



ALDPro

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

РДЦП.10101-01 93 01
Версия: 2.4.1

Содержание

1 Введение	7
2 О системе	8
2.1 Общие сведения	8
2.2 Функциональное назначение	8
2.3 Используемые технические средства и дополнительное программное обеспечение	9
2.4 Входные и выходные данные	10
2.5 Вызов и загрузка	11
3 Аутентификация пользователей	12
3.1 Вход в Систему по логину или паролю	12
3.1.1 Смена пароля с истекшим сроком действия	13
3.1.2 Первый вход	13
3.2 Вход в Систему с Kerberos	14
3.3 Выход из Системы или Смена пользователя	14
4 Управление доменом	15
4.1 Общая информация	15
4.1.1 Описание	15
4.1.2 Работоспособность домена	15
4.1.3 Состав системы	16
4.1.4 Граф топологии	17
4.1.5 Параметры домена	17
4.2 Сайты и службы	17
4.2.1 Сайты и службы	18
4.2.2 Контроллеры домена	21
4.2.3 Соглашения о репликации	23
4.3 Дополнительные параметры групповых политик	25
4.3.1 Параметры компьютеров	25
4.3.2 Параметры пользователей	31
4.4 Каталог заданий автоматизации	37

4.4.1	Управление папками	38
4.4.2	Управление заданиями	39
4.4.3	Удаление задания	42
4.5	Службы и параметры Kerberos	42
4.5.1	Политика билетов Kerberos	42
4.5.2	Службы Kerberos	43
4.6	Пользователи и группы	45
4.6.1	Параметры пользователей	45
4.6.2	Параметры групп	47
4.6.3	POSIX идентификаторы	48
4.6.4	Атрибуты пользователей	49
4.7	Интеграции с доменами	50
4.7.1	Миграции MS AD	50
4.7.2	Доверительные отношения	52
4.8	Роли и права доступа	55
4.8.1	Возможности учетной записи пользователя	55
4.8.2	Права на операции в портале управления	55
4.8.3	Возможности для ограничения областей действия ролей и привилегий	57
4.9	Доверие между доменами ALD Pro	76
4.9.1	Особенности работы раздела «Доверие между доменами ALD Pro»	77
4.9.2	Настройка доверия между доменами ALD Pro	79

5 Пользователи и компьютеры 85

5.1	Организационная структура	85
5.1.1	Общие сведения	85
5.1.2	Добавление нового подразделения	86
5.1.3	Редактирование подразделения	86
5.1.4	Удаление подразделения	95
5.2	Пользователи	96
5.2.1	Список пользователей	96
5.2.2	Добавление пользователя	96
5.2.3	Редактирование информации о пользователе	97
5.2.4	Блокировка и разблокировка пользователя	104
5.2.5	Удаление пользователя	105
5.3	Группы пользователей	106
5.3.1	Список групп пользователей	106
5.3.2	Добавление новой группы	106
5.3.3	Редактирование информации о группе пользователей	108
5.3.4	Удаление группы пользователей	114

5.4	Компьютеры	115
5.4.1	Список компьютеров	115
5.4.2	Добавление компьютера	115
5.4.3	Редактирование информации о компьютере	115
5.4.4	Добавление компьютера в домен	119
5.4.5	Удаление компьютера	119
5.5	Группы компьютеров	120
5.5.1	Список групп компьютеров	120
5.5.2	Добавление новой группы компьютеров	120
5.5.3	Редактирование информации о группе компьютеров	121
5.5.4	Удаление группы компьютеров	125
5.6	Корзина	125
5.6.1	Список пользователей, перемещенных в корзину	125
5.6.2	Восстановление пользователя из корзины	126
5.6.3	Окончательное удаление пользователя	126
6	Автоматизация	127
6.1	Задания автоматизации	127
6.1.1	Журнал заданий	127
6.1.2	Каталог заданий автоматизации	129
6.2	Установка ОС по сети	130
6.2.1	Список серверов установки ОС	130
6.2.2	Создание сервера установки ОС	130
6.2.3	Редактирование сервера установки ОС	131
6.2.4	Удаление сервера установки ОС	146
7	Мониторинг	147
7.1	Журнал событий мониторинга	147
7.1.1	Журнал событий	147
7.1.2	Серверы мониторинга	148
7.2	Витрины мониторинга домена	150
7.2.1	Просмотр витрины	151
7.3	Расширение функционала мониторинга	152
8	Модуль синхронизации	153
8.1	Настройки	154
8.1.1	Контроллеры домена AD	154
8.1.2	Контроллеры домена ALD	155
8.1.3	Синхронизация паролей	157
8.2	Источники	157

8.2.1	Сопоставление подразделений	157
8.2.2	Структура дерева синхронизации	158
8.3	Сопоставление атрибутов	159
8.3.1	Карта сопоставлений	160
8.3.2	Атрибуты AD	160
8.3.3	Атрибуты ALD	161
8.4	Особенности работы модуля синхронизации	162
9	Журнал событий	165
9.1	Серверы журнала событий	165
9.1.1	Список серверов журнала событий	165
9.1.2	Развертывание сервера журнала событий	165
9.1.3	Управление сервером журнала событий	166
9.1.4	Удаление сервера журнала событий	166
9.2	Настройка сбора журналов событий	167
9.2.1	Список правил	167
9.2.2	Добавление нового правила сбора информации о событиях	167
9.2.3	Просмотр информации о правиле	168
9.2.4	Редактирование правила сбора информации о событии	169
9.2.5	Удаление правила	169
10	Групповые политики	171
10.1	Групповые политики	171
10.1.1	Список групповых политик	171
10.1.2	Создание групповой политики	171
10.1.3	Настройка групповой политики	172
10.1.4	Удаление групповой политики	179
10.2	Политики доступа к узлу	179
10.2.1	Правила НВАС	180
10.2.2	Службы НВАС	184
10.2.3	Группы служб НВАС	187
10.3	Политики повышения привилегий	189
10.3.1	Правила Sudo	189
10.3.2	Команды Sudo	196
10.3.3	Группы команд Sudo	198
10.4	Политики паролей	200
10.4.1	Список политик паролей	200
10.4.2	Создание политики паролей	201
10.4.3	Редактирование политики паролей	201

10.4.4 Удаление политики паролей	202
11 Установка и обновление ПО	204
11.1 Политики ПО	204
11.1.1 Список политик ПО	204
11.1.2 Создание политики ПО	204
11.1.3 Настройка политики ПО	205
11.1.4 Применение политики ПО	210
11.1.5 Дополнительные настройки установки ПО	211
11.1.6 Удаление политики ПО	211
11.2 Каталог ПО	211
11.2.1 Каталог программного обеспечения	211
11.2.2 Создание раздела ПО	212
11.2.3 Редактирование раздела ПО	212
11.2.4 Добавление ПО в каталог программного обеспечения	213
11.2.5 Редактирование ПО	214
11.2.6 Удаление программного обеспечения или раздела	221
11.3 Репозитории ПО	221
11.3.1 Репозитории ПО	221
11.3.2 Серверы репозитория ПО	227
11.4 Политики обновления ALD Pro	228
11.4.1 Список политик обновления ALD Pro	228
11.4.2 Создание политики обновления ALD Pro	229
11.4.3 Настройка политики обновления ALD Pro	230
11.4.4 Просмотр назначенных политик на компьютерах и группах компьютеров	232
11.4.5 Удаление политики обновления ALD Pro	232
12 Роли и службы сайта	233
12.1 Служба разрешения имен	233
12.1.1 Зоны DNS	233
12.1.2 Перенаправление запросов	242
12.1.3 Глобальная конфигурация DNS	244
12.2 Служба динамической настройки узла	245
12.2.1 Список серверов	245
12.2.2 Добавление DHCP-сервера	245
12.2.3 Настройка конфигурации DHCP-сервера	246
12.2.4 Удаление DHCP-сервера	252
12.3 Служба синхронизации времени	252
12.3.1 Внешний пул NTP-серверов	252

12.3.2	Корневые NTP-серверы домена	253
12.4	Служба глобального каталога	254
12.4.1	Список серверов	254
12.4.2	Добавление сервера глобального каталога	255
12.4.3	Удаление сервера глобального каталога	255
12.5	Служба печати	255
12.5.1	Серверы печати	256
12.5.2	Добавление сервера печати	256
12.5.3	Настройка сервера печати	256
12.5.4	Удаление сервера печати	259
12.6	Общий доступ к файлам	260
12.6.1	Серверы общих папок	260
12.6.2	Добавление сервера общих папок	260
12.6.3	Настройка сервера общих папок	261
12.6.4	Удаление сервера общих папок	266

13 Личный кабинет 267

13.1	Основное	267
13.1.1	Персональные данные	267
13.1.2	Учетная запись	268
13.1.3	Организационные данные	268
13.1.4	Контактная информация	269
13.1.5	Расположение	269
13.1.6	Сертификаты пользователей	269
13.1.7	Открытые ключи SSH	269
13.2	Группы	270
13.2.1	Состоит в группах	270
13.2.2	Состоит в группах не прямое наследование	270
13.3	Дополнительные сведения	271
13.4	Групповые политики	271
13.5	Расширенные настройки	271
13.6	Назначенные роли	271

Введение

Настоящее руководство пользователя распространяется на программное изделие РДЦП.10101-01 «Программный комплекс «ALD Pro» (далее по тексту — ПК «ALD Pro»), предназначенное для централизованного администрирования ресурсов домена в компьютерных сетях под управлением «Операционной системы специального назначения «Astra Linux Special Edition» (далее по тексту — ОС Astra Linux) посредством графического интерфейса.

Средой функционирования ПК «ALD Pro» является ОС Astra Linux. ПК «ALD Pro» интегрировано с комплексом средств защиты информации ОС Astra Linux, является прикладным программным обеспечением и не реализует самостоятельно функции защиты информации.

Областью применения ПК «ALD Pro» является автоматизация деятельности системных администраторов в рамках эксплуатации ИТ-инфраструктуры на базе ОС Astra Linux.

В данном документе приведено описание функциональных характеристик ПК «ALD Pro» и информация, необходимая для его эксплуатации.

Документ предназначен для системных администраторов доменной инфраструктуры.

Наиболее полную и актуальную информацию о работе системы, а также примеры скриптов и вводимых настроек можно найти в справочном центре, встроенном в ПК «ALD Pro» (далее по тексту — СЦ).

В составе ПК «ALD Pro» имеется встроенный справочный центр (далее — СЦ), представляющий из себя электронный портал для получения наиболее полной и актуальной справочной информации по работе, настройке и управлению ПК «ALD Pro».

Для вызова СЦ необходимо нажать кнопку [?], находящуюся в правом верхнем углу окна ПК «ALD Pro». Вход в СЦ осуществляется при нахождении в любом из разделов ПК «ALD Pro». Дальнейшая навигация в СЦ осуществляется в соответствии с одноименным названием разделов ПК «ALD Pro».

О системе

В данном разделе приведено описание функциональных характеристик программного обеспечения ПК «ALD Pro» и информация, необходимая для его эксплуатации.

2.1. Общие сведения

Наименование программы — «Программный комплекс «ALD Pro».

Сокращенное наименование программы — ПК «ALD Pro».

Тексты программы ПК «ALD Pro» написан на следующих языках:

- Python;
- JavaScript.

2.2. Функциональное назначение

ПК «ALD Pro» предназначен для централизованного администрирования ресурсами домена под управлением ОС Astra Linux и использования в организациях различного масштаба.

Функциональные возможности программы:

- управление конфигурацией домена;
- удаленное подключение к рабочему столу пользователя;
- установка и обновление программного обеспечения;
- установка операционной системы по сети;
- управление службой разрешения имен;
- управление службой динамической настройки узла;
- управление службой синхронизации времени;
- управление службой печати;

- управление заданиями автоматизации;
- навигация и поиск объектов;
- справочный центр;
- интеграция с почтовым сервисом;
- аутентификация пользователей изделия;
- управление параметрами групповых политик;
- управление службами и политиками билетов Kerberos;
- управление параметрами пользователей и групп;
- управление доверительными отношениями с доменами;
- управление организационной структурой, пользователями и компьютерами;
- управление групповыми политиками;
- управление общим доступом к файлам;
- управление доступом к функциям изделия;
- управление мониторингом;
- управление журналированием событий;
- доступ к личному кабинету.

2.3. Используемые технические средства и дополнительное программное обеспечение

Компоненты ПК «ALD Pro» функционируют на технических средствах, состав и характеристики которых представлены в данном подразделе.

Клиентская часть — это набор ПО, который устанавливается на компьютеры домена и состоит из подсистемы «Агент домена». В качестве браузера рекомендуется использовать Chromium или Mozilla FireFox. При использовании любого другого браузера возможно предупреждение «Вероятная угроза безопасности». Чтобы продолжить работу в выбранном браузере, необходимо нажать на кнопку «Принять риски и продолжить».

Требования к оборудованию для функционирования клиентской части:

•компьютер:

- операционная система семейства Astra Linux;

- процессор (CPU) — не менее двух ядер;
- оперативная память (RAM) — не менее 1 Гб;
- свободное место на диске — не менее 4 Гб;
- видеокарта;
- монитор;
- клавиатура;
- мышь.

Для установки пакетов клиентской части приложения на компьютере должен быть доступ к официальным репозиториям компании-производителя (<https://dl.astralinux.ru>) либо к репозиториям, развернутым во внутренней сети.

Серверная часть работает на специальном промышленном компьютере (сервере), который не предназначен для бытового использования.

2.4. Входные и выходные данные

Входными данными для обеспечения функционирования ПК «ALD Pro» являются:

- обращение пользователей (процессов и команд) к подсистемам ПК «ALD Pro» и их специальным модулям, а также средствам IPC.
- атрибуты, определяющие полномочия пользователя и правила разграничения доступа к функциям ПК «ALD Pro»

Выходными данными является результат обработки обращений пользователя (процессов и команд) к функциям ПК «ALD Pro»:

- авторизация пользователя;
- развертывания сетевых служб;
- запуск служб;
- запись, редактирование, удаление объектов;
- запуск, редактирование и исполнение команд управления;
- регистрация результатов выполнения команд управления.

2.5. Вызов и загрузка

Для клиентской части ПК «ALD Pro» вызов осуществляется путем запуска браузера на компьютере, подключенном к домену, и ввода в адресной строке браузера URL системы.

Вызов и загрузка серверной части ПК «ALD Pro» производится путем запуска приложения в соответствии с эксплуатационной документацией.

Примечание: Для корректной работы с порталом управления администратор домена должен использовать доменное имя контроллера домена (не IP-адрес).

Аутентификация пользователей

Раздел содержит следующие подразделы:

3.1. Вход в Систему по логину или паролю

Окно **Вход в Систему** открывается автоматически при входе на **ALD Pro**.

Для входа ввести логин и пароль в соответствующие поля. Для безопасности пароль скрыт. Чтобы просмотреть пароль, нужно нажать на значок глаза в поле **Пароль**.

