

**base  
alt**



**ООО «Базальт СПО»**

**Миграция инфраструктуры  
предприятия – миссия  
выполнима!**

**Владимир Чёрный**

Директор по продуктам  
ООО «Базальт СПО»  
black@basealt.ru

# Проблемы мешающие продолжать использовать AD

- Санкции:
  - × нельзя продлить лицензии,
  - × получить техподдержку.
- Требования безопасности
- Постановления Правительства № 166, 250...



# Возможности ПК «Альт Домен»

- ✓ Единая точка аутентификации (включая SSO)
- ✓ Удобное управление политиками (централизованное управление конфигурациями машин и пользователей)
- ✓ Безопасность (Kerberos v5)
- ✓ Отказоустойчивость (репликация между КД)
- ✓ Удобный обмен файлами
- ✓ Возможность расширения схемы (sudo, LAPSV2, ssh keys)
- ✓ Поддержка аппаратных архитектур (x86, ARM64, e2kv4-v6 )
- ✓ Привычная системным администраторам Windows логика работы и функционал системы.



# Чем заменить AD?

(Что есть в мире Linux?)

- **LDAP + Kerberos** (уже не используется)
- **Samba AD** (независимый, международный, много пользователей, поддержка MS Windows)
- **FreeIPA** (Red Hat, US, только Linux)



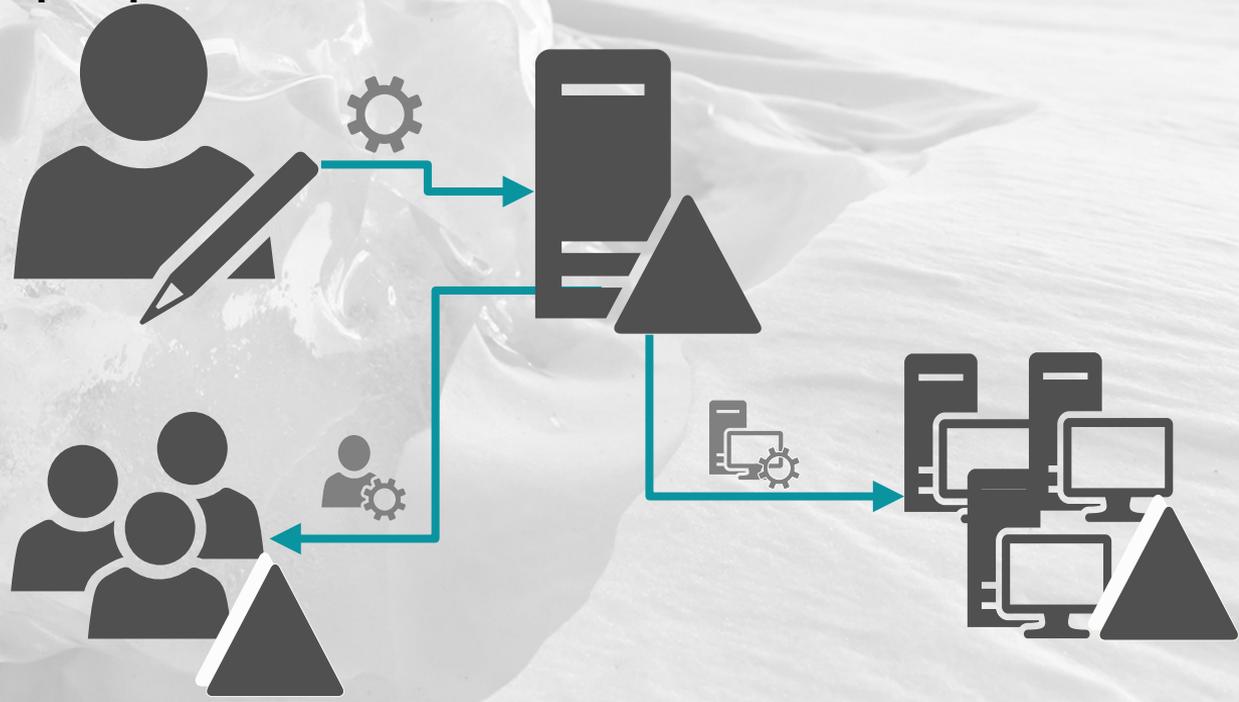
# Наш выбор: SAMBA + GRO = Альт Домен

- **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**



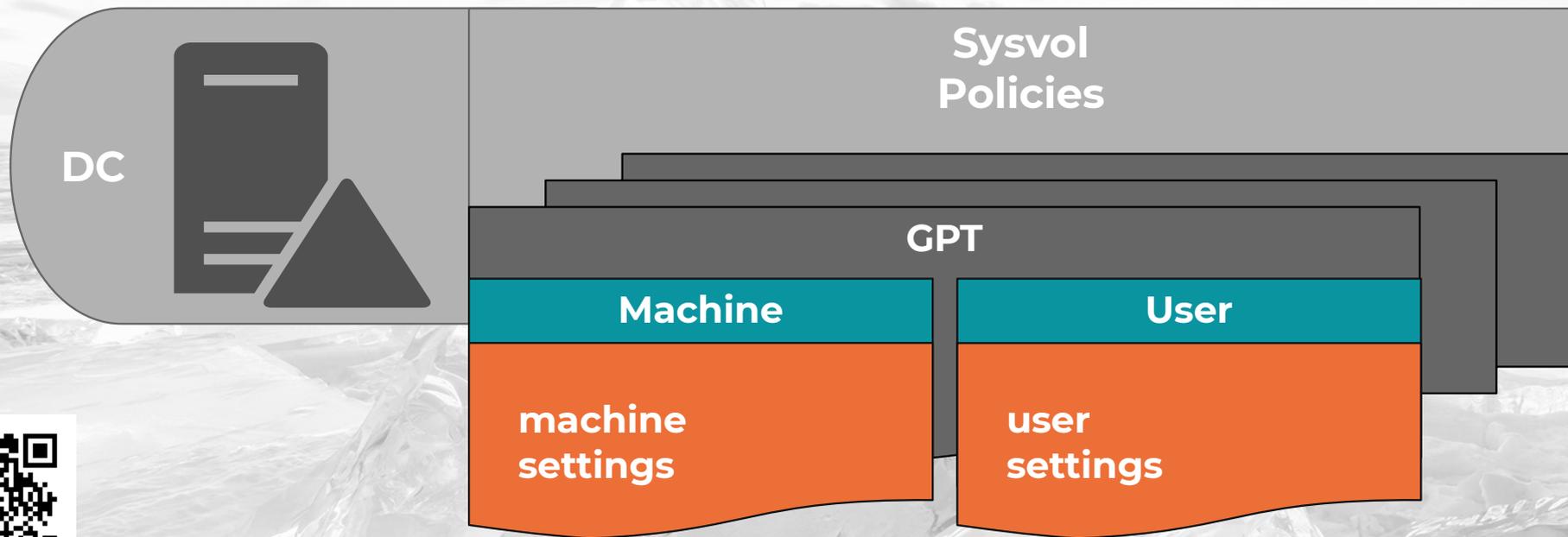
# Альт Домен — SAMBA + GPO

- 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»

