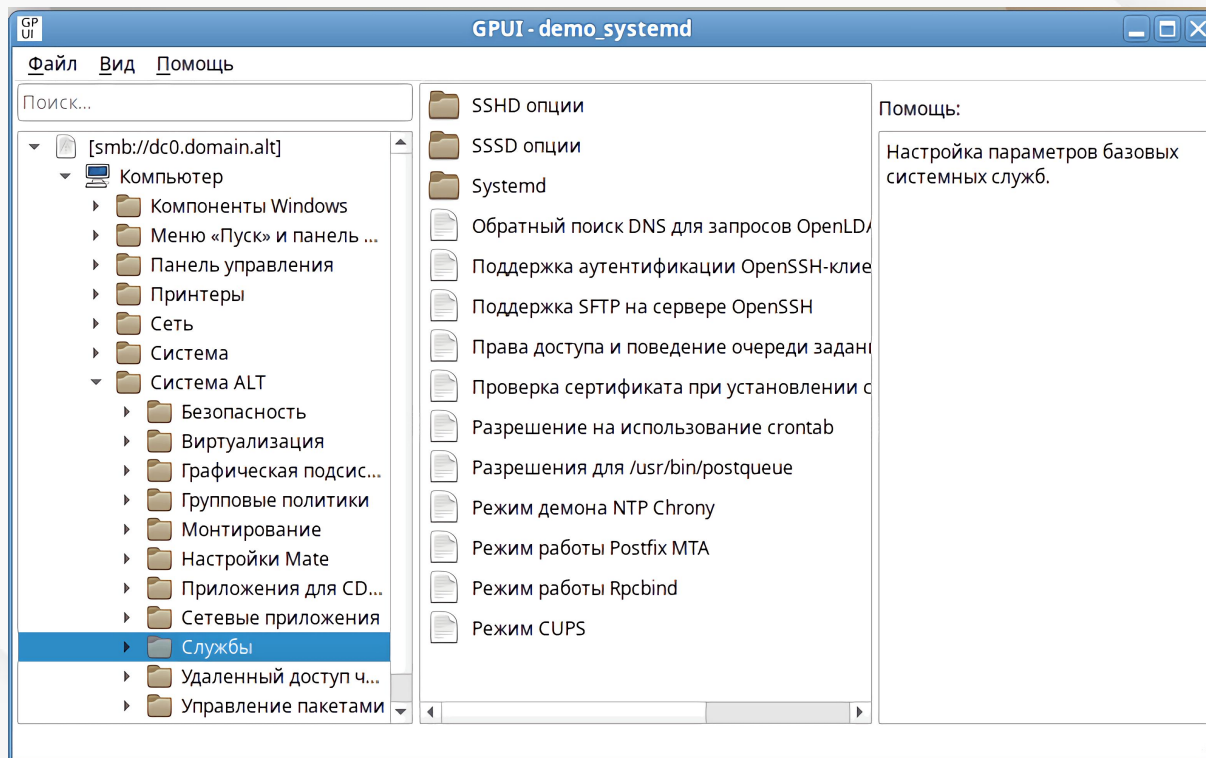


[Подробнее о GPU!](#)