Нажать кнопку **Войти**. Откроется страница **ALD Pro**, соответствующая зонам ответственности пользователя.

Примечание: Время непрерывной сессии составляет 23 часа. При этом будет создан действующий TGT-билет, и на время его действия авторизация компьютера будет проходить через билет.

При некорректно введенном логине/пароле появляется сообщение об ошибке. В Системе число попыток входа ограничено и регулируется администратором.

Вход на портал управления пользователя с пустым паролем невозможен, независимо от того, каким образом такой пользователь был создан.

Если есть проблемы с входом, то возможна одна из следующих причин:

- превышено число попыток ввода логина/пароля;
- срок действия пароля истек или пароль не активирован.

Ежедневно один раз в день после обновления сессии или входа в систему появляется уведомление о сроке действия пароля “Дней до окончания действия пароля N”, при условии, что дней до истечения пароля осталось не больше, чем указано в настройках.

3.1.1. Смена пароля с истекшим сроком действия

Информационное сообщение об истечении срока действия пароля появляется у пользователя согласно настройке Системы.

Если пользователь по каким-то причинам не обновил пароль своевременно, то Система поддерживает возможность смены пароля без авторизации.

При вводе пароля с истекшим сроком действия, на странице входа появляются дополнительные поля, позволяющие пользователю сменить пароль.

Для смены пароля необходимо ввести текущий пароль, новый пароль и подтверждение нового пароля в соответствующие поля и нажать кнопку сохранения изменений.

Пароль изменен. Теперь пользователь может войти в Систему, используя новый пароль.

Таким же образом пользователь может сменить пароль при первом входе в Систему или в случае, если ему был выдан временный пароль в замен аннулированного администратором.

3.1.2. Первый вход

При первом входе Система требует смены пароля, полученного от администратора. Сделать это можно одним из следующих способов:

1. Через окно входа на портал управления.
2. Через доменный компьютер.

3.1.2.1. Смена пароля через доменный компьютер

Для первого входа использовать доменный компьютер пользователя. В открывшуюся форму аутентификации на компьютере ввести полученные от администратора логин и пароль. Откроется форма смены пароля, где нужно указать старый пароль, новый пароль и подтверждение нового пароля. Нажать кнопку сохранения изменений.

Пароль изменен. Теперь вход на портал с доменного компьютера осуществляется без дополнительного ввода логина и нового пароля.

3.1.2.2. Смена пароля через окно входа на портал управления

Действия по смене пароля при первом входе аналогичны смене пароля с истекшим сроком действия и подробно описаны [здесь](#).

3.2. Вход в Систему с Kerberos

Вход в Систему с Kerberos - один из способов аутентификации, поддерживаемый **ALD Pro**.

Доступен только для компьютеров в домене. Настройка браузера и выдача билета автоматическая и не требует участия пользователя.

Для входа нужно нажать **Вход с Kerberos**. Логин и пароль не используются. Откроется страница **ALD Pro**, соответствующая зонам ответственности пользователя.

Примечание: Вход с Kerberos возможен только для тех пользователей, у которых есть действующий билет.

3.3. Выход из Системы или Смена пользователя

Для выхода из Системы или смены пользователя в правом верхнем углу навести курсор мыши на значок пользователя. В выпадающем меню выбрать **Выход**. Откроется окно **Вход в Систему**.

Для входа под другим пользователем воспользуйтесь формой аутентификации.

По умолчанию в Системе зарегистрирован пользователь с типом **главный администратор (ALDPRO - Main Administrator)**. Он изначально регистрирует пользователей и выдает логины и пароли для работы в Системе. Доступ к Системе имеют зарегистрированные администратором пользователи.

Система поддерживает два типа входа в систему:

- вход в Систему по логину/паролю;
- вход в Систему с Kerberos.

Управление доменом

В данном разделе осуществляется настройка и управление структурой и конфигурацией ALD Pro.

4.1. Общая информация

4.1.1. Описание

Подраздел отображает состояние домена, состав системы, граф топологии и основные параметры домена.

Подраздел состоит из вкладок:

- **Работоспособность домена;**
- **Состав системы;**
- **Граф топологии;**
- **Параметры домена.**

4.1.2. Работоспособность домена

На вкладке располагаются четыре виджета с информацией о работоспособности системы:

- **Общее состояние системы** — состояние системы на данный момент;
- **Состояние контроллеров домена** — общее количество контроллеров домена, которые заведены в систему, количество сайтов, которые есть в системе, и их состояние;
- **Количество типов объектов системы** — типы объектов и их количество;
- **Принадлежность сайтов к подсистемам** — количество объектов в каждой подсистеме и их состояние. Также можно узнать к каким именно подсистемам относится тот или иной сайт и его состояние в подсистеме на данный момент.

4.1.3. Состав системы

На вкладке приводится список подсистем с указанием наименования подсистемы (**Подсистема**), сервера (**Сервер**), сайта (**Сайт**), состояния (**Состояние**) и версии системы (**Версия ALD Pro**).

Каждая подсистема может принимать одно из следующих значений:

- **Ошибка:** установка или обновление подсистемы не выполнено;
- **Устанавливается:** выполняется установка подсистемы;
- **Установлена:** подсистема успешно установлена;
- **Удаляется:** выполняется удаление подсистемы;
- **Удалена:** подсистема успешно удалена;
- **Обновляется:** выполняется обновление подсистемы;
- **Обновлена:** подсистема успешно обновлена.

Внимание: Для установки подсистемы на контроллер домена, на котором уже была установлена подсистема (устанавливаемая или любая другая), необходимо предварительно вывести компьютер из домена и переустановить операционную систему на нем.

Для списка доступен поиск по серверу. Для этого в верхнем левом углу вкладки в поле поиска ввести значение.

Для списка доступна фильтрация по значениям полей **Подсистема**, **Сайт** и **Состояние**. Для фильтрации необходимо кликнуть по значку фильтрации и выбрать значение из выпадающего списка. Для поиска необходимого значения доступен функционал поиска. Для этого в поле **Найти значение** вверху списка начать вводить значение. В результате будет обновлен список фильтрации, отвечающий требованиям поиска.

Для списка доступна сортировка по значениям поля **Подсистема**.

В левом нижнем углу указано количество подсистем, а в правом нижнем углу кнопки переключения страниц.

4.1.4. Граф топологии

Граф топологии представляет собой модель связи сайта и контроллера домена.

В верхней правой части вкладки указаны сущности, которые отображены на графе.

При наведении курсора на объект будет показано название объекта и его сущность. При наведении курсора на линию, соединяющую объекты, будет показано какие объекты эта линия соединяет.

Для перемещения по модели необходимо переместить курсор на вкладку, зажать левую кнопку мыши и переместить курсор. Для увеличения/уменьшения масштаба использовать колесо мыши.

В левой верхней части вкладки располагается фильтр отображения объектов топологии. Для его использования необходимо нажать на кнопку **[Фильтр]** и ввести опцию или выбрать из выпадающего списка. Чтобы сбросить опцию фильтра, необходимо нажать на кнопку закрытия в опции. Чтобы сбросить все опции, необходимо нажать на кнопку закрытия рядом с выпадающим списком. Для скрытия опций нажать на кнопку **[Скрыть]**.

Отображение топологии можно отфильтровать также по типу сущности, для этого в верхней правой части вкладки нажать на название сущности для ее скрытия/отображения.

4.1.5. Параметры домена

Во вкладке отображается информация о домене: версия системы **ALD Pro**, исполнение **ALD Pro**, имя области **Kerberos (REALM)** и уровень домена **FreeIPA**.

Поле **Исполнение ALD Pro** принимает значения:

- РДЦП.10101-01 - при несертифицированном исполнении ALD Pro;
- РДЦП.10101-02 - при сертифицированном исполнении ALD Pro.

4.2. Сайты и службы

В подразделе приведены функции управления сайтами и репликацией домена.

4.2.1. Сайты и службы

На вкладке **Сайты и службы** осуществляется управление сайтами домена. Сайты в ALD Pro — это способ сегментирования системы.

4.2.1.1. Список сайтов и сервисов

На вкладке приводится список сайтов с указанием их имен (**Имя сайта**) и расположения (**Расположение IPA**).

Для списка доступен поиск по названию. Для этого в верхнем левом углу вкладки в поле поиска ввести значение.

Для просмотра информации о сайте нажать на соответствующий сайт в списке. Будет открыта карточка сайта с информацией о нем.

В левом нижнем углу указано количество сайтов, а в правом нижнем углу располагаются кнопки переключения страниц.

4.2.1.2. Создание нового сайта

Для создания нового сайта нажать кнопку **[Новый сайт]**. Будет выполнен переход на карточку создания сайта.

На вкладке **Основное** необходимо заполнить обязательные поля **Имя сайта** (например, *Сибирский офис*) и **Расположение IPA** (например, *siberia*). Опционально можно заполнить поле **Описание сайта**.

Важно: В поле **Расположение IPA** допустимы для использования цифры и строчные латинские буквы.

Для сохранения сайта необходимо в правом верхнем углу нажать на кнопку сохранения и подтвердить действие в диалоговом окне.

Для закрытия карточки без сохранения сайта нажать кнопку закрытия.

Вкладки **Контроллеры домена** и **Подсистемы сайта** станут доступны для заполнения после сохранения сайта (см. [Управление сайтом](#)).

4.2.1.3. Управление сайтом

Управление сайтом и редактирования информации о нем выполняется на его карточке. Для открытия карточки необходимо на вкладке **Сайты и службы** нажать на соответствующий сайт.

На карточке сайта информация о нем содержится на вкладках:

- **Основное;**
- **Контроллеры домена;**
- **Подсистемы сайта.**

Для закрытия карточки сайта и возврата к списку сайтов нажать на кнопку закрытия.

Основное

Отображает основную информацию о сайте.

Поля **Расположение IPA** и **Описание сайта** доступны для редактирования. Поле **Расположение IPA** является обязательным для заполнения.

Для сохранения изменений необходимо в правом верхнем углу нажать на кнопку сохранения.

Контроллеры домена

Список контроллеров домена

На вкладке **Контроллеры домена** приводится список контроллеров домена, назначенных сайту, с указанием имени компьютера и его IP-адреса.

В левом нижнем углу указано количество контроллеров, а в правом нижнем углу располагаются кнопки переключения страниц.

Для просмотра информации о контроллере домена необходимо открыть его карточку. Для открытия карточки нажать на контроллер домена в списке.

Для списка доступен поиск по названию. Для этого в верхнем левом углу вкладки в поле поиска ввести значение.

Добавление контроллера домена

Для создания контроллера домена нажать кнопку **[Новый контроллер домена]** на вкладке **Контроллеры домена**. Будет выполнен переход на карточку создания нового контроллера домена, где нужно заполнить обязательные поля **Имя компьютера** и **Имя сайта**.

Затем необходимо заполнить поля **Логин администратора ALD Pro** и **Пароль администратора ALD Pro**. Учетная запись должна обладать правами администратора домена.

Для сохранения нового контроллера необходимо нажать на кнопку сохранения в правом верхнем углу. Будет выполнен переход к списку контроллеров, назначенных сайту.

Для закрытия карточки создания контроллера и возврата к списку контроллеров, назначенных сайту, нажать на кнопку закрытия.

Назначение контроллера домена

Для назначения данному сайту контроллера домена необходимо на вкладке **Контроллеры домена** нажать кнопку **[Назначить контроллер домена]**, будет открыта карточка назначения контроллера. В поле **Имя компьютера** из выпадающего списка выбрать компьютер, который будет назначен контроллером домена. Поле **Имя сайта** заполняется автоматически и не доступно для изменения.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку контроллеров домена нажать на кнопку закрытия.

Удаление контроллера домена

Удаление контроллера домена выполняется на его карточке. Для открытия карточки на вкладке **Контроллеры домена** нажать на контроллер домена в списке. Для удаления контроллера нажать кнопку **[Удалить контроллер]**.

После удаления контроллера будет выполнен переход на вкладку управления контроллерами ALD Pro (см. [Контроллеры домена](#)).

Подсистемы сайта

На вкладке **Подсистемы сайта** отображаются подсистемы, которые затрагивает сайт.

4.2.1.4. Удаление сайта

Удаление сайта осуществляется на его карточке. Для открытия карточки необходимо на вкладке **Сайты и службы** нажать на соответствующий сайт, затем на карточке нажать кнопку **[Удалить сайт]** и в открывшемся окне подтвердить удаление. После удаления сайта будет выполнен переход к списку сайтов.

Важно: Нельзя удалить сайт, к которому привязана хотя бы одна подсистема. При попытке удаления такого сайта появляется сообщение “Удаление невозможно, так как в рамках данного сайта присутствуют подсистемы”.

4.2.2. Контроллеры домена

На вкладке осуществляется управление контроллерами домена.

4.2.2.1. Список контроллеров домена

На вкладке приведен список контроллеров домена с указанием имени компьютера и его IP-адреса, а также имени сайта, которому назначен контроллер домена.

В левом нижнем углу указано количество контроллеров, а в правом нижнем углу располагаются кнопки переключения страниц.

Для списка доступен поиск по названию. Для этого в верхнем левом углу вкладки в поле поиска ввести значение.

Для просмотра информации о контроллере домена нажать на контроллер домена. Будет открыта карточка контроллера домена с информацией о нем: имя компьютера и сайта, роли компьютера, соглашение о репликации.

Роли компьютера

Роли компьютера показывают администратору функции, которые выполняет компьютер в домене. Роли компьютера отображаются в графическом интерфейсе портала и не связаны с ролевой моделью пользователей. Каждая роль определяется уникальным состоянием записей LDAP.

Описание ролей компьютера:

- * ``AD Trust Controller`` отображается, если текущий контроллер является ☐
→ членом группы sysaccounts;
- * ``AD Trust Agent`` отображается, если у ipa-мастера есть запись в LDAP с ☐
→ определенными параметрами в `cn=ADTRUST,cn=XXX,cn=masters,cn=ipa,cn=etc`,
→ dc=XXX`, где `XXX` – имя домена;
- * ``IPA master`` отображается, если компьютер отвечает за запуск и работу ☐
→ служб IPA для обеспечения основных функций: доступ к серверной части LDAP, ☐
→ аутентификация Kerberos, HTTP-сервер;
- * ``DNS server`` отображается, если контроллер выполняет функции DNS-сервера,
→ DNSKeySync;
- * ``Глобальный каталог`` отображается, если контроллер выполняет функции ☐
→ глобального каталога;
- * ``PKIProxy`` отображается, если контроллер назначается для транслирования ☐
→ запроса сертификатов для контроллеров домена и подсистем ALD Pro на любой ☐
→ сервис выпуска сертификатов (Удостоверяющий центр).

Для просмотра администратором ролей компьютера необходимо открыть **Управление доменом -> Контроллеры**.