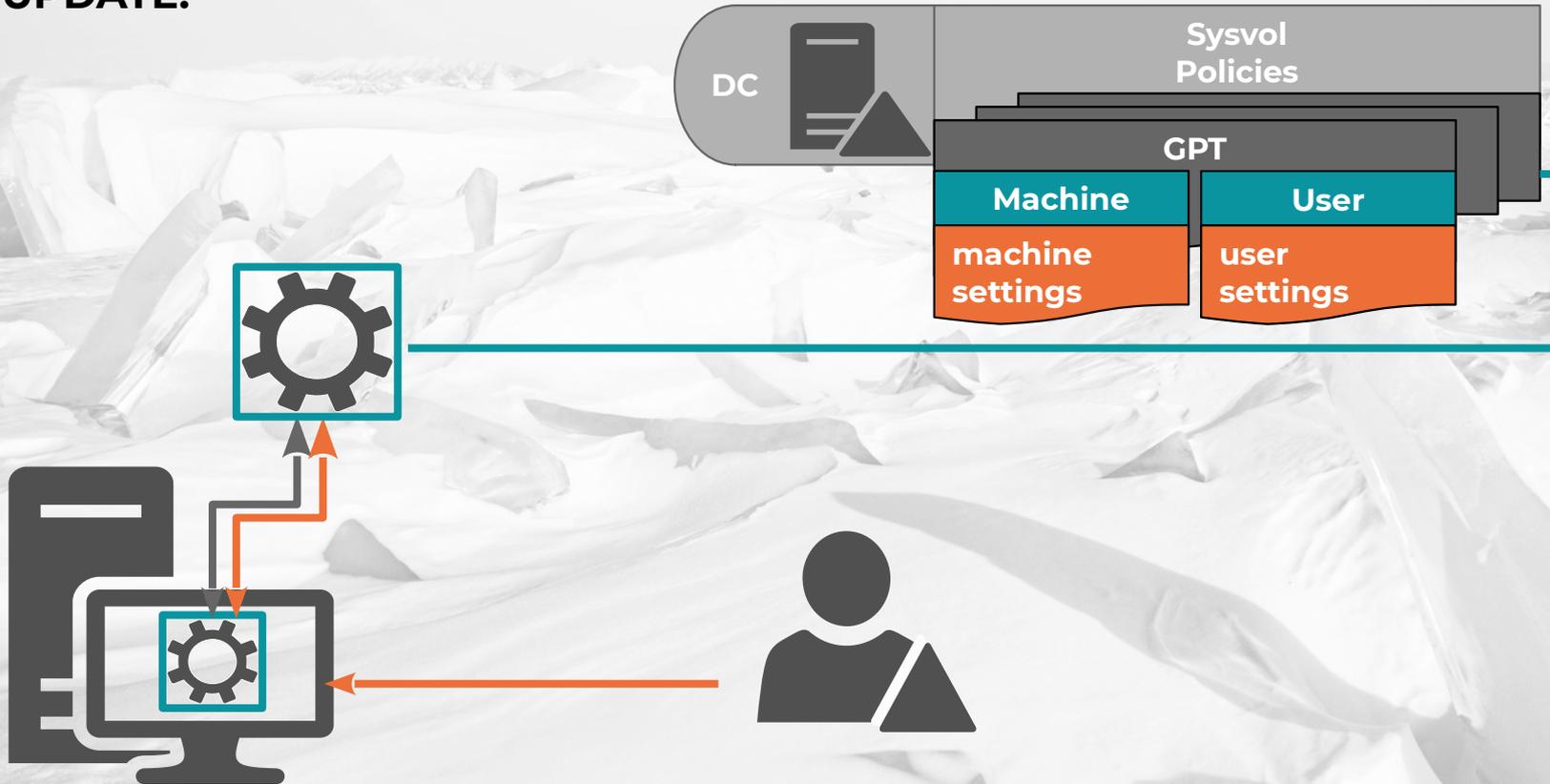
Групповые политики «Альт Домен» — это комплексное решение, которое включает хранение политик и шаблонов в каталоге Sysvol на контроллере домена, инструменты управления политиками, и механизмы применения настроек для компьютеров и пользователей.



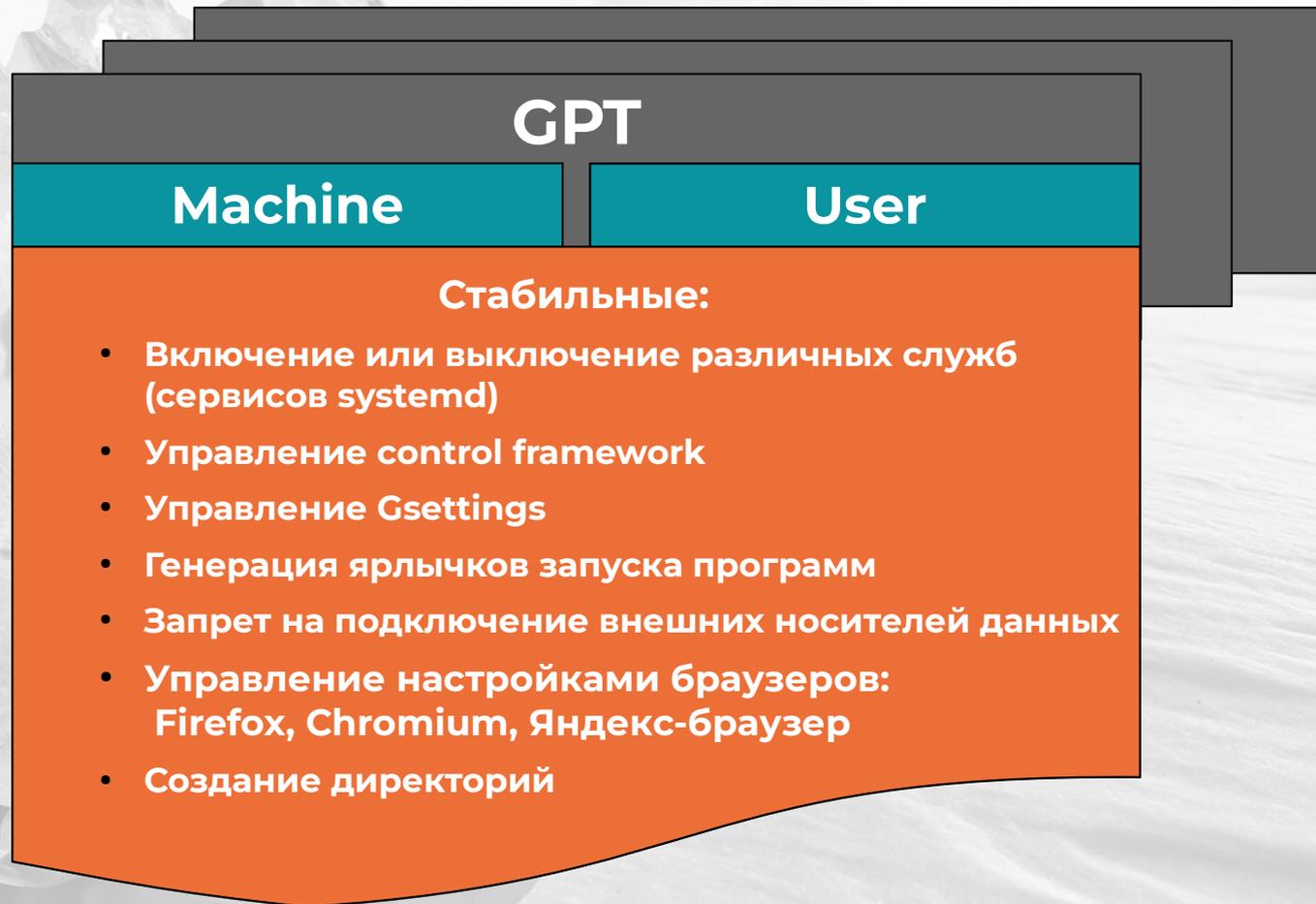
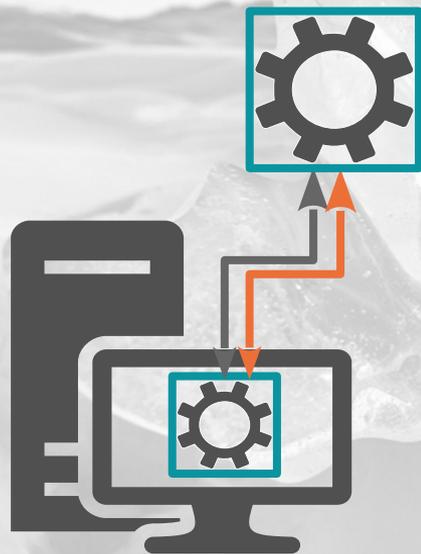
[Подробнее про групповые политики](#)

# Групповые политики в «Альт Домен»

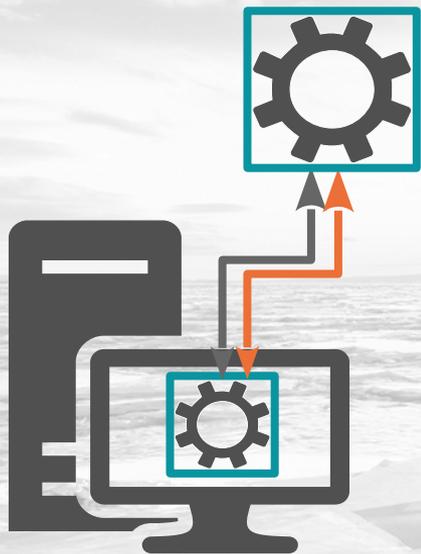
Централизованное управление и настройка парка машин с ОС «Альт» производится через инструмент GRUPDATE.