# GPUI — редактор политик. Службы

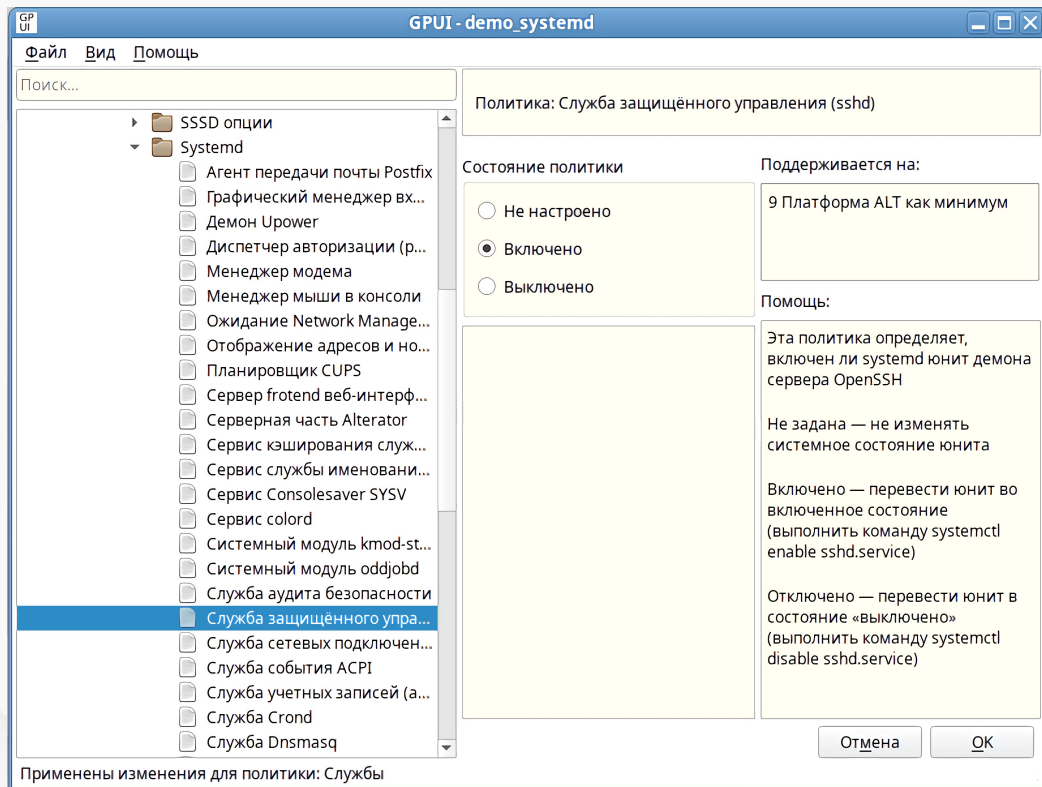


[Подробнее о GPUI](#)





# GPUI — редактор политик. Службы. Состояние



[Подробнее о GPUI](#)

# Групповые политики. Включение



Центр управления системой (от суперпользователя)

↑ Главная ★ Режим эксперта ✕ Выход ? Справка

☐ Локальная база пользователей

☐ Домен ALT Linux или Astra Linux Directory

Домен:

☐ Кэшировать аутентификацию при недоступности сервера домена

☒ Домен Active Directory

Домен:

Рабочая группа:

Имя компьютера:

☐ Домен FreeIPA

Домен:

Имя компьютера:

Внимание!

**Изменение домена заработает только после перезагрузки компьютера**

Введите пароль для учётной записи с правами подключения к домену.

Имя пользователя:

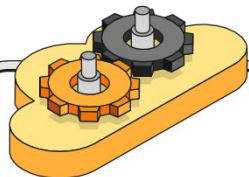
Пароль:

☒ Включить групповые политики

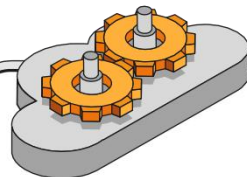


[Подробнее о GPU!](#)

# Подходы к миграции доменной инфраструктуры



**Замещающая**  
миграция — плавный  
перевод инфраструктуры  
на Samba Active  
Directory. Клиенты —  
Windows и Linux.



**Параллельная**  
миграция — на любое  
аналогичное  
инфраструктурное  
решение, например,  
FreeIPA. Клиенты —  
только Linux.