4.2.2.2. Добавление контроллера домена

Для добавления контроллера домена нажать кнопку **[Новый контроллер домена]**. Будет выполнен переход на карточку добавления нового контроллера домена. На карточке из выпадающего списка **Имя компьютера** выбрать компьютер для назначения роли контроллера домена, затем из выпадающего списка **Имя сайта** выбрать сайт, для которого

будет назначен контроллер.

Если контроллеру домена будет назначена роль глобального каталога, необходимо установить флаг **Назначить роль глобального каталога**.

Если контроллеру домена будет назначена роль для транслирования запроса сертификатов для контроллеров домена и подсистем ALD Pro на любой сервис выпуска сертификатов(Удостоверяющий центр), необходимо установить флаг **Назначить роль pkiпроху**.

Для сохранения нового контроллера необходимо нажать на кнопку сохранения в правом верхнем углу. Будет выполнен переход к списку контроллеров.

Для закрытия карточки и возврата к списку контроллеров домена нажать на кнопку закрытия.

Важно: Среднее время разворачивания контроллера домена может составлять от 10 до 70 минут, в зависимости от используемой конфигурации.

4.2.2.3. Удаление контроллера домена

На вкладке **Контроллеры домена** нажать на контроллер домена и в открывшейся карточке с информацией о нем нажать кнопку **[Удалить контроллер]**. После удаления будет выполнен переход к списку контроллеров домена.

4.2.3. Соглашения о репликации

На вкладке **Соглашения о репликации** осуществляется управление репликациями домена. Наличие соглашения о репликации между двумя доменами ALD Pro означает, что данные двух доменов будут синхронизироваться при изменении с обеих сторон.

4.2.3.1. Список соглашений о репликации

На вкладке приведен список соглашений о репликации. Каждая строка в списке отображает связь двух контроллеров домена, между которыми настроена репликация. В

случае недоступности одного контроллера домена его функции переходят другому контроллеру, с которым было создано соглашение.

Для списка доступен поиск по названию контроллера домена. Для этого начать вводить в поле поиска название, результат поиска будет выводиться по мере ввода.

Для просмотра информации о соглашении нажать на соответствующее соглашение в списке. Будет открыта карточка соглашения с информацией о нем.

В левом нижнем углу указано количество соглашений, а в правом нижнем углу располагаются кнопки переключения страниц.

4.2.3.2. Создание соглашения о репликации

Для создания соглашения о репликации нажать кнопку **[Новое соглашение]**. Будет открыта карточка создания нового соглашения.

На карточке необходимо из выпадающих списков **Левый узел** и **Правый узел** выбрать контроллеры домена, между которыми необходимо установить соглашение о репликации.

В поле **Название соглашения** задать имя соглашения. Если имя не будет задано, то при сохранении соглашения оно присвоится автоматически.

Для сохранения нового соглашения нажать на кнопку сохранения в правом верхнем углу и подтвердить действие.

Для закрытия карточки нажать кнопку закрытия.

4.2.3.3. Управление соглашениями о репликации

Управление соглашением осуществляется на его карточке. Для открытия карточки необходимо на вкладке **Соглашения о репликации** нажать на соглашение. На карточке указано название соглашения и контроллеры, между которыми установлено соглашение.

Поля **Левый узел** и **Правый узел** можно переинициализировать, тем самым вернув работоспособность недоступному контроллеру.

Для активации или отмены соглашения, соответственно, установить флаг **Включено** или **Выключено**.

Для закрытия карточки и возврата к списку соглашений нажать кнопку закрытия.

4.2.3.4. Удаление соглашения о репликации

Удалить соглашения можно из его карточки. Для открытия карточки необходимо на вкладке **Соглашения о репликации** нажать на соглашение списке, затем на карточке нажать кнопку **[Удалить соглашение]**. После подтверждения удаления будет выполнен переход к списку соглашений.

4.3. Дополнительные параметры групповых политик

Подраздел содержит функции расширения параметров и атрибутов групповых политик.

4.3.1. Параметры компьютеров

На вкладке осуществляется настройка и управление дополнительными параметрами компьютеров.

4.3.1.1. Каталог дополнительных параметров

На вкладке **Параметры компьютеров** отображен каталог дополнительных параметров, содержащий корневую папку **Дополнительные параметры**.

Внутри корневой папки параметров возможно добавлять параметры компьютеров и дополнительные папки. Папки возможно использовать для группировки параметров по функциональному назначению. Папки и параметры компьютеров отображаются в иерархическом виде.

Корневая папка недоступна для удаления и редактирования. Нельзя создавать объекты на одном уровне с этой папкой.

На вкладке доступен поиск папки или параметра. Для этого в соответствующем поле поиска начать вводить название параметра/папки, результат поиска будет выводиться по мере ввода.

Параметры из каталога дополнительных параметров компьютеров будут отображаться в карточке групповой политики, настраиваемой в подразделе *Групповые политики* (раздел *Групповые политики*).

4.3.1.2. Управление папками

Создание новой папки

Для создания папки нажать кнопку **[Новая папка]**. Будет открыта карточка создания папки.

На карточке необходимо заполнить обязательные поля **Название папки** и **Родительская папка**. По умолчанию для поля **Родительская папка** указана корневая папка **Дополнительные параметры**, при необходимости ее можно сменить.

Поле **Тип каталога** заполняется автоматически.

Для сохранения новой папки нажать на кнопку сохранения. Будет выполнен переход к каталогу дополнительных параметров.

Для закрытия карточки создания папки и возврата к каталогу дополнительных параметров нажать на кнопку закрытия.

Редактирование папки

Для редактирования папки необходимо выделить папку и нажать на кнопку **[Редактировать]**. Откроется карточка папки, где можно изменить поля **Название папки**, **Тип каталога** и **Родительская папка**.

Для применения изменений нажать на кнопку сохранения.

Для закрытия карточки создания папки и возврата к каталогу дополнительных параметров нажать на кнопку закрытия.

Удаление папки

Для удаления папки необходимо открыть карточку соответствующей папки и нажать на кнопку **[Удалить папку]**. После удаления папки будет выполнен переход к каталогу дополнительных параметров.

4.3.1.3. Управление параметрами

Добавление параметра

Для добавления параметра необходимо нажать кнопку **[Новый параметр]**. Будет открыта карточка создания нового параметра.

В карточке создания на вкладке **Основное** необходимо заполнить обязательные поля **Название параметра** (например, *Создание файла*), **Уникальный идентификатор** (например, *rbta_idap_filemanaged*), **Тип параметра**, **Папка параметра**.

В разделе **Требования к ОС** задается информация о том, с какими версиями ОС совместим данный параметр.

Для определения требований к ОС необходимо выбрать в выпадающем списке **Параметр ОС** один из атрибутов, задать значение параметра и выбрать один из следующих операторов сравнения:

- = - точное соответствие;
- ~ - указанная подстрока присутствует в значении;
- ; - задать несколько требований в ОС, читается через ИЛИ.

Если фильтр не указан, то проверка не выполняется.

В качестве значения в поле **Уникальный идентификатор** задать уникальное имя параметра, которое не совпадает с идентификаторами других параметров.

В поле **Тип параметра** выбор значения **Составной параметр** дает возможность использовать данный параметр множество раз при настройке групповой политики в подразделе *Групповые политики* (раздел *Групповые политики*). Выбор значения **Простой параметр** такую возможность исключает.

В поле **Папка параметра** в качестве значения указывается папка, из которой была нажата кнопка создания нового параметра. При необходимости папку можно изменить.

Поле **Тип каталога** будет заполнено автоматически.

Также можно заполнить поле **Назначение параметра**, указав описание параметра.

Вкладки **Атрибуты параметра** и **Конфигурация скрипта** станут доступны после сохранения параметра (см. *Редактирование параметра*).

Для сохранения нового параметра необходимо нажать кнопку сохранения. Будет выполнен переход к каталогу дополнительных параметров.

Для закрытия карточки создания параметра и возврата к каталогу дополнительных параметров нажать на кнопку закрытия.

Редактирование параметра

Редактирование параметра выполняется на его карточке. Для открытия карточки параметра необходимо в каталоге параметров выделить параметр и нажать кнопку **[Редактировать]**.

На карточке параметра присутствуют вкладки:

- **Основное;**
- **Атрибуты параметра;**
- **Конфигурация скрипта.**

Для закрытия карточки и возврата к каталогу дополнительных параметров нажать на кнопку закрытия.

Основное

На вкладке **Основное** приведена основная информация о параметре (см. [Добавление параметра](#)). Для редактирования доступны поля **Название параметра**, **Папка параметра** и **Назначение параметра**.

Для сохранения изменений нажать на кнопку сохранения. Будет выполнен переход к каталогу дополнительных параметров.

Атрибуты параметра

Список атрибутов параметра

На вкладке **Атрибуты параметра** приведен список атрибутов данного параметра с указанием их имен, идентификаторов и описания.

Для атрибутов в списке доступен поиск по названию и по идентификатору. Для этого в

поле поиска начать вводить название/идентификатор атрибута, результат поиска будет выводиться по мере ввода.

Добавление атрибута параметра

Для добавления нового атрибута нажать кнопку **[Новый атрибут]**. Будет открыта карточка создания атрибута. В карточке указать обязательные поля **Название атрибута** (например, *Наименование файла*) и **Уникальный идентификатор** (например, *rbta_idap_filename*). Также можно указать **Описание**.

Для сохранения атрибута нажать на кнопку сохранения. Будет выполнен переход к списку атрибутов.

Для закрытия карточки атрибута и возврата к списку атрибутов нажать на кнопку закрытия.

Редактирование атрибута параметра

Редактирование атрибута выполняется на его карточке. Для открытия карточки необходимо на вкладке **Атрибуты параметра** в списке нажать на атрибут. На карточке возможно изменить название атрибута и его описание.

Атрибут можно сделать обязательным. Атрибуты, отмеченные как **Обязательный**, должны быть заполнены при применении параметра. По умолчанию флаг **Обязательный** снят для нового атрибута параметра.

Атрибут составного параметра можно сделать уникальным, т.е. установить запрет на использование данного имени в параметрах этой или других групповых политик. Для этого необходимо нажать на кнопку **Сделать уникальным**. Уникальным можно сделать только обязательный атрибут. У параметра может быть только один уникальный атрибут, который используется для разрешения конфликтов при суммировании.

Для сохранения изменений нажать на кнопку сохранения. Будет выполнен переход к списку атрибутов.

Для закрытия карточки и возврата к списку атрибутов нажать на кнопку закрытия.

Удаление атрибута параметра

Удаление атрибута выполняется из его карточки. Для открытия карточки необходимо на вкладке **Атрибуты параметра** в списке нажать на атрибут. Для удаления атрибута нажать кнопку **[Удалить атрибут]**.

После подтверждения удаления будет выполнен переход к списку атрибутов.

Конфигурация скрипта

На вкладке **Конфигурация скрипта** в текстовом поле указывается скрипт, выполняемый при включении данного параметра.

Пример скрипта

Описание: скрипт создает файл в директории /opt, содержащий строку “Содержание файла”

```
{% set my_host = salt['grains.get']("nodename") %}
{% if salt['pillar.get']('aldpro-hosts:' + my_host) is defined %}
{% set filename = salt['pillar.get']('aldpro-hosts:' + my_host +
  ↳ ':gpид:attrid') %}

create_file:
  cmd.run:
    - name : |
        touch /opt/{{ filename }}.txt
        echo "Содержимое файла" >> /opt/{{ filename }}.txt

{% endif %}
```

Скрипт доступен для редактирования, для этого необходимо нажать кнопку **Редактировать файл**. Для сохранения изменений в скрипте нажать на кнопку сохранения в правом верхнем углу. Для отмены внесения изменений нажать кнопку **[Отменить]**.

Так как выполняется проверка конфигурации скрипта на предмет соблюдения общих правил, при сохранении может возникнуть предупреждение **Ошибка конфигурации скрипта. Игнорировать ошибку и сохранить изменения**. В случае, если автор скрипта уверен в его правильности, необходимо игнорировать данное предупреждение, нажав кнопку **Да**.

Для просмотра истории изменений скрипта нажать кнопку **История изменений**, будет открыта карточка с журналом изменений. Для закрытия карточки нажать на кнопку закрытия.

Удаление параметра

Удаление параметра выполняется из его карточки. Для открытия карточки параметра необходимо в каталоге параметров выделить параметр и нажать кнопку **[Редактировать]**. В карточке параметра нажать кнопку **[Удалить параметр]**.

После подтверждения удаления будет выполнен переход к каталогу дополнительных параметров.

4.3.2. Параметры пользователей

На вкладке осуществляется настройка и управление дополнительными параметрами пользователей.

4.3.2.1. Каталог дополнительных параметров

На вкладке **Параметры пользователей** отображен каталог дополнительных параметров, содержащий корневую папку **Дополнительные параметры**.

Внутри корневой папки параметров возможно добавлять параметры пользователей и дополнительные папки. Папки возможно использовать для группировки параметров по функциональному назначению. Папки и параметры пользователей отображаются в иерархическом виде.

Корневая папка недоступна для удаления и редактирования. Нельзя создавать объекты на одном уровне с этой папкой.

На вкладке доступен поиск папки или параметра. Для этого в соответствующем поле поиска начать вводить название параметра/папки, результат поиска будет выводиться по мере ввода.

Параметры из каталога дополнительных параметров пользователей будут отображаться в карточке групповой политики, настраиваемой в подразделе *Групповые политики* (раздел *Групповые политики*)

4.3.2.2. Управление папками

Создание новой папки

Для создания папки нажать кнопку **[Новая папка]**. Будет открыта карточка создания папки.

На карточке необходимо заполнить обязательные поля **Название папки** и **Родительская папка**. По умолчанию для поля **Родительская папка** указана корневая папка **Дополнительные параметры**, при необходимости ее можно сменить.

Поле **Тип каталога** заполняется автоматически.

Для сохранения новой папки нажать на кнопку сохранения. Будет выполнен переход к каталогу дополнительных параметров.

Для закрытия карточки создания папки и возврата к каталогу дополнительных параметров нажать на кнопку закрытия.

Редактирование папки

Для редактирования папки необходимо выделить папку и нажать на кнопку **[Редактировать]**. Откроется карточка папки, где можно изменить поля **Название папки**, **Тип каталога** и **Родительская папка**.

Для применения изменений нажать на кнопку сохранения.

Для закрытия карточки создания папки и возврата к каталогу дополнительных параметров нажать на кнопку закрытия.

Удаление папки

Для удаления папки необходимо открыть карточку соответствующей папки и нажать на кнопку **[Удалить папку]**. После удаления папки будет выполнен переход к каталогу дополнительных параметров.

4.3.2.3. Управление параметрами

Добавление параметра

Для добавления параметра необходимо нажать кнопку **[Новый параметр]**. Будет открыта карточка создания нового параметра.