# Групповые политики в «Альт Домен»



# Групповые политики в «Альт Домен»



# 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 >

Duo Security >

FSLogix >

Mozilla Firefox and Thunderbird >

Community >

Foxit Software Inc. >

## 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 directo
    - Permissions for Xorg
    - Show or hide the list of known users in the greeter (LightDM)
  - Group Policies
    - GPUUpdate Mechanisms
      - Chromium browser
      - Control system facilities
      - Firefox browser
      - Firewall configuration support
      - GSettings configuration
      - GSettings mechanisms for users
      - Install and remove for users
      - Install and remove packages
      - Local folders control
      - Local folders control for users
      - Network drives mounting for users
      - PolicyKit authorization
      - PolicyKit authorization for users



ADMX шаблоны на международном ресурсе



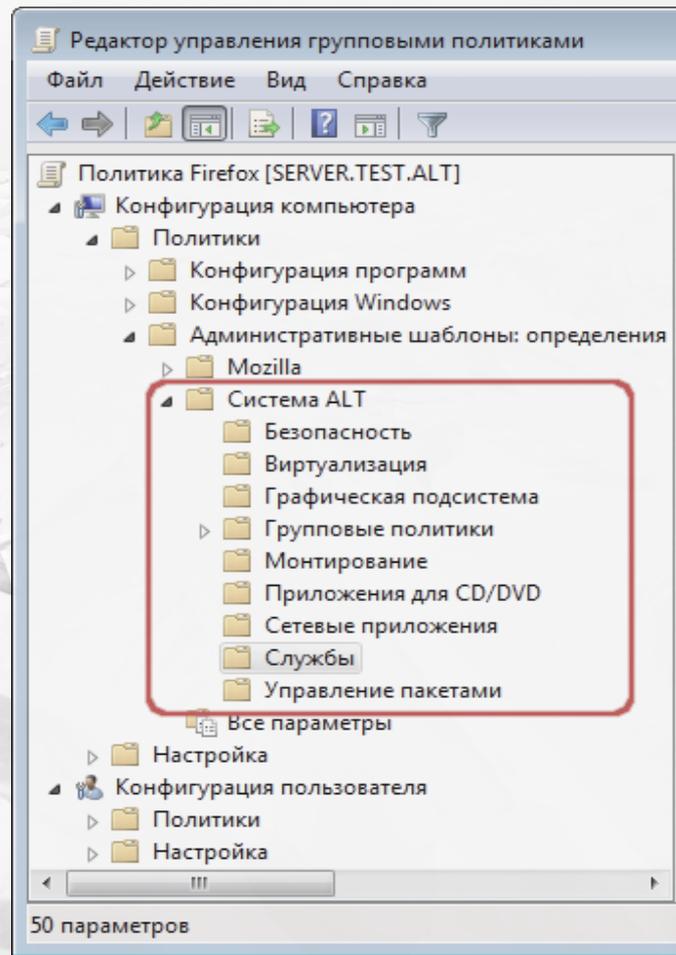


# Инструменты управления групповыми политиками MS AD

## Управление политиками происходит через знакомую всем администраторам Windows оснастку RSAT

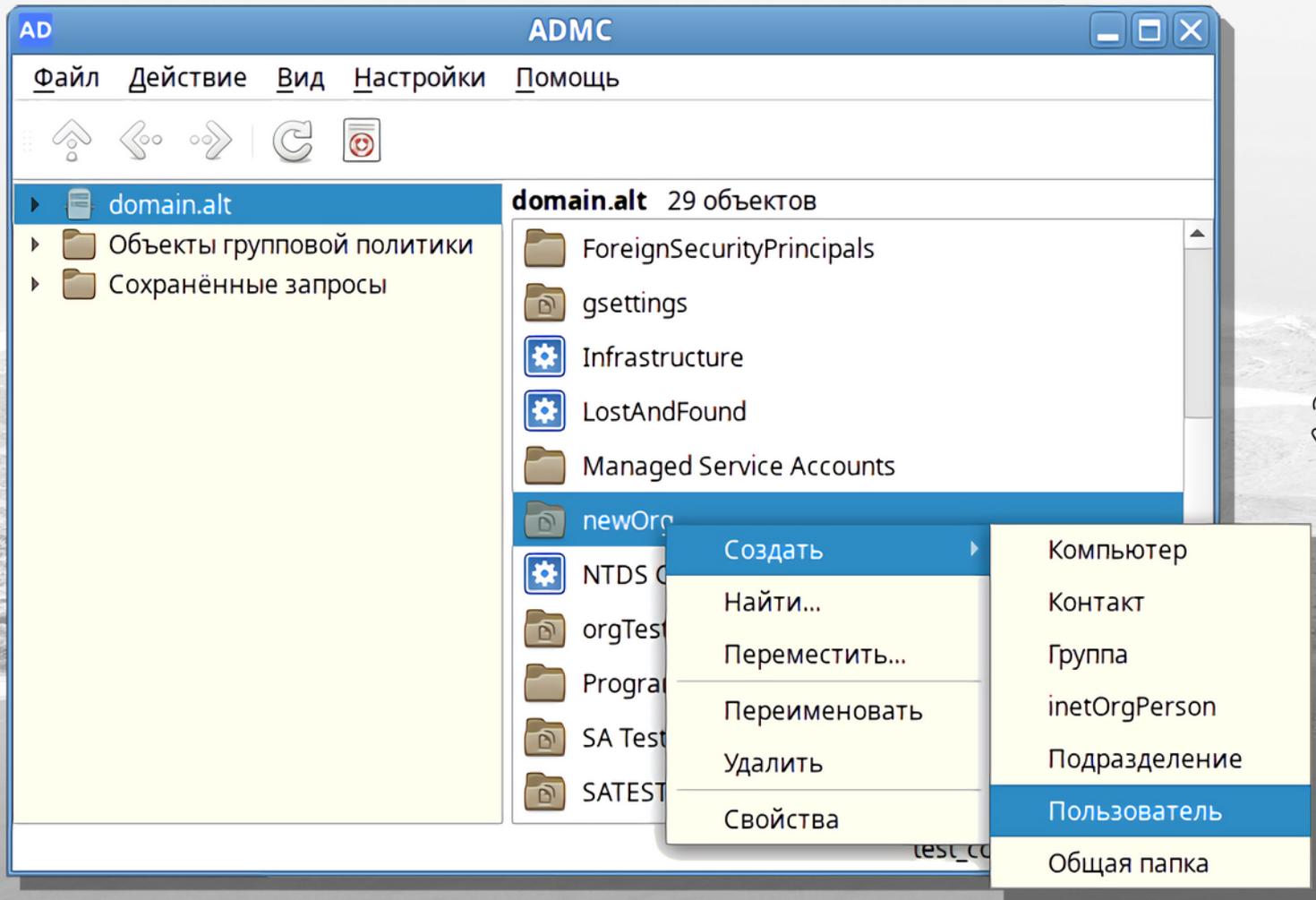
### Реализованные политики:

- 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 браузерами FF, Chromium, Ynadex-browser;
- управление средой рабочего стола MATE/КДЕ
- выполнение скриптов при входе/выходе, включении/выключении
- и др.