**Миграция — это замена операционных систем клиентов и серверов под управлением семейства ОС Windows на базе инфраструктуры Microsoft Active Directory на аналогичные по функциональным возможностям свободные операционные системы и инфраструктурные решения.**

# Сценарий «замещающей» миграции доменной инфраструктуры MS AD на Samba DC

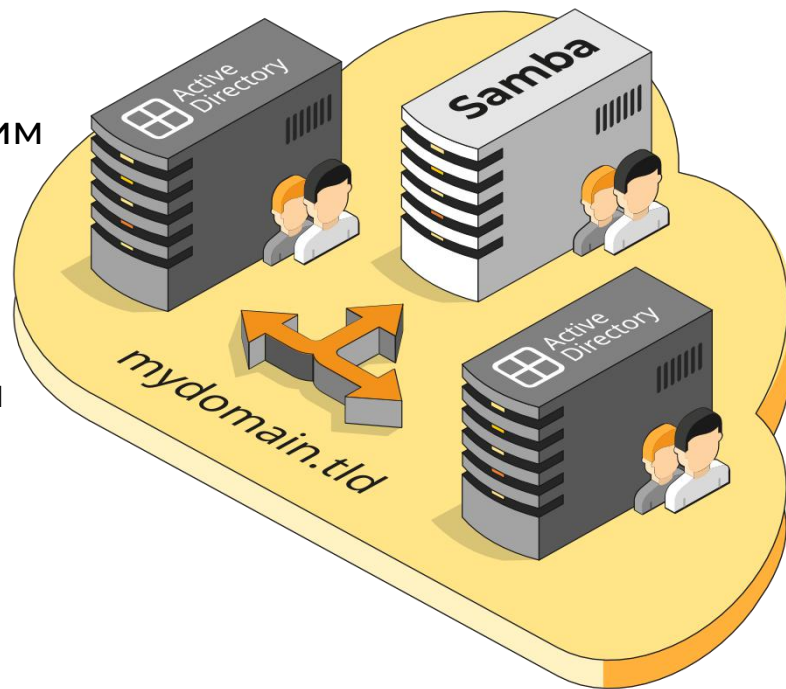
Единовременное замещение имеющихся контроллеров домена (КД) **MS AD** на контроллеры домена (КД) **Samba**; основная часть учётных данных из базы **MS AD** сохраняется.



В зависимости от конфигурации сетевой инфраструктуры (DNS, DHCP), новые контроллеры могут дублировать имена и IP-адреса своих MS AD прототипов.

# Замещающая миграция: особенности

- Имя домена остаётся прежним
- **SID\*** домена остаётся прежним
- Сохраняются аккаунты и пароли пользователей
- Сохраняются группы
- Сохраняются подразделения
- Сохраняются машинные аккаунты
- Сохраняются **DNS**-записи



\* Идентификатор безопасности



# Замещающая миграция

## Этапы процесса

1. Подготовка закрытого окружения
2. Выгрузка слепка базы из **MS AD**
3. Развёртывание первого КД **Samba DC** с использованием полученной базы
4. Дублирование структуры парка КД **MS AD**, но уже на **Samba DC**
5. Публикация полученной доменной инфраструктуры



# Замещающая миграция

## 1. Подготовка закрытого окружения

Под закрытым окружением здесь подразумевается сетевое окружение, отрезанное от оригинальной **MS AD** инфраструктуры и позволяющее использовать **IP**-адреса **MS AD** контроллеров домена без конфликтов.

Такое окружение позволяет свободно построить доменную инфраструктуру на базе **Samba DC**, дублирующую оригинальную инфраструктуру **MS AD**, отработать процесс переноса слепка базы **MS AD** на КД с **Samba DC** и проверить получившийся результат.

В окружении рекомендуется развернуть следующие машины:

- Промежуточный КД **MS AD** (если необходим);
- Сервер с **Samba DC** на базе **ALT Server**;
- Рабочая станция на базе **MS Windows**;
- Рабочая станция с **ALT Workstation**.



# Замещающая миграция

## 2. Выгрузка слепка базы из MS AD

Создание полного слепка базы MS AD является ключевым этапом миграции доменной инфраструктуры.

Для создания этого слепка существует два варианта:

- **Выгрузка базы в закрытом окружении**  
Подразумевает создание промежуточного КД MS AD, его очистку и перенос в закрытое окружение. Затем производится выгрузка базы.
- **Выгрузка базы в рабочем окружении**  
Выгрузка базы производится напрямую с одного из КД рабочей MS AD инфраструктуры. В процессе производится исключительно чтение данных с КД, потому **оригинальная MS AD** инфраструктура **не будет затронута**.