В карточке создания на вкладке **Основное** необходимо заполнить обязательные поля **Название параметра** (например, *Создание файла*), **Уникальный идентификатор** (например, *rbta_idap_filemanaged*), **Тип параметра** и **Папка параметра**.

В разделе **Требования к ОС** задается информация о том, с какими версиями ОС совместим данный параметр.

Для определения требований к ОС необходимо выбрать в выпадающем списке **Параметр ОС** один из атрибутов, задать значение параметра и выбрать один из следующих операторов сравнения:

- = - точное соответствие;
- ~ - указанная подстрока присутствует в значении;
- ; - задать несколько требований в ОС, читается через ИЛИ.

В качестве значения в поле **Уникальный идентификатор** задать уникальное имя параметра, которое не совпадает с идентификаторами других параметров.

В поле **Тип параметра** выбор значения **Составной параметр** дает возможность использовать данный параметр множество раз при настройке групповой политики в подразделе *Групповые политики* (раздел *Групповые политики*). Выбор значения **Простой параметр** такую возможность исключает.

В поле **Папка параметра** в качестве значения указывается папка, из которой была нажата кнопка создания нового параметра. При необходимости папку можно изменить.

Поле **Тип каталога** будет заполнено автоматически.

Также можно заполнить поле **Назначение параметра**, указав описание параметра.

Вкладки **Атрибуты параметра** и **Конфигурация скрипта** станут доступны после сохранения параметра (см. *Редактирование параметра*).

Для сохранения нового параметра необходимо нажать кнопку сохранения. Будет выполнен переход к каталогу дополнительных параметров.

Для закрытия карточки создания параметра и возврата к каталогу дополнительных параметров нажать на кнопку закрытия.

Редактирование параметра

Редактирование параметра выполняется на его карточке. Для открытия карточки параметра необходимо в каталоге параметров выделить параметр и нажать кнопку **[Редактировать]**.

На карточке параметра присутствуют вкладки:

- **Основное;**
- **Атрибуты параметра;**
- **Конфигурация скрипта.**

Для закрытия карточки и возврата к каталогу дополнительных параметров нажать на кнопку закрытия.

Основное

На вкладке **Основное** приведена основная информация о параметре (см. [Добавление параметра](#)). Для редактирования доступны поля **Название параметра**, **Папка параметра** и **Назначение параметра**.

Для сохранения изменений нажать на кнопку сохранения. Будет выполнен переход к каталогу дополнительных параметров.

Атрибуты параметра

Список атрибутов параметра

На вкладке **Атрибуты параметра** приведен список атрибутов данного параметра с указанием их имен, идентификаторов и описания.

Для атрибутов в списке доступен поиск по названию и по идентификатору. Для этого в поле поиска начать вводить название/идентификатор атрибута, результат поиска будет выводиться по мере ввода.

Добавление атрибута параметра

Для добавления нового атрибута нажать кнопку **[Новый атрибут]**. Будет открыта карточка создания атрибута. В карточке указать обязательные поля **Название атрибута** (например, *Наименование файла*) и **Уникальный идентификатор** (например, *rbta_idap_filename*). Также можно указать **Описание**.

Для сохранения атрибута нажать на кнопку сохранения. Будет выполнен переход к списку атрибутов.

Для закрытия карточки атрибута и возврата к списку атрибутов нажать на кнопку закрытия.

Редактирование атрибута параметра

Редактирование атрибута выполняется на его карточке. Для открытия карточки необходимо на вкладке **Атрибуты параметра** в списке нажать на атрибут. На карточке возможно изменить название атрибута и его описание.

Атрибут можно сделать обязательным. Атрибуты, отмеченные как **Обязательные**, должны быть заполнены при применении параметра. По умолчанию флаг **Обязательный** снят для нового атрибута параметра.

Атрибут составного параметра можно сделать уникальным, т.е. установить запрет на использование данного имени в параметрах этой или других групповых политик. Для этого необходимо нажать на кнопку **Сделать уникальным**. Уникальным можно сделать только обязательный атрибут. У параметра может быть только один уникальный атрибут, который используется для разрешения конфликтов при суммировании.

Для сохранения изменений нажать на кнопку сохранения. Будет выполнен переход к списку атрибутов.

Для закрытия карточки и возврата к списку атрибутов нажать на кнопку закрытия.

Удаление атрибута параметра

Удаление атрибута выполняется из его карточки. Для открытия карточки необходимо на вкладке **Атрибуты параметра** в списке нажать на атрибут. Для удаления атрибута нажать кнопку **[Удалить атрибут]**.

После подтверждения удаления будет выполнен переход к списку атрибутов.

Конфигурация скрипта

На вкладке **Конфигурация скрипта** в текстовом поле указывается скрипт, выполняемый при включении данного параметра.

Пример скрипта

```
{% if user is not defined %}
  {% set user = salt['pillar.get']("user") %}
{% endif %}
{% set homedir = salt['user.info'](user).home %}

{% set folder_name = salt['pillar.get']('aldpro-users:'+ user +':gpid:attrid
↪ ') %}

{% if folder_name %}
file_create:
  cmd.run:
    - name : "touch {{ homedir }}/{{folder_name}}.txt"

{% endif %}
```

где:

gpid - Уникальный идентификатор параметра - значение из поля “Уникальный идентификатор” карточки созданного параметра

attrid - Уникальный идентификатор атрибута параметра - значение из поля “Уникальный идентификатор” карточки атрибута созданного параметра.

Скрипт доступен для редактирования, для этого необходимо нажать кнопку

Редактировать файл. Для сохранения изменений в скрипте нажать на кнопку сохранения в правом верхнем углу. Для отмены внесения изменений нажать кнопку **[Отменить]**.

Так как выполняется проверка конфигурации скрипта на предмет соблюдения общих правил, при сохранении может возникнуть предупреждение **Ошибка конфигурации скрипта. Игнорировать ошибку и сохранить изменения**. В случае, если автор скрипта уверен в его правильности, необходимо игнорировать данное предупреждение, нажав кнопку **Да**.

Для просмотра истории изменений скрипта нажать кнопку **История изменений**, будет открыта карточка с журналом изменений. Для закрытия карточки нажать на кнопку закрытия.

Удаление параметра

Удаление параметра выполняется из его карточки. Для открытия карточки параметра необходимо в каталоге параметров выделить параметр и нажать кнопку **[Редактировать]**. В карточке параметра нажать кнопку **[Удалить параметр]**.

После подтверждения удаления будет выполнен переход к каталогу дополнительных параметров.

Внимание: Названия дополнительных параметров групповых политик должны быть уникальными, в т.ч. относительно списка заданий автоматизации.

4.4. Каталог заданий автоматизации

В подразделе представлены функции управления заданиями автоматизации для рабочих станций и серверов.

В подразделе на вкладке **Задания автоматизации** приведен каталог заданий автоматизации, содержащий корневую папку **Задания автоматизации**. Внутри корневой папки дополнительных настроек возможно добавлять задания автоматизации и дополнительные папки. Папки и задания автоматизации отображаются в иерархическом виде.

Корневая папка недоступна для удаления и редактирования. Нельзя создавать объекты на одном уровне с этой папкой.

На вкладке доступен поиск папки или задания. Для этого в соответствующем поле поиска начать вводить название задания/папки, результат поиска будет выводиться по мере ввода.

Данные задания автоматизации будут отображаться в подразделе [Задания автоматизации](#) (раздел [Автоматизация](#)).

4.4.1. Управление папками

4.4.1.1. Создание новой папки

Для создания папки необходимо в структуре папок выбрать любую папку и нажать кнопку **[Новая папка]**. Будет открыта карточка создания папки.

На карточке необходимо заполнить обязательные поля **Название папки** и **Родительская папка**. По умолчанию для поля **Родительская папка** указана папка, из которой была нажата кнопка создания папки, при необходимости ее можно сменить.

Для сохранения новой папки нажать на кнопку сохранения. Будет выполнен переход к каталогу дополнительных заданий автоматизации.

Для закрытия карточки создания папки и возврата к каталогу дополнительных заданий автоматизации нажать на кнопку закрытия.

4.4.1.2. Редактирование папки

Для редактирования папки необходимо выделить папку в структуре и нажать на кнопку **[Редактировать]**. Откроется карточка папки, для редактирования доступны все поля.

Для применения изменений нажать на кнопку сохранения.

Для закрытия карточки создания папки и возврата к каталогу дополнительных заданий автоматизации нажать на кнопку закрытия.

4.4.1.3. Удаление папки

Для удаления папки необходимо открыть ее карточку и на карточке нажать кнопку **[Удалить папку]**. После удаления папки будет выполнен переход к каталогу дополнительных заданий автоматизации.

4.4.2. Управление заданиями

4.4.2.1. Добавление задания

Для добавления задания необходимо в структуре выбрать папку и нажать кнопку **[Новое задание]**. Будет открыта карточка добавления нового задания.

В карточке добавления задания на вкладке **Основное** необходимо заполнить обязательные поля **Название задания**, **Уникальный идентификатор** и **Родительская папка**. По умолчанию для поля **Родительская папка** указана папка, из которой была нажата кнопка добавления задания, при необходимости ее можно сменить. Также можно заполнить атрибут **Описание**.

Важно: Названия заданий должны быть уникальными, в т.ч. относительно списка кастомных параметров групповых.

После сохранения задания станут доступны для редактирования остальные вкладки (см. [Редактирование задания](#)).

Для сохранения нового задания необходимо нажать на кнопку сохранения. Будет выполнен переход к каталогу дополнительных заданий автоматизации.

Для закрытия карточки и возврата к каталогу дополнительных заданий автоматизации нажать на кнопку закрытия.

4.4.2.2. Редактирование задания

Для редактирования задания необходимо в каталоге дополнительных заданий выделить задание и нажать на кнопку **[Редактировать]**. Будет открыта карточка задания.

На карточке задания присутствуют вкладки:

- **Основное;**
- **Атрибуты задания;**
- **Конфигурация скрипта.**

Для закрытия карточки задания и возврата к каталогу дополнительных заданий автоматизации нажать на кнопку закрытия.

Основное

На вкладке **Основное** приведена основная информация о задании. Для редактирования доступны поля **Название задания** (например, *Создать новый файл*), **Уникальный идентификатор** (например, *createafile*), **Родительская папка** и **Описание**.

Для сохранения изменений нажать на кнопку сохранения. Будет выполнен переход к каталогу дополнительных заданий автоматизации.

Атрибуты задания

Список атрибутов задания

На вкладке **Атрибуты задания** приведен список атрибутов данного задания с указанием их имен, идентификаторов и описания.

Данные атрибуты будут использоваться в качестве параметров задания. Значения этих параметров будут задаваться при запуске задания автоматизации на вкладке **Каталог заданий автоматизации** в подразделе *Задания автоматизации* (раздел *Автоматизация*).

Для атрибутов в списке доступен поиск по названию и по идентификатору. Для этого в поле поиска начать вводить название/идентификатор атрибута, результат поиска будет выводиться по мере ввода.

Добавление атрибута задания

Для добавления нового атрибута нажать кнопку **[Новый атрибут]**. Будет открыта карточка создания атрибута. В карточке заполнить обязательные поля **Название атрибута** (например, *Содержимое файла*) и **Уникальный идентификатор** (например, *content*). Также можно указать **Описание**.

Для сохранения атрибута нажать на кнопку сохранения. Будет выполнен переход к списку атрибутов.

Для закрытия карточки атрибута и возврата к списку атрибутов нажать на кнопку закрытия.

Редактирование атрибута задания

Редактирование атрибута выполняется на его карточке. Для открытия карточки необходимо на вкладке **Атрибуты задания** в списке нажать на атрибут. На карточке возможно изменить название атрибута и его описание.

Для сохранения изменений нажать на кнопку сохранения. Будет выполнен переход к списку атрибутов.

Для закрытия карточки и возврата к списку атрибутов нажать на кнопку закрытия.

Удаление атрибута задания

Удаление атрибута выполняется из его карточки. Для открытия карточки необходимо на вкладке **Атрибуты задания** в списке нажать на атрибут. Для удаления атрибута нажать кнопку **[Удалить атрибут]**.

После подтверждения удаления будет выполнен переход к списку атрибутов.

4.4.2.3. Конфигурация скрипта

На вкладке **Конфигурация скрипта** в текстовом поле указывается скрипт, выполняемый при выполнении данного задания.

Пример

```
{% set vars1 = salt['pillar.get']("content") %}
test:
  cmd.run:
    - name: |
        echo {{ vars1 }} > /opt/test.txt
    - failhard: True
```

Скрипт доступен для редактирования, для этого необходимо нажать кнопку **Редактировать файл**. Для сохранения изменений в скрипте нажать на кнопку сохранения в правом верхнем углу. Для отмены внесения изменений нажать кнопку **[Отменить]**.

Для просмотра истории изменений скрипта нажать кнопку **История изменений**, будет открыта карточка с журналом изменений. Для закрытия карточки нажать на кнопку

закрытия.

4.4.3. Удаление задания

Удаление задания выполняется из его карточки. Для открытия карточки задания необходимо в каталоге дополнительных заданий автоматизации выбрать задание и нажать кнопку **[Редактировать]**. В карточке задания нажать кнопку **[Удалить задание]**.

После подтверждения удаления будет выполнен переход к каталогу дополнительных заданий автоматизации.

4.5. Службы и параметры Kerberos

Подраздел отображает функции управления службами Kerberos (те службы ALD Pro, где необходима аутентификация пользователя через действующий TGT-билет) и политикой билетов Kerberos.

4.5.1. Политика билетов Kerberos

На вкладке приведены поля для установки значений следующих настроек политики билетов Kerberos:

- **Максимальный срок для обновления (в секундах)** — срок, до наступления которого можно продлевать срок действия билета. Значение по умолчанию 604 800 секунд;
- **Максимальный срок жизни (в секундах)** — срок действия билета. Значение по умолчанию 86 400 секунд.

Максимально возможное значение для установки 2 147 483 647 секунд.

Для сохранения изменений нажать на кнопку сохранения в правом верхнем углу.

Чтобы вернуть настройки по умолчанию необходимо нажать кнопку **[Сбросить по умолчанию]**.

4.5.2. Службы Kerberos

На вкладке осуществляется управление службами. Доступно добавление новых служб, настройка и управление службами, а также удаление служб.

4.5.2.1. Список служб

На вкладке приводится список служб с указанием имени учетной записи.

Для служб в списке доступен поиск по названию атрибутов. Для этого в поле поиска начать вводить название/идентификатор атрибута, результат поиска будет выводиться по мере ввода.

Для просмотра информации о службе нажать на соответствующую службу в списке. Будет открыта карточка службы с информацией о ней.

В левом нижнем углу указано количество служб, а в правом нижнем углу располагаются кнопки переключения страниц.

4.5.2.2. Добавление службы

Для добавления новой службы нажать кнопку **[+ Новая служба]**. Будет выполнен переход на карточку новой службы.