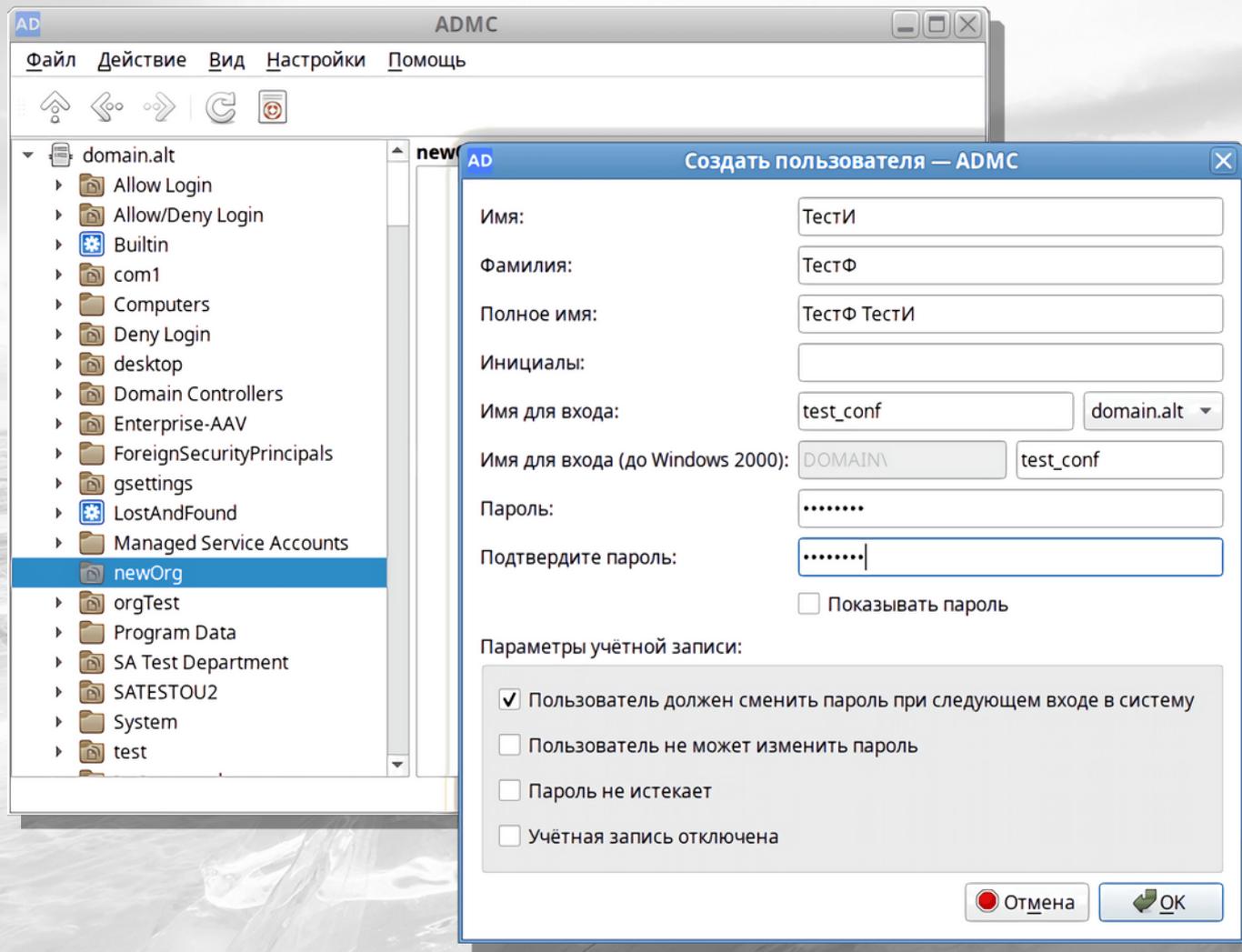


# ADMC. Создание пользователя



[Подробнее о ADCM](#)

# ADMS. Внесение данных пользователя



The image shows the ADMS (Active Directory Management Service) console interface. The main window displays a tree view of the domain structure, with 'newOrg' selected under 'domain.alt'. A dialog box titled 'Создать пользователя — ADMS' is open, allowing the creation of a new user. The dialog contains the following fields and options:

- Имя:** Тести
- Фамилия:** ТестФ
- Полное имя:** ТестФ Тести
- Инициалы:** (empty)
- Имя для входа:** test\_conf (domain: domain.alt)
- Имя для входа (до Windows 2000):** DOMAIN test\_conf
- Пароль:** (masked with dots)
- Подтвердите пароль:** (masked with dots)
- 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

Buttons at the bottom: Отмена (Cancel), OK.



# ADMC. Просмотр свойств пользователя

AD ТестФ Тести — свойства — ADCM

Общее  
Объект  
Атрибуты  
Адрес  
Организация  
Телефоны  
Учётная запись  
Группы  
Делегирование  
Безопасность

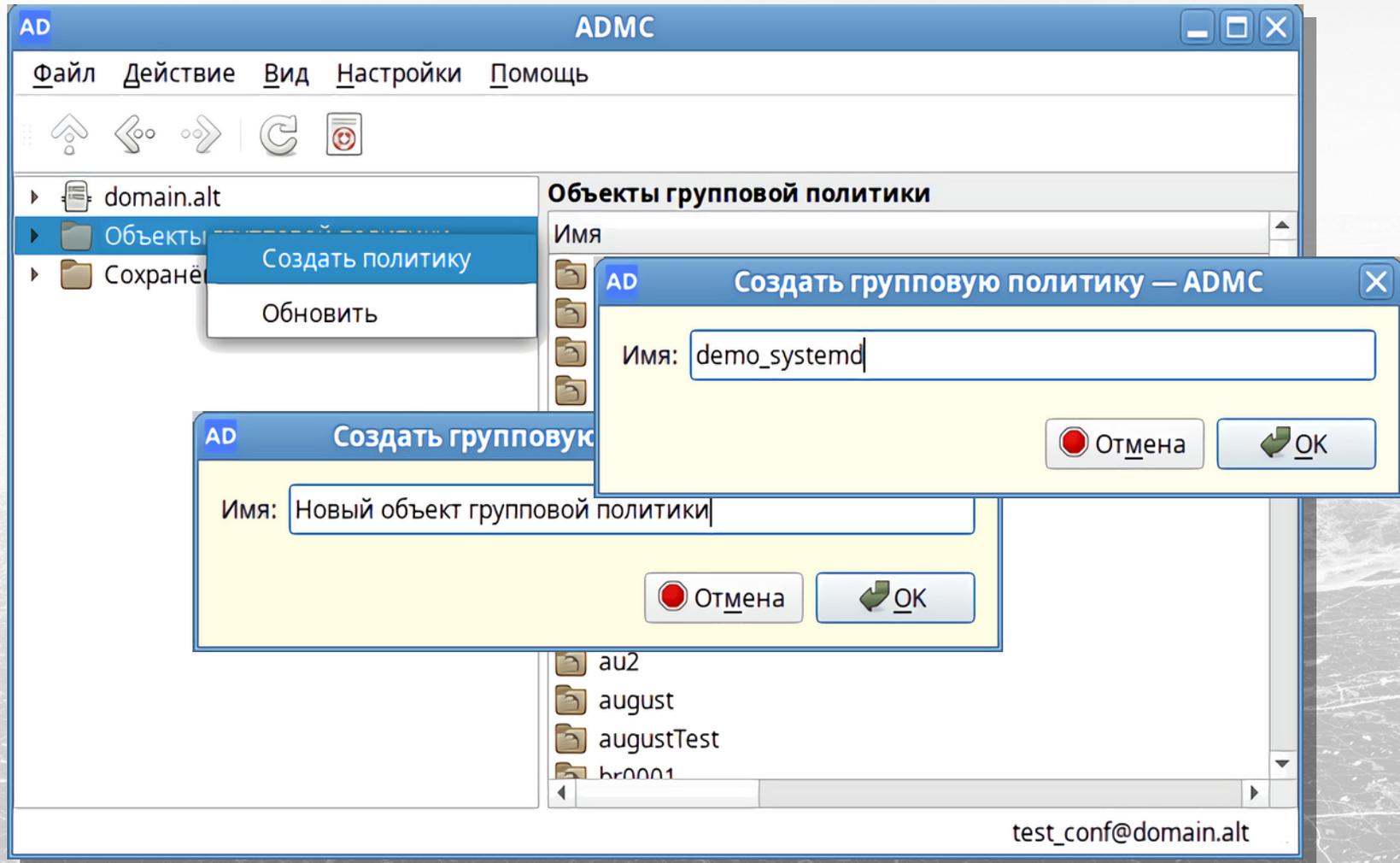
Имя	Значение	Тип
USNIntersite	<без значени...	Целое число
aCSPolicyN...	<без значени...	Юникод
accountExp...	(никогда)	Большое целое число
accountNa...	<без значени...	Юникод
adminCount	<без значени...	Целое число
adminDesc...	<без значени...	Юникод
adminDispl...	<без значени...	Юникод
allowedAttr...	<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