# Замещающая миграция

## 3. Развёртывание первого контроллера домена Samba DC с использованием полученной базы

Этап восстановления из файла резервной копии аналогичен развёртыванию домена, который выполнялся при первой настройке сети Samba, за исключением того, что резервная копия содержит в себе все объекты базы данных, которые были добавлены с момента создания домена.

Как и при создании нового домена, при запуске команды восстановления домена потребуется указать новый контроллер домена. Этот контроллер домена **не должен был существовать** ранее в сети Samba.

# Замещающая миграция



Заключительные шаги 4 и 5

**4.** Дублирование структуры парка КД MS AD, но уже на Samba DC.

**5.** Публикация полученной доменной инфраструктуры.



Подробнее на [wiki Alt Linux](#)



# Преимущества решения «Альт Домен»

- **«Альт Домен» основан на свободном проекте Samba**, разработка идет с ведома и согласия upstream пакета Samba, что говорит о качестве кода; шаблоны и весь код наших доработок открыты. Проект постоянно обновляется и развивается.
- **Бесшовная миграция** — в имеющийся домен «плавно вливаются» машины с ОС «Альт» без каких-либо изменений в имеющемся домене Windows.
- **Управление «Альт Доменом»** возможно знакомыми всем администраторам инструментами MS RSAT (на Windows) или нативными (для Linux) инструментами ADMC/GPUI, разработанными «Базальт СПО». Это позволяет, в итоге, совсем отказаться от использования MS Windows.
- **«Альт Домен» обеспечивается технической поддержкой от вендора** в соответствии с SLA\*.
- **С помощью групповых политик «Альт Домена»** можно управлять пользователями и компьютерами.
- В **«Альт Домен»** можно включить Linux-решения от других разработчиков (требуется сборка инструментов «Базальт СПО» для целевой ОС).

\* Программный комплекс «Альт Домен»:

- развёртывается на базе ОС «Альт Сервер» или на базе ОС «Альт СП Сервер»,
- лицензируется и поддерживается отдельно.



# Сравнение «Альт Домен» с решением на FreeIPA

- **FreeIPA** (авторы из RedHat), **ориентирован только на Linux**.
- **FreeIPA не имеет политик для пользователей**, только для компьютера/сервера.
- **Миграция** на FreeIPA возможна только как параллельный домен рядом с имеющимся доменом с односторонним трастом — это дополнительные затраты на обслуживание и обучение персонала.
- Для организации сервиса **обмена файлами** с компьютерами на Windows нужно развёртывать Samba.
- Требуется переобучения персонала с Windows на Linux.