На карточке из выпадающего списка **Класс службы** выбрать службу, затем из выпадающего списка **Имя компьютера** выбрать компьютер, на котором она будет запущена.

Для сохранения новой службы необходимо нажать на кнопку сохранения в правом верхнем углу. Будет выполнен переход к карточке настройки службы (см. [Управление службой](#)).

Для закрытия карточки службы и возврата к списку служб нажать на кнопку закрытия.

4.5.2.3. Управление службой

Управление службой осуществляется на ее карточке. Карточка открывается при нажатии на службу в списке служб.

Настройка службы

На карточке службы приведено присвоенное автоматически имя учетной записи службы, информация о классе службы и имени компьютера, на котором запущена служба. Данная информация недоступна для редактирования.

Для настройки доступны следующие пункты:

- **Доверено для делегирования;**
- **Доверие для аутентификации в качестве пользователя;**
- **Требуется предварительная аутентификация.**

Для включения/выключения соответствующей возможности установить/снять флаг в пункте.

Состояние службы определяется пунктом **Имеется ключ Kerberos, служба подготовлена к работе**. Если для службы создан контейнер ключа Kerberos, то отметка в пункте ставится автоматически, и служба готова к работе.

Добавление сертификата

Сертификат Kerberos возможно добавить двумя способами:

- загрузить сертификат в формате base64 или PEM из файла;
- ввести ключ сертификата вручную.

Для загрузки сертификата из файла нажать на кнопку **[Добавить из файла]**, в открывшемся окне навигации выбрать необходимый файл и затем в карточке нажать **[Сохранить]**. Система преобразует выбранный файл в необходимый формат. После успешной загрузки сертификата отобразятся даты начала и окончания действия сертификата, а также ключ сертификата.

Для ввода ключа сертификата вручную необходимо ввести его в поле **Введите ключ сертификата** и нажать **[Сохранить]**. После успешной загрузки сертификата отобразятся даты начала и окончания действия сертификата.

Одновременно можно установить только один сертификат. Для добавления нового сертификата с обновленным сроком действия необходимо удалить действующий сертификат и затем добавить новый.

Удаление сертификата

Удаления сертификата службы (например, при замене на сертификат с новым сроком действия) выполняется из карточки службы. Необходимо открыть карточку нажатием на службу в списке служб, затем на карточке нажать кнопку **[Удалить]**.

Для закрытия карточки службы и возврата к списку служб нажать на кнопку закрытия.

4.5.2.4. Удаление службы

Для удаления службы или одновременно несколько служб необходимо на вкладке **Службы** в списке отметить требуемые службы и нажать кнопку **[Удалить]**.

Чтоб отметить все имеющиеся службы — отметить пункт **Имя учетной записи**.

Также удалить службу можно из ее карточки: открыть карточку нажатием на службу в списке служб, затем на карточке нажать кнопку **[Удалить службу]**. После подтверждения удаления будет выполнен переход к списку служб.

4.6. Пользователи и группы

В подразделе выполняется управление параметрами пользователей и групп, а также расширение списка дополнительных атрибутов пользователей.

Подраздел состоит из вкладок:

- **Параметры пользователей;**
- **Параметры групп;**
- **POSIX идентификаторы;**
- **Атрибуты пользователей.**

4.6.1. Параметры пользователей

На вкладке приводятся значения параметров пользователей, которые будут использоваться по умолчанию при добавлении новых пользователей.

Параметры пользователей, обязательные для заполнения (заполняются автоматически после развертывания контролера домена, при необходимости могут быть изменены):

- **Группа пользователей по умолчанию** — указывается наименование группы пользователей, в которую добавляются все новые пользователи;
- **Основа домашних каталогов** — указывается директория, в которой будут создаваться домашние папки пользователей при первой авторизации на клиентском компьютере;
- **Оболочка по умолчанию** — указывается оболочка, которая будет отображена при работе в терминале;
- **Максимальная длина имени пользователя** — задается максимальная длина имени учетной записи пользователя;
- **Уведомление об окончании действия пароля (в днях)** — настраивается за сколько дней до истечения срока действия пароля уведомлять пользователя о необходимости сменить пароль.

Важно: Для корректной работы пользователя на портале управления **ALD Pro** при чтении информации о группах пользователей или работе пользователя с **API** по получению данных о группах пользователей рекомендуется оставить значение `ipausers` для поля **Группа пользователей по умолчанию**. Если такой возможности нет - необходимо, чтобы роль, назначенная пользователю, включала в себя привилегию `User groups - Read`.

Дополнительно можно указать следующие параметры:

- заполнить поля **Почтовый домен по умолчанию** и **Порядок разрешения доменов** - разделенный двоеточиями список доменов, которые используются для обработки кратких имен. По умолчанию поле не заполнено, т.к. используется контроллер домена;
- в блоке **Возможности подключаемого модуля пароля** отметить требуемые возможности:
 - **AllowNTHash** (отключен по умолчанию. Параметр необходим в случае использования траста с MS AD. Хэш NT будет записан в атрибуты `sambaNTPassword` и/или `ipaNTHash` во время смены пароля);
 - **KDC:Disable Last Success** (отслеживание последней успешной аутентификации пользовательских аккаунтов отключено по умолчанию во FreeIPA для уменьшения нагрузки на серверы, отключено . Если параметр активировать, то

вырастет нагрузка на контроллеры домена);

- **KDC:Disable Lockout** (отключение блокировки учетной записи при неверном вводе пароля. По умолчанию опция отключена, т.е. учетные записи будут блокироваться);

- при необходимости отметить пункт **Включить режим миграции**.

В списке **Выбранные объектные классы** приведены объектные классы, которые будут отображаться в карточке пользователя.

Чтобы добавить объектные классы для отображения необходимо в списке **Все объектные классы** отметить требуемые классы и перенести их в список **Выбранные объектные классы** нажатием кнопки [**<-**].

Чтобы исключить объектные классы необходимо в списке **Выбранные объектные классы** отметить требуемые классы и перенести их в список **Все объектные классы** нажатием кнопки [**->**].

Для списков объектных классов доступен поиск по названию. Для этого в соответствующем поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Внизу списков указано количество записей в данном списке.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

4.6.2. Параметры групп

На вкладке приводятся значения параметров групп пользователей, которые будут использоваться по умолчанию при добавлении новых групп.

В списке **Выбранные объектные классы** приведены объектные классы, которые будут отображаться в карточке группы.

Чтобы добавить объектные классы для отображения необходимо в списке **Все объектные классы** отметить требуемые классы и перенести их в список **Выбранные объектные классы** нажатием кнопки [**<-**].

Чтобы исключить объектные классы необходимо в списке **Выбранные объектные классы** отметить требуемые классы и перенести их в список **Все объектные классы** нажатием кнопки [**->**].

Для списков объектных классов доступен поиск по названию. Для этого в соответствующем поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Внизу списков указано количество записей в данном списке.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

4.6.3. POSIX идентификаторы

На вкладке осуществляется управление диапазонами идентификаторов.

4.6.3.1. Список диапазонов

На вкладке приведен список с указанием имени диапазона, первого идентификатора POSIX диапазона и общего количества идентификаторов в диапазоне.

Для списка доступен поиск по имени диапазона, первому идентификатору и количеству идентификаторов. Для этого в поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Внизу списка указано количество записей в списке.

4.6.3.2. Добавление диапазона

Для добавления нового диапазона необходимо нажать на кнопку **[Новый диапазон]**, будет выполнен переход на карточку нового диапазона.

На карточке заполнить обязательные поля **Имя диапазона**, **Основной ID**, **Размер диапазона**, **Основа основного RID** и **Основа вторичного RID**.

Для сохранения нового диапазона необходимо нажать на кнопку сохранения в правом верхнем углу. Будет выполнен переход к списку диапазонов.

Для закрытия карточки и возврата к списку диапазонов нажать на кнопку закрытия.

4.6.3.3. Удаление диапазона

Для удаления диапазона или одновременно несколько диапазонов необходимо в списке отметить требуемый диапазон и нажать кнопку **[Удалить диапазон]**.

4.6.4. Атрибуты пользователей

4.6.4.1. Список атрибутов

На вкладке приведен список атрибутов пользователей с указанием имени атрибута, типа данных атрибута и статуса атрибута.

Данные атрибуты будут определять поля для заполнения на вкладке **Дополнительные сведения** карточки пользователя в подразделе *Пользователи* (раздел *Пользователи и компьютеры*).

Для списка доступен поиск по имени и типу данных атрибута. Для этого в поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Внизу списка указано количество записей в списке.

4.6.4.2. Добавление атрибута

Для добавления нового атрибута необходимо нажать на кнопку **[Новый атрибут]**, будет выполнен переход на карточку нового атрибута.

На карточке заполнить обязательные поля **Имя атрибута** (например, *Дата рождения*) и **Тип данных атрибута**. Пункт **Статус атрибута** отмечается автоматически и не может быть изменен.

Для сохранения нового атрибута необходимо нажать на кнопку сохранения в правом верхнем углу. Будет выполнен переход к списку атрибутов.

Для закрытия карточки и возврата к списку атрибутов нажать на кнопку закрытия.

4.6.4.3. Удаление атрибута

Удаление атрибута выполняется на его карточке. Для открытия карточки необходимо в списке нажать на соответствующий атрибут, затем на карточке нажать кнопку **[Удалить атрибут]**. После подтверждения удаления будет выполнен переход к списку атрибутов.

4.7. Интеграции с доменами

4.7.1. Миграции MS AD

В подразделе представлены функции управления миграцией LDAP-объектов службы каталогов Microsoft Active Directory – пользователей, группы пользователей и подразделения в домен ALD Pro. Также, можно настроить правила переноса атрибутов, поскольку структура LDAP-объектов в MS AD и ALD Pro отличается.

Внимание: Для управления миграцией объектов из MS AD, учетная запись пользователя должна обладать соответствующей привелегией и должна быть добавлена в группы пользователей `trust admins` и `ald trust admin`.

4.7.1.1. Редактирование подключения к Active Directory

Редактирование подключения к Active Directory выполняется на его карточке. Для открытия карточки необходимо на вкладке **Миграция MS AD** нажать на соответствующий домен в списке.

Для закрытия карточки и возврата к списку нажать на кнопку закрытия.

Сопоставление полей при миграции

На вкладке настраивается сопоставление полей домена Active Directory с полями домена ALD Pro при выполнении миграции.

Список миграций

На вкладке приведен список настроенных сопоставлений с указанием поля в домене Active Directory, соответствующего поля в домене ALD Pro и относящегося к ним объекта миграции.

Для списка доступен поиск по названиям полей доменов. Для этого в поле поиска начать вводить название, результат поиска будет выводиться по мере ввода.

В левом нижнем углу указано количество записей в списке, а в правом нижнем углу кнопки переключения страниц.

Новое сопоставление полей миграции

Для создания нового сопоставления полей миграции необходимо выбрать подключение к домену, нажать на кнопку **Редактировать**, будет выполнен переход на карточку нового сопоставления.

На карточке необходимо в поле **Атрибут AD** указать поле домена Active Directory, в поле **Атрибут ALD Pro** указать поле домена ALD Pro и в выпадающем списке **Объект миграции** выбрать тип объекта.

Для сохранения нового сопоставления необходимо нажать на кнопку **Добавить**.

Для закрытия карточки и возврата к списку миграций нажать на кнопку закрытия.

Удаление сопоставления полей миграции

Для удаления сопоставления полей миграции или несколько сопоставлений одновременно необходимо в списке отметить требуемые сопоставления и нажать кнопку **[Удалить]**.

Чтоб отметить все имеющиеся сопоставления — отметить пункт **Атрибут Active Directory**.

Запуск миграции

Для запуска миграции из данного домена Active Directory необходимо выбрать подключение к домену, нажать кнопку **Настроить и запустить миграцию**, будет выполнен переход на карточку запуска миграции.

На карточке в обязательных для заполнения выпадающих списках необходимо выбрать из какого подразделения Active Directory в какое подразделение ALD Pro будет выполнена миграция.

При необходимости отметить требуемые объекты миграции. При выборе пункта **Пользователи** необходимо ввести пароль.

Затем необходимо заполнить поля **Логин администратора ALD Pro** и **Пароль администратора ALD Pro**. Учетная запись должна обладать правами администратора домена.

Для выполнения миграции необходимо нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку миграций нажать на кнопку закрытия.

4.7.1.2. Удаление подключения к Active Directory

Удаление подключения к Active Directory выполняется на его карточке. Для открытия карточки подключения необходимо в списке подключений на вкладке **Миграция объектов Active Directory** нажать на подключение, затем нажать на кнопку **Удалить**. После подтверждения удаления будет выполнен переход к списку подключений.

Важно: При удалении подключения к Active Directory, связанная с ним зона DNS не будет удалена автоматически. Удаление такой зоны DNS осуществляется только в ручном режиме (при необходимости).

4.7.2. Доверительные отношения

В подразделе представлены функции управления доверительными отношениями с доменами ALD Pro и Microsoft Active Directory (MS AD).

На вкладке подраздела приведен список доменов ALD Pro и MS AD, к которым выполнено подключение данным доменом.

Подключения к домену находятся в одном из трех состояний, указанные в столбце **Тип доверия**:

- **входящие:** доверительные отношения установлены для данного домена ALD Pro касательно пользователей другого домена ALD Pro или MS AD (ALD Pro имеет доступ к пользователям другого домена ALD Pro или MS AD). Входящее доверие нельзя создать на данном домене, оно создается автоматически, при создании исходящего доверия на другом домене с данным доменом;
- **исходящие:** доверительные отношения установлены для другого домена ALD Pro или MS AD касательно пользователей данного домена ALD Pro (другой домен ALD Pro или MS AD имеет доступ к пользователям ALD Pro);
- **двусторонние:** доверительные отношения установлены между другим доменом ALD Pro или MS AD и данным доменом ALD Pro.

Для списка доступен поиск по названию домена. Для этого в поле поиска начать вводить название, результат поиска будет выводиться по мере ввода. Список может быть отфильтрован по типу домена (**ALD Pro** или **MS AD**) и по типу доверия.

В левом нижнем углу указано количество доменов, а в правом нижнем углу кнопки переключения страниц.

4.7.2.1. Авторизации пользователей Active Directory

После установки доверительных отношений между доменами пользователи Active Directory получают возможность авторизоваться на рабочих станциях в домене ALD Pro, используя свои идентификаторы в домене Active Directory.

4.7.2.2. Создание нового подключения

Для установки доверительных отношений с новым доменом необходимо кликнуть кнопку **+** **Новое подключение**.