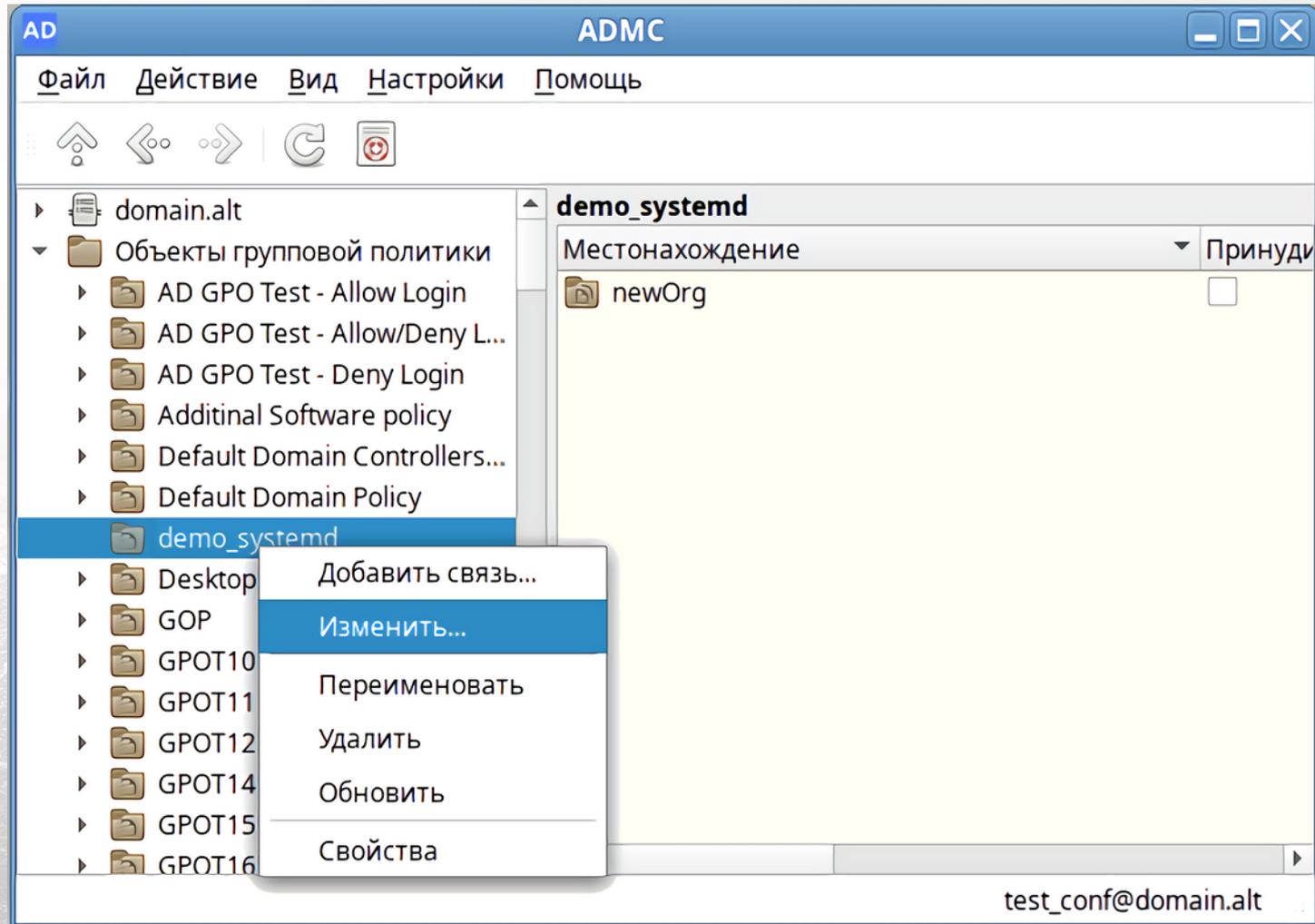
The image shows the ADMC (Active Directory Management Console) interface. The main window displays a tree view of Group Policy Objects (GPOs) under the domain 'domain.alt'. The 'demo\_systemd' GPO is selected, and a context menu is open over it, with 'Добавить связь...' (Add link) highlighted. A dialog box titled 'Добавление связи — ADMC' is open in the foreground. It contains the following fields and controls:

- Классы:** Подразделение (Department) with a 'Выбрать...' (Select...) button.
- Искать в:** domain (Search in) with an 'Обзор...' (Browse...) button.
- Имя:** newOrg (Name).
- Выбранные объекты:** A table listing the selected objects.

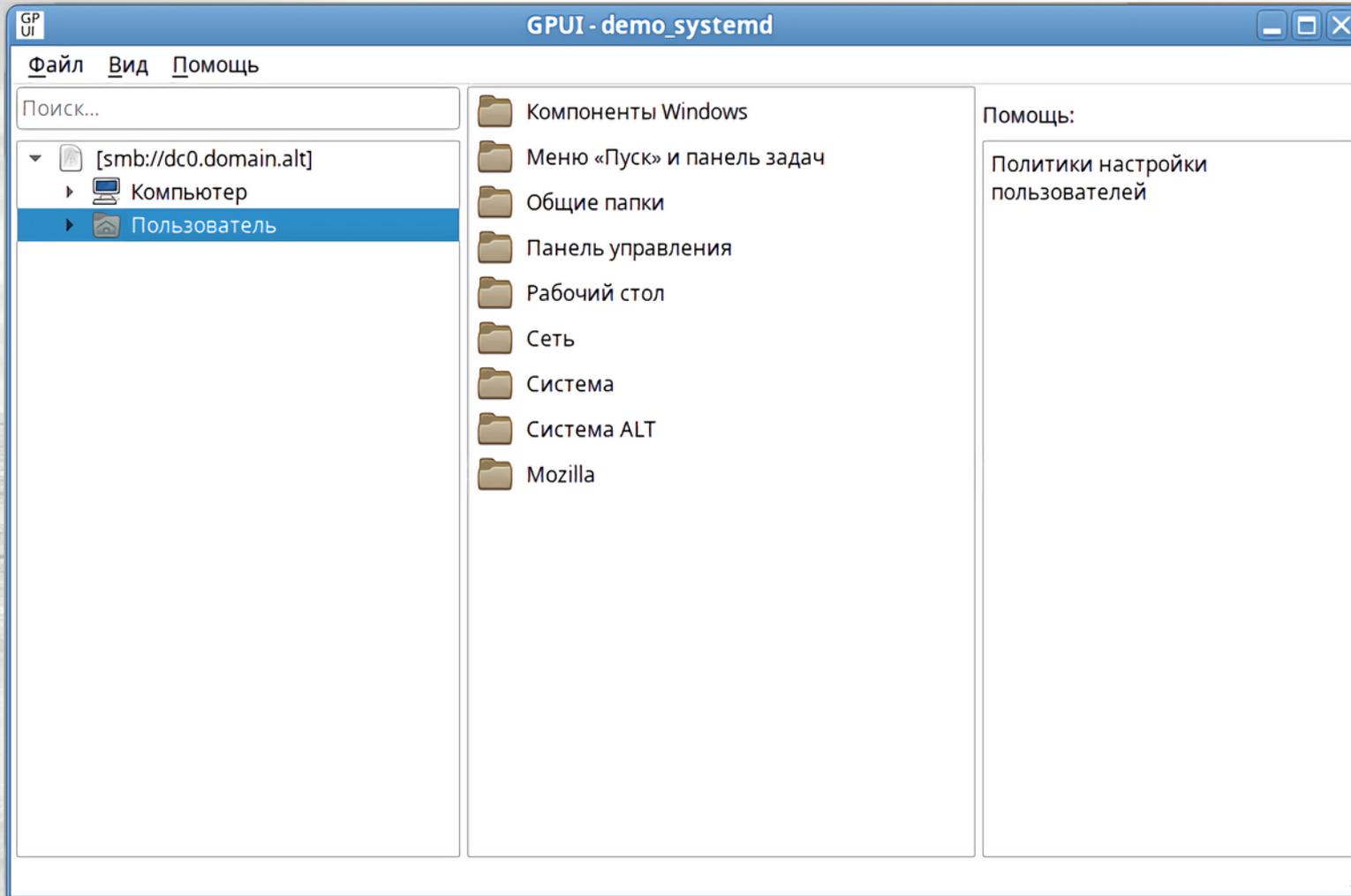
Имя	Тип	Папка
newOrg	Подразделение	domain.alt/