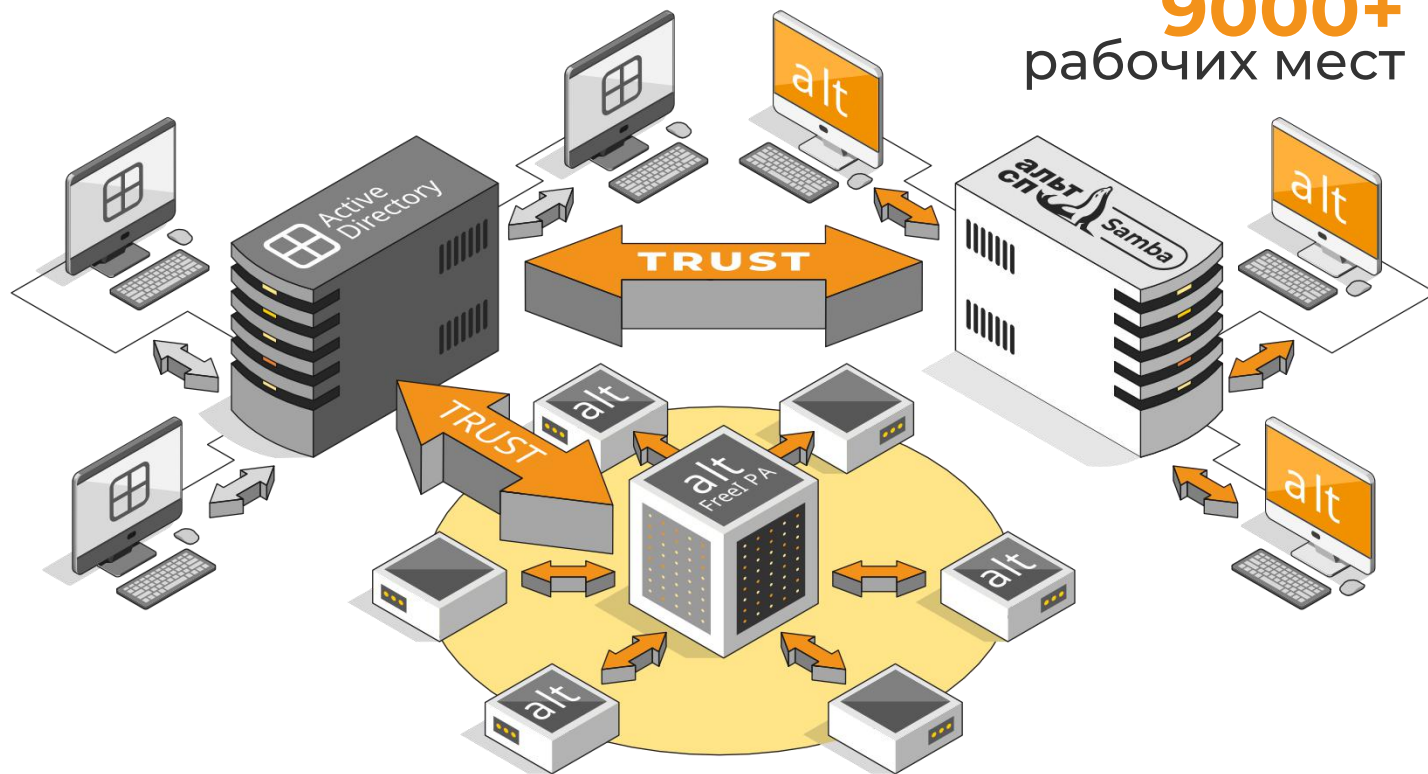
**ОС «Альт» поддерживают оба варианта: Samba DC и FreeIPA**



# Внедрения: ПАК «Патриот» (Новосибирская область)

Samba DC и FreeIPA

**9000+**  
рабочих мест





# Внедрения: школа в Нижнем Тагиле

## Samba DC

Компьютерный парк школы – более 500 единиц, из них под управлением ОС «Альт» – работают 186 ПК.

ОС «Альт Сервер» 10 с установленной утилитой **ADMC** и Windows 7 с RSAT — контроллер домена и место администратора.

*«Утилиты имеют схожий интерфейс и внутреннюю логику, что очень упрощает их совместное использование. Заложенные в **ADMC** возможности перекрывают большую часть задач, возникающих в повседневной работе с доменом: создание и редактирование информации о пользователях и компьютерах, настройка общих папок и так далее. RSAT используется для настройки групповых политик в той части, которая пока не реализована средствами **ADMC**. По мере увеличения функциональности встроенных в ОС «Альт» средств управления доменом — в частности, **ADMC** и **GPUI** — ИТ-специалисты школы планируют отказаться от использования связки Windows–RSAT».*

Александр Клепалов,  
инженер-электроник Нижнетагильской школы №100.



### **Контакты:**

**Тел.:** +7 (495) 123-47-99

**E-mail:** [sales@basealt.ru](mailto:sales@basealt.ru)

Бесплатная техническая  
поддержка на этапе  
тестирования:  
**[basealt.ru/sales2](http://basealt.ru/sales2)**

### **Офисы:**

**Москва**, ул. Бутырская, д. 75

**Санкт-Петербург**, 4-я линия В.О., д. 17, БЦ «ЛВА»

**Саратов**, ул. Октябрьская 44, корпус А, офис № 3

**Обнинск**, ул. Королёва, д. 4Б, БЦ «Британика»

**[www.basealt.ru](http://www.basealt.ru)**