В карточке подключения в разделе **Настройка доверенного домена** указать:

- **Имя домена:** имя домена, с которым устанавливаются доверительные отношения, без указания контроллера домена;
- **Тип домена:** тип домена **ALD Pro** или **MS AD**, выбирается вручную в соответствие с типом домена, с которым устанавливаются доверительные отношения. При выборе некорректного типа домена доверительные отношения установлены не будут;
- **Учетная запись:** учетная запись, под которой устанавливаются доверительные

отношения, должна принадлежать домену, с которым устанавливаются доверительные отношения и обладать правами на установку доверительных отношений;

- **Пароль:** пароль учетной записи домена, с которым устанавливаются доверительные отношения;
- **Подтверждение пароля.**

В разделе **Настройки доверия** выбрать тип доверия: двусторонние или исходящие.

Для сохранения нового подключения необходимо нажать на кнопку **+ Добавить** в правом нижнем углу.

Для закрытия карточки и возврата к списку доменов нажать на кнопку закрытия.

Важно: Установление доверительных отношений (ДО) с доменами **MS AD** требует дополнительных действий. Перед установкой ДО на всех контроллерах домена **ALD Pro** необходимо выполнить команды:

```
sudo net conf setparm global "restrict anonymous" "0"
```

```
sudo aldroctl restart -i
```

После необходимо создать на портале управления **ALD Pro** ДО с доменом **MS AD**.

Затем на каждом контроллере домена **ALD Pro** необходимо выполнить команду:

```
rm /var/lib/sss/db/* && systemctl restart sssd
```

4.7.2.3. Редактирование подключения

Созданное подключение нельзя редактировать. Для внесения изменений в подключение необходимо удалить и создать заново.

4.7.2.4. Удаление подключения

Для удаления подключения на вкладке **Доверительные отношения** необходимо выбрать домен, отношения с которым необходимо разорвать, и нажать на кнопку **Удалить**. После подтверждения удаления домен пропадет из списка.

Внимание: При удалении доверительных отношений с доменом **ALD Pro** требуется дополнительное подтверждение. Необходимо ввести данные учетной записи (логин и пароль) домена, с которым удаляются отношения. Учетная запись должна обладать правами на управление доверительными отношениями.

4.8. Роли и права доступа

В подразделе приведены функции управления зонами ответственности при администрировании к разделам и функциям системы.

4.8.1. Возможности учетной записи пользователя

По умолчанию любой пользователь с учетной записью и без назначенных ему ролей в портале управления **ALD Pro** имеет доступ к следующей информации:

- **Личный кабинет портала управления ALD Pro:**

- просмотр информации о своей учетной записи (данные с вкладки **Основное** карточки пользователя);
- изменение мобильного телефона, открытых ключей SSH и пароля;

- Чтение информации и ряд операций с использованием **API ALD Pro**.

4.8.2. Права на операции в портале управления

Привилегии

Чтобы разрешить пользователю дополнительные (помимо доступных по умолчанию любой учетной записи без ролей) действия в портале управления, необходимо выдать ему

привилегии на требуемые операции. На каждую операцию или группу операций в портале управления есть соответствующая привилегия.

Привилегии выдаются на:

- Чтение (Read);
- Создание (Create или Add);
- Изменение (Modify);
- Удаление (Drop или Delete);
- Полные права: создание, изменение, удаление (Manage).

Каждая привилегия в составе роли позволяет выполнять определенные действия в конкретном подразделе портала управления. Полный перечень привилегий доступен в `privilege_matrix`.

Для выполнения некоторых действий в портале управления одной выбранной привилегии может быть недостаточно. Поэтому для корректной работы необходимо добавление дополнительных (связанных) привилегий.

При добавлении каждой привилегии в роль выполняется автоматическая проверка на наличие связанных с ней привилегий. Если связанные привилегии есть, отображается их перечень. Необходимо ознакомиться со списком дополнительных привилегий и убедиться, что их наличие в роли допускается. Связанные привилегии будут добавлены в роль только после подтверждения. Если добавление связанных привилегий не будет подтверждено, активация роли завершится с ошибкой.

Добавление связанных привилегий можно выполнить в любой момент до активации роли. Все привилегии, требующие внимания, отмечены в списке привилегий роли информационным значком.

Роли

Привилегии выдаются в составе ролей. Роли назначаются (делегируются) пользователям напрямую или могут наследоваться пользователями от групп, в которых они состоят.

На одного пользователя (группу пользователей) можно назначить несколько ролей. Тогда привилегии пользователя на операции в портале управления будут суммироваться по всем назначенным ему ролям и ролям, унаследованным от групп.

Внимание: Использование циклических (замкнутых) наследований групп пользователей будет приводить к некорректной работе механизма управления доступом на основе ролей в связи с особенностями работы с такими зависимостями. Будут учитываться только вложенные группы первого уровня. Создание таких наследований в продуктивных средах не рекомендуется.

На пользователей (группы пользователей) с помощью портала управления **ALD Pro** можно назначать роли с типами:

- Предустановленная;
- Пользовательская.

Все варианты ролей, доступных по умолчанию в портале управления, описаны в документе «Матрица и описание ролей».

4.8.3. Возможности для ограничения областей действия ролей и привилегий

В **ALD Pro** существует возможность ограничения областей действия ролей и привилегий.

Область действия роли - это совокупность привязки роли к подразделению и признака **Включая дочерние подразделения**. Если признак **Включая дочерние подразделения** не выбран, то область действия роли будет ограничена указанным подразделением. Если признак **Включая дочерние подразделения** выбран, то область действия роли будет ограничиваться всеми подразделениями ниже в иерархии, начиная с указанного подразделения.

Область действия привилегии наследуется от роли. Но есть исключения:

- Привилегии, которые не могут быть ограничены подразделением. Независимо от того, какая привязка указана для роли, в состав которой входит привилегия, такая привилегия всегда будет действовать на весь домен.
- Привилегии, которые могут быть ограничены и подразделением, и сайтом. Это привилегии на администрирование сервисов и подсистем. Для таких привилегий привязка к сайту указывается в свойствах самой привилегии в составе роли и от роли не наследуется. В роль можно включить несколько одинаковых привилегий с привязками к разным сайтам (одна привилегия - один сайт) или одну привилегию с

привязкой ко всем сайтам домена. При этом привязку к подразделению такие привилегии будут наследовать от роли.

Если привилегия назначена пользователю в составе нескольких ролей с разными областями действия, то суммарная область действия привилегии для пользователя будет складываться из областей действия всех его ролей с этой привилегией.

4.8.3.1. Типы администратора в системе

На вкладке **Роли в системе** приведен список типов администраторов с указанием наименования, типа (**Предустановленная, Системная, Пользовательская**), его состояния (**Активна, Редактируется, Ожидает активации, Активируется, Ошибка**), подразделения, описания. По умолчанию, на вкладке отображаются пользовательские и предустановленные типы администраторов.

Важно: Если изменить состав типов пользователя, который на данный момент находится на портале управления (сессия активна), то изменения согласно новым правам активируются только после обновления сессии браузера данного пользователя.

Для списка типов доступна фильтрация по значениям столбцов **Роль** (**Предустановленная, Системная, Пользовательская**) и **Состояние** (**Активна, Редактируется, Ожидает активации, Активируется, Ошибка**). Для этого необходимо нажать на значок фильтра рядом с названием соответствующего столбца и отметить требуемые значения для фильтрации.

В списке типов доступен поиск по названию типа и его описанию. Для этого в соответствующем поле поиска начать вводить название типа или описание, результат поиска будет выводиться по мере ввода.

Виды и состояния типов администраторов

Виды типов администраторов

Типы в Системе делятся на:

- **Предустановленная:** тип, который находится в **ALD Pro** по умолчанию. Существует одна предустановленная роль Главного администратора (**ALD Pro - Main**

Administrator). Эта роль по умолчанию при установке **ALD Pro** назначается пользователю `admin`. Пользователи с этой ролью обладают полными правами на весь портал управления.

Роль **ALD Pro - Main Administrator** обладает следующими свойствами для обеспечения и сохранения возможности полного доступа к portalу управления:

- Роль нельзя удалить;
- Данная роль должна быть назначена как минимум на одного активного пользователя;
- Постоянный состав привилегий и параметров роли.

На роль **ALD Pro - Main Administrator** можно назначить любого пользователя с учетной записью в портале управления **ALD Pro**.

Также поддерживается создание копии роли **ALD Pro - Main Administrator**, которая будет содержать полный набор привилегий, доступный для назначения средствами портала управления.

- **Системные:** типы, которые находятся в **ALD Pro** по умолчанию и используются для работы Системы. Недоступны для изменения, копирования, удаления и назначения на пользователей. Всегда в состоянии **Активна**. Для отображения их в таблице ролей по пути Управление доменом/Роли и права доступа необходимо установить флаг «Показывать системные роли», после чего эти роли появятся в таблице и будут доступны как по фильтру, так и по поиску, флаг сохраняется.

В **ALD Pro** присутствуют следующие системные роли:

- ALDPRO - CIFS server
- ALDPRO - Organization units
- ALDPRO - Organizational Units Service Account
- ALDPRO - RuPost Service Integrations
- ALDPRO - Saltstack Administrators
- ALDPRO - Service Role
- ALDPRO - Trusts Service Account
- Enrollment Administrator (с версии 2.4.0 - системная, до версии 2.4.0 - предустановленная)
- helpdesk (с версии 2.4.0 - системная, до версии 2.4.0 - предустановленная)
- Security Architect (с версии 2.4.0 - системная, до версии 2.4.0 - предустановленная)

- User Administrator (с версии 2.4.0 - системная, до версии 2.4.0 - предустановленная)
- **Пользовательские:** региональный администратор, типы, дающие доступ к подразделам портала, для чтения всего портала и созданные пользователями в **ALD Pro**. Доступны для создания, изменения, делегирования, копирования и удаления и назначения на пользователей.

По умолчанию в портале управления присутствуют следующие пользовательские роли, доступные после установки **ALD Pro**:

- роли с полными правами на операции в подразделах портала управления

Внимание: Для выполнения некоторых операций требуется дополнительное участие в группах. Детальная информация присутствует в описаниях привилегий. Пример: привилегия Domain Integrations - Manage требует участия пользователя в группах trust admins и ald trust admin.

- роль на чтение всего портала: **ALDPRO - Domain Viewer** предоставляет привилегии читать информацию во всех подразделах портала управления **ALD Pro**, за исключением подраздела **Управление доменом - Интеграция с доменами**.
- роль Регионального администратора: **ALD Pro - Regional Administrator** является ограниченной по правам копией роли Главного администратора (**ALD Pro - Main Administrator**), для которой можно указать область действия (**ALD Pro - Main Administrator** распространяется на весь домен).

В случае необходимости состав привилегий любой пользовательской роли может быть изменен (удалены лишние привилегии или добавлены недостающие). Если в роль, присутствующую в **ALD Pro** по умолчанию, будут внесены изменения (добавлены или удалены привилегии) доступы к подразделам могут отличаться от заявленных в документации.

Существует возможность создавать пользовательские роли с любым набором существующих в **ALD Pro** привилегий и необходимыми ограничениями областей действий.

Если требуется использовать пользовательскую роль как шаблон, рекомендуется в продуктивных средах создать копию шаблонной роли и работать дальше с копией. В этом случае появляется возможность вносить изменения в состав привилегий, менять привязки роли без опасения изменить начальную конфигурацию пользовательской роли.

Состояния типов администраторов

Тип может находиться в одном из следующих состояний:

- **Редактируется:** состояние для вновь созданного, скопированного, деактивированного типа или при смене статуса типа из состояния **Ошибка**. Все вкладки карточки типа доступны для внесения изменений. Тип можно изменить, копировать, активировать или удалить.
- **Ожидает активации:** состояние для типа после нажатия кнопки **Активировать роль**. Любые действия (копирование, редактирование, удаление, деактивация) с типом запрещены до окончания активации.
- **Активируется:** состояние для типа после состояния **Ожидает активации**. Любые действия (копирование, редактирование, удаление, деактивация) с типом запрещены до окончания активации.
- **Активна:** состояние для типа после успешного завершения процесса активации. Вкладка **Пользователи** карточки типа доступна для внесения изменений. Тип можно копировать, удалить, делегировать или перевести в статус редактирования.
- **Ошибка:** состояние для типа в случае провала активации. Вкладка **Пользователи** карточки типа доступна для внесения изменений. Тип можно копировать, удалить или перевести в статус редактирования.

Важно: Активный пользовательский тип администратора можно деактивировать, нажав кнопку **Деактивировать роль**. В этом случае пользователь, которому назначен данный тип, теряет права, которые давал данный тип.

Таблица состояний ролей и операций с ними

Состояния ролей и операции с ними	Редактируется	Ожидает активации	Активируется	Активна	Ошибка
Действия, приведшие к статусу	<ul style="list-style-type: none">• Создание новой роли• Создание копии роли• Деактивация роли• Перевод на редактирование из состояния «Ошибка»	Команда на активацию роли	Старт внутренних механизмов (демон активации)	Успешное завершение работы внутреннего демона активации	Ошибка в работе внутреннего демона активации

continues on next page

Таблица 4.1 – продолжение с предыдущей страницы

Состояния ролей и операции с ними	Редактируется	Ожидает активации	Активируется	Активна	Ошибка
Действия для выхода из статуса	Команда на активацию роли	Старт внутренних механизмов (демон активации)	Завершение работы демона активации	Команда на редактирование роли	Команда на редактирование роли
Изменение названия роли	Нет	Нет	Нет	Нет	Нет
Изменение описания роли	Да	Нет	Нет	Нет	Нет
Изменение привязки роли к подразделению	Да	Нет	Нет	Нет	Нет
Изменение признака «Включая дочерние подразделения»	Да	Нет	Нет	Нет	Нет
Создание копии роли	Да	Нет	Нет	Да	Да
Удаление роли	Да	Нет	Нет	Да	Да
Перевод в статус редактирования	Нет	Нет	Нет	Да	Да
Активация роли	Да	Нет	Нет	Нет	Нет
Делегирование роли (назначение на пользователей и группы пользователей)	Да	Нет	Нет	Да	Нет
Добавление привилегий в состав роли	Да	Нет	Нет	Нет	Нет
Удаление привилегий из роли	Да	Нет	Нет	Нет	Нет
Изменение назначений привилегий роли на сайты	Да	Нет	Нет	Нет	Нет