Buttons on the right side of the dialog include 'Добавить' (Add), 'Удалить' (Remove), and 'Продвинутый' (Advanced). At the bottom, there are 'Отмена' (Cancel) and 'ОК' (OK) buttons.

# ADMC. Создание политики. Изменение

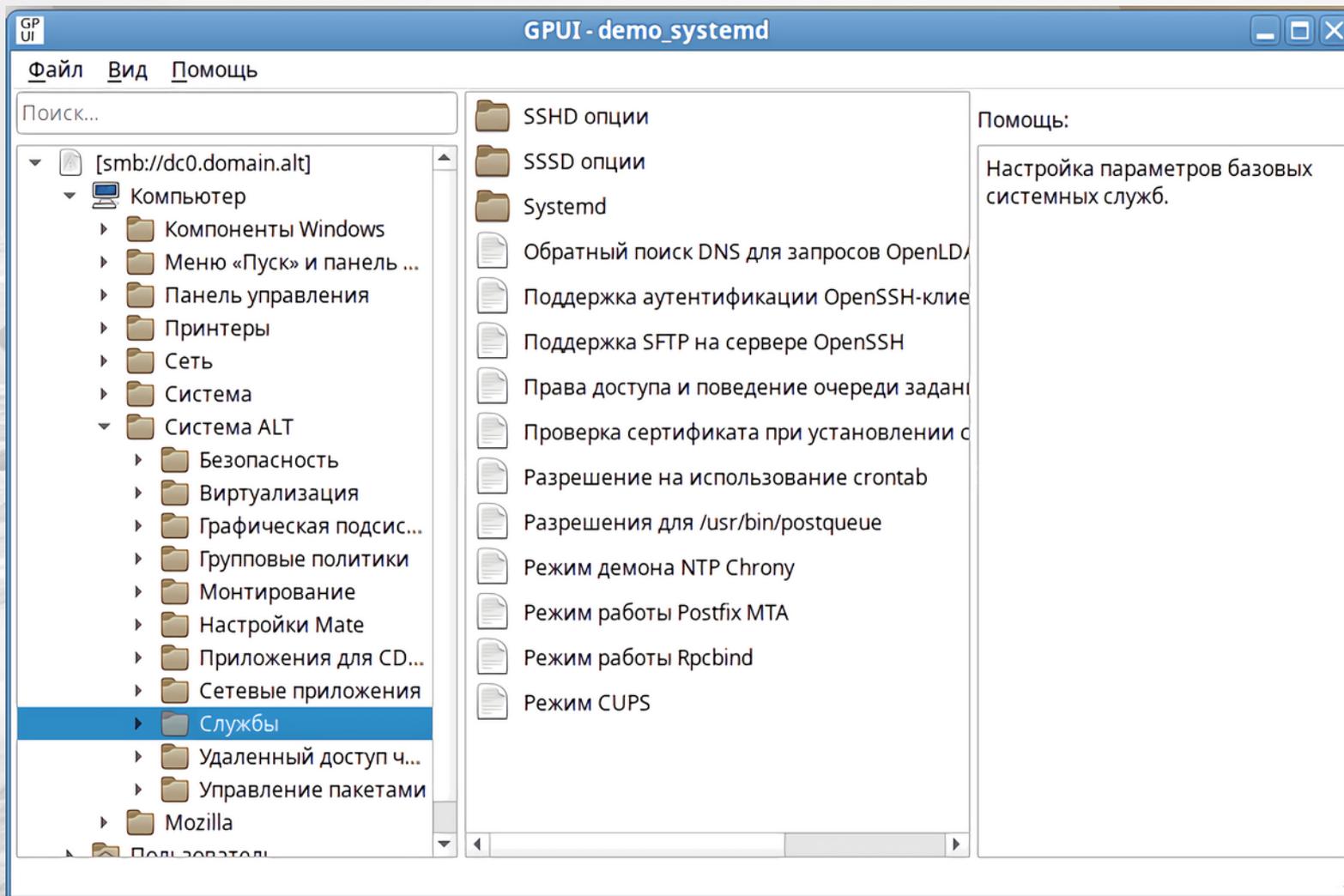


# GPUI – редактор политик



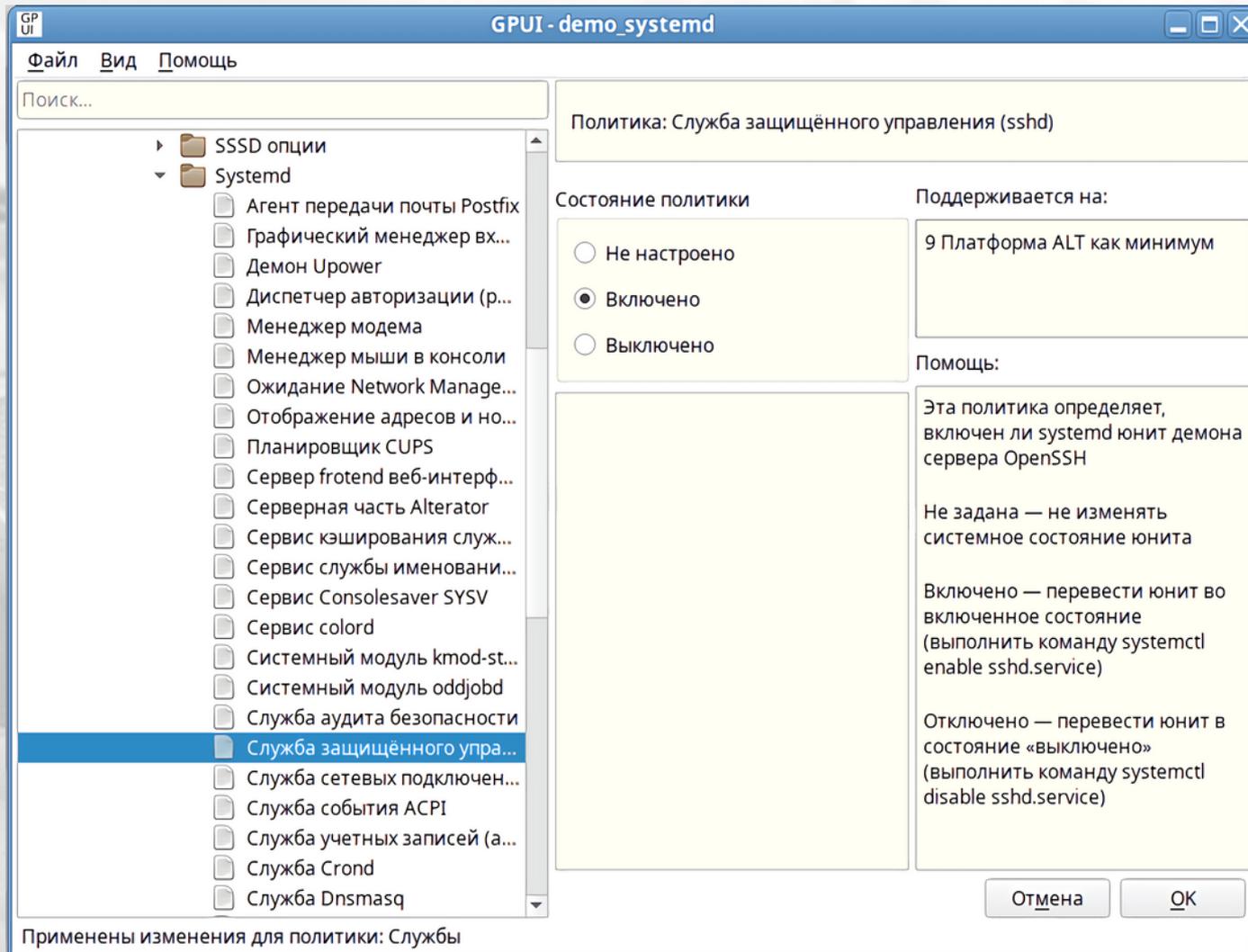
[Подробнее о GPUI](#)