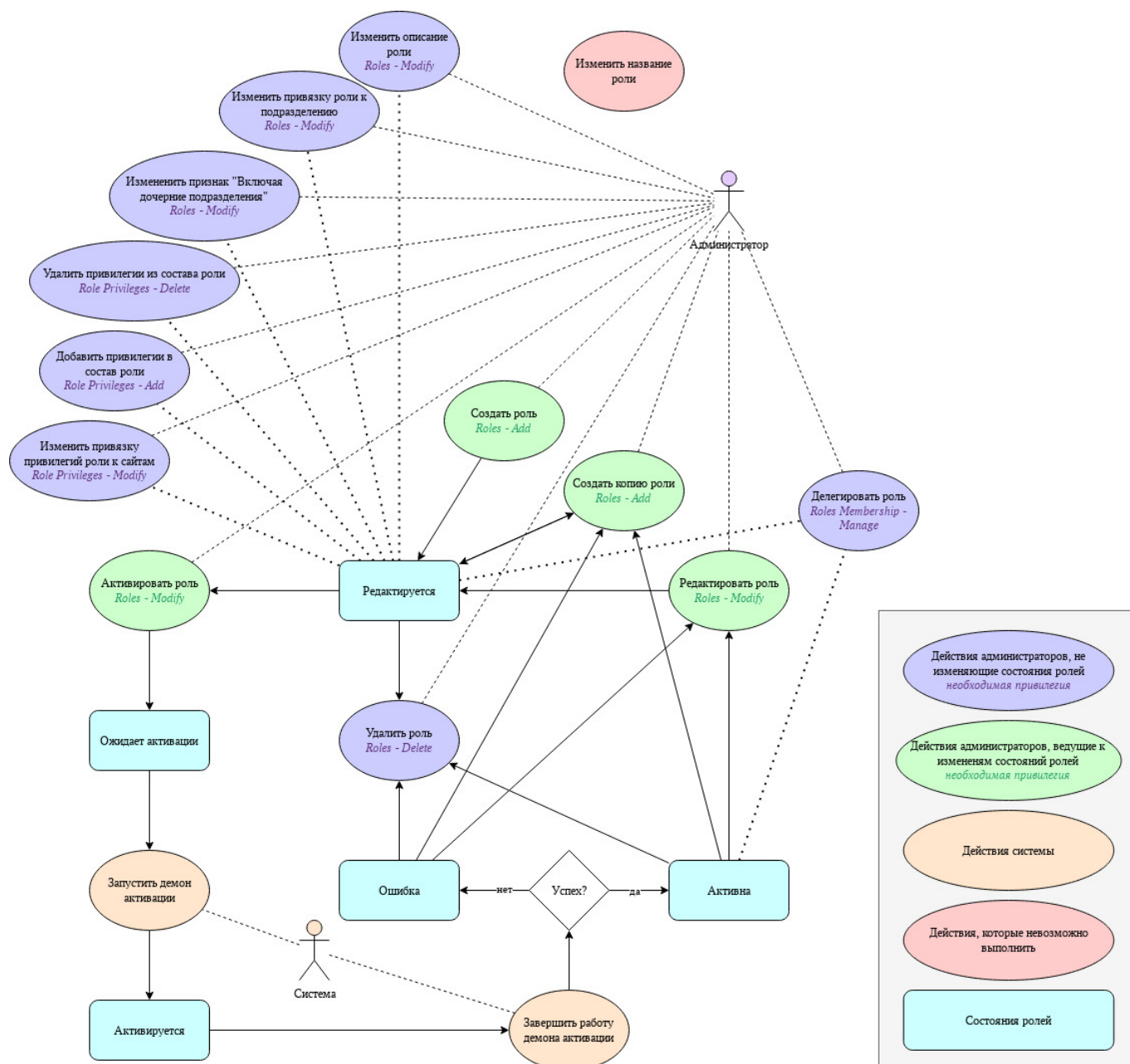


Рисунок 4.1 – Схема состояний ролей и операций с ними

Статус «Редактируется»

Характеристики статуса	Описания и значения
Предшествующие статусы	«Активна» - «Ошибкa»

continues on next page

Таблица 4.2 – продолжение с предыдущей страницы

Характеристики статуса	Описания и значения
Условия получения статуса	- Создание новой роли (после команды «Сохранить» на форме создания новой роли) Сохранение роли после копирования (доступно копирование ролей из статусов «Редактируется», «Активна» и «Ошибка» по команде «Копировать роль») Деактивация роли (операцию можно выполнить из статуса «Активна» командой «Деактивировать роль»)- Смена статуса роли из состояния «Ошибка» (выполняется командой «Редактировать роль»)
Следующие статусы	«Ожидает активации»
Условия перехода в следующие статусы	Команда на активацию роли

В статусе «Редактируется»:

- Пользователи, которым назначена роль, не получают привилегии из состава этой роли: привилегии становятся доступными только в статусе роли «Активна»
- Возможны следующие операции при наличии привилегий в активных ролях пользователей, выполняющих операции, и при выполнении ограничений:

Операции	Необходимые привилегии	Ограничения
Изменение описания роли	Roles Modify	- Область действия активной роли пользователя с привилегией Roles - Modify включает в себя область действия роли, над которой выполняется действие
Изменение привязки роли к подразделению		
Изменение распространения роли на дочерние подразделения		
Создание копии роли	Roles - Add	- Без ограничений: можно создать копию любой роли. Внимание: Для успешного выполнения дальнейших операций с полученной в результате копирования ролью необходимо убедиться, что области действия ролей с привилегиями на эти операции включают в себя область действия новой роли.
Удаление роли	Roles Delete	- Область действия активной роли пользователя с привилегией Roles - Delete включает в себя область действия роли, над которой выполняется действие

continues on next page

Таблица 4.3 – продолжение с предыдущей страницы

Операции	Необходимые привилегии	Ограничения
Активация роли	Roles Modify	- Область действия активной роли пользователя с привилегией Roles Modify включает в себя область действия активируемой роли - Подразделения всех без исключения пользователей, назначенных на роль, попадают в область действия активной роли пользователя с привилегией Roles Membership - Manage - Подразделения всех без исключения пользователей, входящих в состав групп, назначенных на роль, попадают в область действия активной роли пользователя с привилегией Roles Membership - Manage. Принадлежность групп пользователей к подразделениям не учитывается - Для исключения возможности эскалации привилегий добавлены следующие ограничения при активации роли: - Пользователь, выполняющий активацию, обладает всеми привилегиями (суммарно по всем назначенным ему активным ролям), которые входят в состав активируемой роли - Привязки к сайтам привилегий в составе активируемой роли соответствуют привязкам к сайтам привилегий в активных ролях пользователя, выполняющего активацию
Делегирование роли	Roles Membership Manage	- Без ограничений: достаточно наличия привилегии Roles Membership - Manage Внимание: Проверки на соответствие подразделений делегируемых пользователей и привязок роли к подразделению выполняются при активации роли от имени активирующего роль администратора
Добавление привилегий в состав роли	Role Privileges - Add	- Область действия активной роли пользователя с привилегией Role Privileges - Add включает в себя область действия роли, над которой выполняется действие
Удаление привилегий из роли	Role Privileges - Delete	- Область действия активной роли пользователя с привилегией Role Privileges - Delete включает в себя область действия роли, над которой выполняется действие
Изменение привязок привилегий роли к сайтам	Role Privileges - Modify	- Область действия активной роли пользователя с привилегией Role Privileges - Modify включает в себя область действия роли, над которой выполняется действие

Статус «Ожидает активации»

Характеристики статуса	Описания и значения
Предшествующие статусы	- «Редактируется»
Условия получения статуса	- Переводится автоматически после команды «Активировать роль»
Следующие статусы	- «Активируется»
Условия перехода в следующие статусы	Старт внутренних процессов по активации роли

В статусе «Ожидает активации»:

- Пользователи, которым назначена роль, не получают привилегии из состава этой роли: привилегии становятся доступными только в статусе роли «Активна»
- Никакие операции с ролью не доступны

Статус «Активируется»

Характеристики статуса	Описания и значения
Предшествующие статусы	- «Ожидает активации»
Условия получения статуса	- Переводится автоматически при старте внутренних процессов по активации роли
Следующие статусы	- «Ошибка» - «Активна»
Условия перехода в следующие статусы	- «Ошибка» - завершение внутренних процессов по активации роли с ошибкой - «Активна» - успешное завершение внутренних процессов по активации роли

В статусе «Активируется»:

- Пользователи, которым назначена роль, не получают привилегии из состава этой роли: привилегии становятся доступными только в статусе роли «Активна»
- Никакие операции с ролью не доступны

Статус «Активна»

Характеристики статуса	Описания и значения
Предшествующие статусы	- «Активируется»
Условия получения статуса	- Переводится автоматически при успешном завершении внутренних процессов по активации роли
Следующие статусы	- «Редактируется»
Условия перехода в следующие статусы	- Команда на редактирование роли

В статусе «Активна»:

- Пользователи, которым назначена роль, получают все привилегии из состава этой роли
- Возможны следующие операции при наличии привилегий в активных ролях пользователей, выполняющих операции, и при выполнении ограничений:

Статус «Ошибка»

Характеристики статуса	Описания и значения
Предшествующие статусы	- «Активируется»
Условия получения статуса	- Переводится автоматически при завершении с ошибкой внутренних процессов по активации роли
Следующие статусы	- «Редактируется»
Условия перехода в следующие статусы	- Команда на редактирование роли

В статусе «Ошибка»:

- Пользователи, которым назначена роль, не получают привилегии из состава этой роли: привилегии становятся доступными только в статусе роли «Активна»
- Возможны следующие операции при наличии привилегий в активных ролях пользователей, выполняющих операции, и при выполнении ограничений:

Операции	Необходимые привилегии	Ограничения
Создание копии роли	Roles - Add	- Без ограничений: можно создать копию любой роли. Внимание: Для успешного выполнения дальнейших операций с полученной в результате копирования ролью необходимо убедиться, что области действия ролей с привилегиями на эти операции включают в себя область действия новой роли
Удаление роли	Roles Delete	- Область действия активной роли пользователя с привилегией Roles - Delete включает в себя область действия роли, над которой выполняется действие
Перевод в статус редактирования	Roles Modify	- Область действия активной роли пользователя с привилегией Roles - Modify включает в себя область действия роли, над которой выполняется действие

Добавление типа администратора

Для добавления нового типа администратора необходимо нажать на кнопку [+ Новая роль], будет выполнен переход на карточку нового типа.

На карточке на вкладке **Основное** ввести информацию о типе. Обязательные для заполнения поля отмечены соответствующим образом.

Для добавления типа нажать на кнопку сохранения в правом верхнем углу. После этого станут доступны для редактирования вкладки **Пользователи** и **Привилегии**.

Для активации типа нажать кнопку **Активировать роль**.

Важно: Тип может быть активирована только при наличии хотя бы одной возможности при администрировании.

Для копирования типа администратора нажать кнопку **Копировать роль**. После подтверждения копирования откроется новая несохраненная копия типа.

Для закрытия карточки и возврата к списку типов администратора нажать на кнопку

закрытия.

В ALD Pro можно создать копии:

- любой пользовательской роли
- роли ALD Pro - Main Administrator

Копия роли содержит:

- набор привилегий, который отображается на вкладке «Привилегии» исходной роли
- набор пользователей и групп, на которых была назначена исходная роль
- привязку к подразделению исходной роли
- ограничения привилегий сайтами, как в исходной роли (при наличии)

Названия ролей в рамках домена должны быть уникальны, название копии не должно совпадать с названием исходной роли.

Важно: Копия роли ALD Pro - Main Administrator не будет содержать системных привилегий исходной роли, поэтому возможна потеря части прав Главного администратора пользователями, которым будет назначена копия его роли.

Пользователи

На вкладке **Пользователи** тип назначается на пользователей и группы пользователей.

В блоке **Назначена на пользователей** в списке **Выбранные пользователи** указаны пользователи, которым присвоен данный тип. В списке **Все пользователи** указаны все пользователи домена.

Во всех списках доступен поиск по названию. Для этого в соответствующем поле поиска ввести значение от трех символов, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для назначения пользователям типа необходимо в списке **Все пользователи** отметить пользователей, которым нужно назначить данный тип, и перенести их в список **Выбранные пользователи** нажатием кнопки [**<-**].

Для отмены назначения типа пользователям необходимо в списке **Выбранные**

пользователи отметить требуемые записи и перенести их в список **Все пользователи** нажатием кнопки [->].

В блоке **Назначена на группу пользователей** в списке **Выбранные группы** указаны группы, которым присвоен данный тип. В списке **Все группы** указаны все группы домена.

Во всех списках доступен поиск по названию. Для этого в соответствующем поле поиска начать вводить название группы, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для назначения группам пользователей типа администратора необходимо в списке **Все группы** отметить группы, которым нужно назначить данный тип, и перенести их в список **Выбранные группы** нажатием кнопки [<-].

Для отмены назначения типа администратора группам пользователей необходимо в списке **Выбранные группы** отметить требуемые записи и перенести их в список **Все группы** нажатием кнопки [->].

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку типов администратора нажать на кнопку закрытия.

Возможности при администрировании

На вкладке **Привилегии** типа администратора назначаются возможности при администрировании.

Важно: Возможности при администрировании можно назначить только типу в состоянии **Редактируется**.

На вкладке приведен список возможностей, назначенных типу, с указанием наименования возможности, сайта (заполнено для возможностей, для которых требуется привязка к сайту), подразделения, наследует ли от типа значение признака **Включая дочерние подразделения** и статуса.

Для списка доступен поиск по наименованию возможности. Для этого в поле поиска начать

вводить имя, результат поиска будет выводиться по мере ввода.

Для списка доступна фильтрация по значениям полей **Сайт**, **Подразделение**, **Дочерние** и **Статус**. Для этого нужно кликнуть по значку фильтрации рядом с соответствующим столбцом и выбрать параметр фильтрации.

Для списка доступна сортировка по полю **Подразделение**. Для этого нужно кликнуть по стрелочке рядом с полем.

Внизу списка указано количество возможностей.

Для добавления возможности при администрировании нажать кнопку **[+ Добавить привилегию]**. В результате откроется карточка новой возможности.

Выбрать нужную возможность из выпадающего списка поля **Привилегия**. Описание данной возможности отобразится в поле **Описание**.

Важно: У добавленной в тип администратора возможности можно редактировать только сайт, если возможность требует привязки к сайту. Во всех остальных случаях редактировать возможность нельзя. Ее можно только удалить и создать заново.

Если выбранная возможность имеет зависимости и не может использоваться без других возможностей, в столбце **Статус** таблицы возможностей отобразится ошибка. При открытии карточки возможности, в поле **Связанные привилегии** отобразится список связанных возможностей.

В разделе **Нужно добавить** также появятся связанные привилегии и кнопки со стрелками. Для добавления связанной возможности достаточно кликнуть стрелку вниз. Возможность перейдет в раздел **Добавленные** и автоматически добавится в список возможностей редактируемого типа при сохранении.

Для удаления одной или нескольких возможностей последовательно зайти в карточки возможности и нажать кнопку **Удалить привилегию**. Или выделить возможности, которые необходимо удалить, в списке возможностей и нажать кнопку **[- Удалить]**.

Для закрытия вкладки **Привилегии** и возврата к списку типов нажать на кнопку закрытия.