# GPUИ – редактор политик. Службы



[Подробнее о GPUИ](#)

# GPUi – редактор политик. Службы. Состояние



The screenshot shows the GPUi GUI window titled "GPUi - demo\_systemd". The interface is in Russian and displays the configuration for the "Служба защищённого управления (sshd)" policy. The left sidebar shows a tree view with "Systemd" expanded, listing various services. The main area is divided into several sections:

- Поиск...**: Search bar.
- Состояние политики**: Policy status section with radio buttons for "Не настроено", "Включено" (selected), and "Выключено".
- Поддерживается на:**: Section indicating the minimum platform: "9 Платформа ALT как минимум".
- Помощь:**: Help section explaining the policy's function and providing instructions for enabling and disabling the service.

Buttons for "Отмена" (Cancel) and "ОК" (OK) are located at the bottom right. A status bar at the bottom left reads "Применены изменения для политики: Службы".



[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: DOMAIN.ALT

Кэшировать аутентификацию при недоступности сервера домена

Домен Active Directory  
Домен: DOMAIN.ALT  
Рабочая группа: DOMAIN  
Имя компьютера: TEST

Домен FreeIPA  
Домен: domain.alt  
Имя компьютера: p10grehpc

Настройки SSSD...

Внимание!  
**Изменение домена заработает только после перезагрузки компьютера**

Применить

Введите пароль для учётной записи с правами подключения к домену.

Имя пользователя: Administrator

Пароль:

Включить групповые политики

OK

Отмена

# Варианты миграции доменной инфраструктуры

Прямой	Включение SAMBA как КД, к уже существующим КД MS AD <i>(не для продолжительной совместной работы, только на время миграции и тестирования )</i>
Миграторы	Использование внешних средств <ul style="list-style-type: none"><li>• ADMT</li><li>• Pragmatic Tools Migrator,</li><li>• Самописные скрипты</li></ul>
Трасты	Построение параллельного домена с доверием
Импорт БД	«Замещающая миграция» - попытка втянуть всю базу AD в самбу (уз, sid, группы, ou, dns, gpo, sites, ....)

# Замещающая миграция

## MS AD → Альт Домен

Данный сценарий подразумевает единовременное замещение имеющихся MS AD контроллеров домена на контроллеры домена Samba. При этом основная часть учётных данных из базы MS AD сохраняется.

- Вначале база данных MS AD переносится в закрытое окружение, где, на её основе, разворачивается КД (контроллер домена) Samba.
- Следующим этапом разворачиваются другие контроллеры (реплики первого), соответствующие своим MS AD оригиналам.
- 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



# Планы развития

- Разработка инструментов диагностики домена (ADT) и тестов к нему
- Инструменты контроля за выполнением GPO (gpresult)
- Интеграция с FreeIPA (libdomain)
- Расширение набора групповых политик
- **Управление доменными парольными политиками (v0.17.0)**
- **Управление делегированием прав (v0.17.1)**
- LAPS v2 (конец 2024 года)
- Управление сайтами (в разработке)
- Просмотр состава политики (в разработке)
- Графический редактор DNS (в разработке)
- Управление трастами (в разработке)

# Полезные ссылки

## Документация Альт Домен

(руководство администратора)

[https://www.basealt.ru/fileadmin/user\\_upload/manual/ALT\\_Domain\\_guide.pdf](https://www.basealt.ru/fileadmin/user_upload/manual/ALT_Domain_guide.pdf)



## Доменная инфраструктура на базе Samba

(руководство администратора)

<https://docs.altlinux.org/ru-RU/domain/10.4/html/samba/index.html>



## Групповые политики

(Руководство пользователя)

<https://docs.altlinux.org/ru-RU/domain/10.2/html/group-policy/index.html>



# Лицензионные вопросы

- функционал Альт Домен входит в Альт Сервер и в Альт СП Сервер (скоро 10.2, ПК «Альт Домен» отражен в Формуляре)
- В реестре уже находится продукт(с 16.07.2024 ) № 1541, «Альт Домен» (альтернативное название «Альт Сервер»-а).
- Необходимо купить лицензию на контроллер домена на Альт Домен по числу контроллеров
- Купить техподдержку на КД и клиентов (SLA)

[https://www.basealt.ru/fileadmin/user\\_upload/pdf/TP\\_ALT\\_Domain.pdf](https://www.basealt.ru/fileadmin/user_upload/pdf/TP_ALT_Domain.pdf)



# Прайс. Лицензии Альт Домен

Тип ОС	На что лицензия?	Цена (т.р.) бесср./год
Альт Сервер 10	ПК АД на 1 КД	185/74
Альт Сервер 10 → АД	Апгрейд на ПК АД 1 КД	171,8/-
Альт Сервер 9 → АД	Апгрейд на вер. 10 + 1 КД	178,4/-
Альт СП Сервер 10	1 КД	220/88
Альт СП Сервер 10	Апгрейд на 1 КД	174,4/-
Альт СП Сервер 9 → СП АД	Апгрейд на вер. 10 + 1 КД	197,2/-
Клиент АД	На подключение 1 уст. к КД	0/0



# Прайс. Техподдержка Альт Домен

Тип ОС	Уровень ТП	Цена (т.р./год)
Альт Сервер 10 (Альт Домен)	Стандартная	70
Альт Сервер 10 (Альт Домен)	Расширенная	200
Альт СП Сервер 10 (Альт Домен)	Стандартная	70
Альт СП Сервер 10 (Альт Домен)	Расширенная	200
Клиент КД на Альт Сервер	Стандартная	1,2
Клиент КД на Альт Сервер	Расширенная	3
Клиент КД на Альт СП Сервер	Стандартная	1,2
Клиент КД на Альт СП Сервер	Расширенная	3



# Техподдержка Альт Сервер

Пользователи для частного продукта

Консультации по использованию Продукта в гетерогенных [корпоративных сетях](#), в том числе, по настройке [групповых политик](#) и [миграции решений с Active Directory](#)<sup>17</sup>

Нет

Да

Да

Консультации по использованию Продукта для

17 Включает консультации по возможностям Продукта, но не включает проектирование и внедрение. Если иное не указано в договоре поставки, по настоящим Правилам услуга предоставляется по Сертификатам, приобретенным до 02.09.2024. Начиная с 02.09.2024, услуга предоставляется в рамках техподдержки «Альт Домен» ([SLA](#)). Уточняйте у менеджера «Базальт СПО», какие Сертификаты необходимо приобрести для получения указанного вида техподдержки.



# Прайс. Техподдержка Альт Сервер

Тип ОС	Уровень ТП	Цена (т.р./год)
Альт Сервер 10 (без ТП АД)	Стандартная	17,78 (было 24)
Альт Сервер 10 (без ТП АД)	Расширенная	40 (было 50)
Альт СП Сервер 10 (без ТП АД)	Стандартная	27,36 (было 40)
Альт СП Сервер 10 (без ТП АД)	Расширенная	50 (было 60)



# Альт Домен SLA 1/4

Услуги, относящиеся к ПК «Альт Домен» в целом			
Переход на очередную минорную версию Продукта	Да	Да	Да
Доступ к "Справочному центру" <sup>3</sup>	Да	Да	Да
Доступ к BugTracker (система отслеживания ошибок) <sup>4</sup>	Да	Да	Да
Доступ к информационному порталу о закрытии уязвимостей <sup>5</sup>	Да	Да	Да
Доступ к обновлениям Продукта <sup>6</sup> (в том числе к обновлениям по безопасности)	Да	Да	Да
Прием сообщений об ошибках <sup>7</sup>	Да	Да	Да
Исправление ошибок в Продукте <sup>8</sup>	Нет <sup>9</sup>	Да	Да
Воспроизведение проблемы на стенде Службы сопровождения при наличии технической возможности <sup>10</sup>	Нет	Да	Да
	<b>БАЗОВЫЙ</b>	<b>СТАНДАРТНЫЙ</b>	<b>РАСПИРЕННЫЙ</b>
Удаленное подключение к рабочей системе Пользователя для анализа проблемы <sup>11</sup>	Нет	Нет	Да
Выделенный технический менеджер с 9:00 до 18:00 (МСК)	Нет	Нет	Да

# Альт Домен SLA 2/4

## Услуги, относящиеся к серверной части ПК «Альт Домен»

Консультации по установке Продукта <sup>12</sup>	Да	Да	Да
Консультации по развертыванию нового домена	Да	Да	Да
Консультации по включению контроллера домена в существующий домен	Нет	Да	Да
Консультации по использованию серверной части Продукта в гетерогенных корпоративных сетях <sup>13</sup>	Нет	Да	Да
Консультации по управлению пользователями и группами	Да	Да	Да
Консультации по настройке групповых политик <sup>14</sup>	Нет	Да	Да
Консультации по планированию миграции инфраструктуры на «Альт Домен» <sup>15</sup>	Нет	Нет	Да
Консультации по миграции серверных решений <sup>16</sup>	Нет	Нет	Да
Консультации по репликации службы каталогов <sup>17</sup>	Нет	Да	Да
Консультации по репликации Sysvol <sup>18</sup>	Нет	Да	Да
Консультации по настройке доверительных отношений (трасов) <sup>19</sup>	Нет	Нет	Да

# Альт Домен SLA 3/4

## серверная часть (продолжение)

Параметры	Уровень сопровождения (поддержки)		
	БАЗОВЫЙ	СТАНДАРТНЫЙ	РАСШИРЕННЫЙ
Консультации по настройке резервного копирования домена <sup>20</sup>	Нет	Да	Да
Консультации по восстановлению домена в режиме мультимастерной репликации <sup>21</sup>	Нет	Нет	Да
Консультации по настройке инфраструктурных сервисов, задействованных в функционировании «Альт Домен» <sup>22</sup>	Нет	Да	Да
Консультации по автоматизации процессов в доменной инфраструктуре <sup>23</sup>	Нет	Нет	Да

# Альт Домен SLA 4/4

Услуги, относящиеся к клиентской части ПК «Альт Домен»			
Консультации по миграции клиентских решений на ОС «Альт».	Нет	Да	Да
Консультации по выбору механизма и по настройке аутентификации и авторизации клиентов <sup>24</sup>	Да	Да	Да
Консультации по выбору механизма и по настройке аутентификации и авторизации сервисов <sup>25</sup>	Нет	Нет	Да
Консультации по настройке на клиентских системах доменных сервисов	Да	Да	Да
Консультации по созданию собственных ADMX-шаблонов групповых политик на базе существующих механизмов применения групповых политик	Нет	Нет	Да

# SLA Red ADM

		СТАНДАРТНЫЙ	РАСШИРЕННЫЙ
			(24/7 для «Срочного» приоритета Запроса)
5.6	База знаний	+	+
5.7	Доступ к обновлениям безопасности <sup>1</sup>	+	+
5.8	Доступ к обновлению ПО <sup>2</sup>	+	+
5.9	Возможность перехода (обновления) на новую версию ПО <sup>3</sup>	+	+
5.10	Личный кабинет (Портал) <sup>4</sup>	+	+
5.11	Консультации по установке, настройке, обновлению ПО, в рамках Документации на ПО.	+	+
5.12	Моделирование проблемных ситуаций на тестовом стенде СТП, при наличии технической возможности и пошаговой инструкции по воспроизведению	-	+
5.13	Удаленное подключение к системе Пользователя для сбора информации, необходимой для решения Запроса <sup>5</sup>	-	+
5.14	Консультации по функционированию ПО в гетерогенной среде <sup>6</sup>	-	+

# ALD Pro

SLA — очень лаконичный:

№	Услуга	Стандартный	Привилегированный
4.1	Доступ к обновлениям безопасности Продукта (минорные обновления)	+	+
4.2	Доступ к очередным обновлениям Продукта (мажорные обновления)	+	+
4.3	Регистрация ошибок, Предложений и отслеживание их статуса через Исполнителя <sup>1</sup>	+	+
4.4	Консультации по установке Продукта	+	+
4.5	Консультации по настройке Продукта	+	+
4.6	Моделирование сценариев на тестовом стенде Исполнителя при наличии технической возможности	+	+
4.7	Удаленное подключение к системе Пользователя для сбора информации, необходимой для решения Запроса*	-	+
4.8	Консультации по функционированию Продукта в гетерогенных сетях <sup>2</sup>	-	+
4.9	Выделенный менеджер (Рабочие дни с 09:00 до 18:00 по МСК)	-	+

# Альт Домен внедрения

Новосибирская область (ПАК Патриот, более 10. тыс мест Samba + FreeIPA )

Росимущество (около 3000 раб. мест в 60 регионах, возможны рефренс-визиты)

Администрация г. Ставрополь (возможны рефренс-визиты)

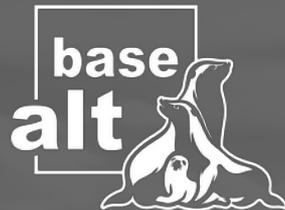
ООО «Бизнес ИТ» (партнер Базальт СП, внедрили себе).

<https://cloud.ru/news/basalt-spo-domain-controller> :

Контроллер домена от «Базальт СПО» управляет операционными системами разных производителей: подтверждено испытаниями Cloud.ru

Программный комплекс «Альт Домен», разработанный «Базальт СПО», успешно управляет в единой облачной инфраструктуре операционными системами ведущих российских производителей. Это подтверждено испытаниями, которые провела комиссия технических специалистов провайдера [Cloud.ru](https://cloud.ru).





#### **Контакты**

Тел.: +7 (495) 123-47-99

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

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

#### **оптовые продажи:**

[sales@basealt.ru](mailto:sales@basealt.ru)

#### **Офисы:**

Москва,

ул. Бутырская, д. 75

Санкт-Петербург, Коломяжский

пр-т, 27,

БЦ «Содружество», 3 этаж

Саратов,

ул. Октябрьская 44,

корпус А, офис № 3

Обнинск,

ул. Королёва, д. 4Б, БЦ

“Британика”