Управление типами администратора

Управление типами администратора доступно:

- из карточки **типа администратора**
- из карточки **пользователя**
- из карточки **группы пользователей**

Возможности для управления типами администраторов

Для создания типа администратора требуются следующие возможности:

Действие	Необходимые привилегии	Коментарии
Создать новую роль и сохранить ее	Roles - Add	При создании роли надо определить подразделение, к которому эта роль будет привязана. Подразделение новой роли должно входить в ограничение области действия по подразделениям (с учетом признака «Включая дочерние подразделения») всех привилегий Roles - Add у текущего пользователя
Добавить привилегии в роль	Role Privileges - Add	Достаточно наличия привилегии Role Privileges - Add у исполнителя. Для удаления привилегий потребуется привилегия Role Privileges - Delete
Добавить связанные привилегии	Role Privileges - Add	Достаточно наличия привилегии Role Privileges - Add у исполнителя. Операция должна быть выполнена до активации роли
Указать привязки привилегий к сайтам	Role Privileges - Modify	Достаточно наличия привилегии Role Privileges - Modify у исполнителя
Назначить пользователей на роль	Roles Membership - Manage	Достаточно наличия привилегии Roles Membership - Manage у исполнителя. Эта привилегия дает право на назначение роли как пользователям, так и группам пользователей. Этот пункт может не выполняться, если необходимо добавлять пользователей в активную роль

continues on next page

Таблица 4.4 – продолжение с предыдущей страницы

Действие	Необходимые привилегии	Комментарии
Активировать роль	Roles - Modify	- Привязка к подразделению активной роли пользователя с привилегией Roles - Modify включает в себя область действия активируемой роли - Подразделения всех без исключения пользователей, назначенных на роль, попадают в область действия активной роли пользователя с привилегией Roles Membership - Manage - Подразделения всех без исключения пользователей, входящих в состав групп, назначенных на роль, попадают в область действия активной роли пользователя с привилегией Roles Membership - Manage. Принадлежность групп пользователей к подразделениям не учитывается - Подразделения всех без исключения пользователей, входящих в состав групп, назначенных на роль, попадают в область действия активируемой роли - Подразделения всех без исключения пользователей, назначенных на роль, попадают в область действия активируемой роли - Для исключения возможности эскалации привилегий добавлены следующие ограничения при активации роли: * Пользователь, выполняющий активацию, обладает всеми привилегиями (суммарно по всем назначенным ему активным ролям), которые входят в состав активируемой роли * Привязки к сайтам привилегий в составе активируемой роли соответствуют привязкам к сайтам привилегий в активных ролях пользователя, выполняющего активацию
Добавить пользователей в активную роль	Roles Membership - Manage	- Область действия активной роли пользователя с привилегией Roles Membership - Manage включает в себя область действия роли, над которой выполняется действие - Подразделение пользователя, назначаемого на роль (исключаемого из роли), попадает в область действия активной роли пользователя с привилегией Roles Membership - Manage- Подразделения всех без исключения пользователей, входящих в состав группы, назначаемой на роль (исключаемой из роли), попадают в область действия активной роли пользователя с привилегией Roles Membership - Manage. Принадлежность групп пользователей к подразделениям не учитывается

В таблице не приводится перечень связанных привилегий, которые необходимо будет добавить по требованию системы для корректной работы привилегий, указанных в графе «Необходимые привилегии».

Управление типами администратора из карточки типа администратора

В разделе **Назначена на пользователя** на вкладке **Пользователи** в списке **Выбранные пользователи** приведен список пользователей, наделенных типом. В списке **Все пользователи** приведен список всех пользователей домена. Во всех списках доступен поиск по имени пользователя и по должности. Для этого в соответствующем поле поиска начать вводить имя/должность, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для наделения пользователей возможностями соответствующего типа необходимо в списке **Все пользователи** отметить требуемые записи и перенести их в список

Выбранные пользователи нажатием кнопки [**<-**].

Для исключения пользователей из списка обладателей соответствующего типа необходимо в списке **Выбранные пользователи** отметить требуемые записи и перенести их в список **Все пользователи** нажатием кнопки [**->**].

В разделе **Назначена на группу пользователей** на вкладке **Пользователи** в списке **Выбранные группы** приведен список групп, наделенных типом. В списке **Все группы** приведен список всех групп домена. Во всех списках доступен поиск по названию группы. Для этого в соответствующем поле поиска начать вводить название, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для наделения группы возможностями соответствующего типа необходимо в списке **Все группы** отметить требуемые записи и перенести их в список **Выбранные группы** нажатием кнопки [**<-**].

Для исключения группы из списка обладателей соответствующего типа необходимо в списке **Выбранные группы** отметить требуемые записи и перенести их в список **Все группы** нажатием кнопки [**->**].

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

Управление типами администратора из карточки пользователя

Управление типами администратора из карточки пользователя осуществляется на вкладке **Роли**. На вкладке задаются типы администратора, которыми будет наделена учетная запись пользователя.

В списке **Выбранные роли** указаны типы администратора, которыми будет наделена учетная запись пользователя. В списке **Все роли** указаны все типы администратора в системе.

Во всех списках доступен поиск по названию. Для этого в соответствующем поле поиска начать вводить название типа администратора, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для наделения пользователей возможностями соответствующего типа необходимо в списке **Все роли** отметить типы, которыми требуется наделить пользователя, и перенести их в список **Выбранные роли** нажатием кнопки [**<-**].

Для исключения пользователей из списка обладателей соответствующего типа необходимо в списке **Выбранные роли** отметить требуемые записи и перенести их в список **Все роли** нажатием кнопки [**->**].

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

Управление типами администратора из карточки группы пользователей

Управление типами администратора из карточки группы пользователей осуществляется на вкладке **Роли**. На вкладке задаются типы администратора, которыми будет наделена группа пользователей.

В списке **Выбранные роли** указаны типы администратора, которыми будет наделена группа пользователей. В списке **Все роли** указаны все типы администратора в системе.

Во всех списках доступен поиск по названию. Для этого в соответствующем поле поиска начать вводить название типа администратора, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для наделения группы пользователей возможностями соответствующего типа необходимо в списке **Все роли** отметить типы, которыми требуется наделить группу пользователей, и перенести их в список **Выбранные роли** нажатием кнопки [**<-**].

Для исключения группы пользователей из списка обладателей соответствующего типа необходимо в списке **Выбранные роли** отметить требуемые записи и перенести их в список **Все роли** нажатием кнопки [**->**].

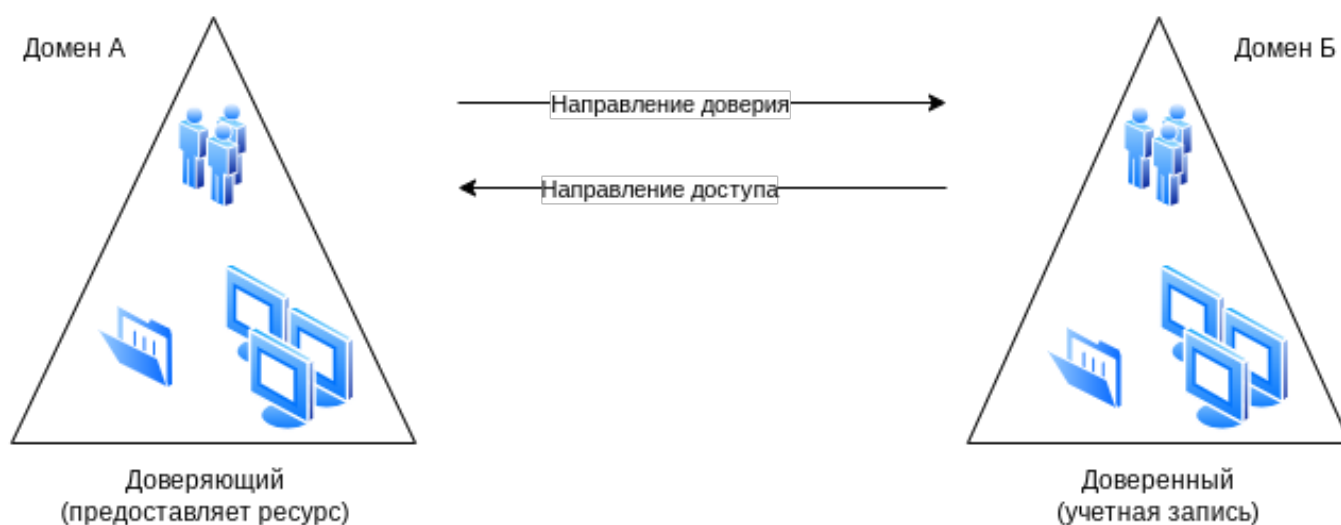
Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

4.9. Доверие между доменами ALD Pro

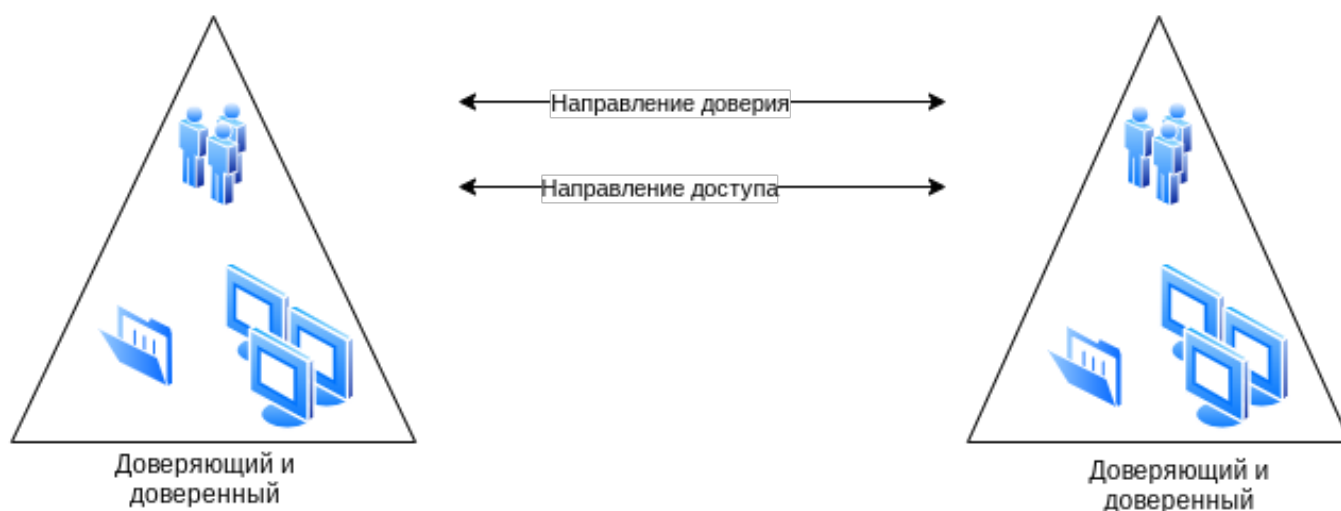
Доверие между доменами ALD Pro представляет собой инструмент создания доверительных отношений между доменами ALD Pro, одного уровня.

Отношения доверия обеспечивают доступ в одном или двух направлениях:

- Одностороннее доверие позволяет пользователям и группам из домена Б получать доступ к ресурсам в домене А, но не наоборот. Домен А доверяет домену Б, но домен Б не доверяет домену А. При создании такого доверия в интерфейсе ALD Pro будут созданы исходящие доверительные отношения;



- Двустороннее доверие позволяет пользователям и группам из домена А получать доступ к ресурсам в домене Б и наоборот. Запросы проверки подлинности могут передаваться между двумя доменами в обоих направлениях. Домен А доверяет домену Б, а домен Б доверяет домену А.



Доверительные отношения между доменами позволяют:

- Авторизацию пользователей доверенных доменов на компьютерах доверяющих доменов;
- Доступ к сетевым ресурсам доверяющего домена пользователям доверенного домена;
- Разграничение доступа к ресурсам доверяющего домена.

Интерфейс раздела “Доверие между доменами ALD Pro” состоит из одного подраздела - “Подключение к доменам ALD Pro”.

Важно: Создание доверительных отношений между доменами ALD Pro на портале управления без патчей sssd и freeipa из личного кабинета может привести к сбоям в работе samba.

4.9.1. Особенности работы раздела «Доверие между доменами ALD Pro»

Доверительные отношения(ДО) устанавливаются только между доменами одного уровня.

При создании ДО между двумя доменами **ALD Pro** может произойти пересечение диапазонов идентификаторов пользователей и групп пользователей (uid и gid), в следствии чего пользователи смогут получить несанкционированный доступ к ресурсам доверяющего домена.

Пример: имеются пользователь **user1** домена `domain1.test` с условным uid `10000` и пользователь **user2** домена `domain2.lan` с таким же условным uid `10000`. Пользователь **user2** домена `domain2.lan` имеет доступ к папке `ib_doc`, содержащей конфиденциальную информацию. При установлении ДО между доменами `domain1.test` и `domain2.lan` (как двусторонних, так и односторонних), пользователь **user1** получит доступ к папке `ib_doc` в домене `domain2.lan`.

Отслеживание пересечений диапазонов uid и gid выполняется силами администратора домена.

В частном случае можно вручную переопределить uid или gid при пересечении диапазонов - на примере пользователя **test**, изменить ему uid на `5555`

```
[tbabej@vm-124 labtool]$ ipa idoverrideuser-add 'Default Trust View'
↳testuser@tbad.idm.lab.eng.brq.redhat.com --uid 5555
-----
Added User ID override "testuser@tbad.idm.lab.eng.brq.redhat.com"
-----
Anchor to override: testuser@tbad.idm.lab.eng.brq.redhat.com
UID: 5555
```

Для того чтобы проверить переопределение:

```
[tbabej@vm-124 labtool]$ sudo systemctl restart sssd
[tbabej@vm-124 labtool]$ id testuser@tbad.idm.lab.eng.brq.redhat.com
uid=5555(testuser@tbad.idm.lab.eng.brq.redhat.com)
↳gid=1218201156(testuser@tbad.idm.lab.eng.brq.redhat.com)
↳groups=1218201156(testuser@tbad.idm.lab.eng.brq.redhat.com),
↳1218201425(test group@tbad.idm.lab.eng.brq.redhat.com),1218200513(domain
↳users@tbad.idm.lab.eng.brq.redhat.com)
```

Аналогичным образом переопределяется GID или другие атрибуты, см. `ipa idoverrideuser-add -help`.

Возникновение ошибки:

```
Ошибка на удаленном сервере [имя сервера]: Сущность уже существует (424
↳FailedDependency)
```

В процессе создания доверительных отношений между доверяющим и доверенным доменами может возникнуть ситуация, когда на доверенном (удаленном) домене ДО были созданы, а на доверяющем - нет. Такая ситуация может произойти в случае сетевых проблем, возникновения ошибок с кодом 500 и т.д. Для решения данной ошибки администраторы доверенного (удаленного) домена должны удалить ДО в интерфейсе портала **ALD Pro**.

4.9.1.1. Особенности работы ДО в версиях ALSE 1.7.6 и 1.7.6uu1

При настройке двустороннего отношения доверия между двумя доменами **ALD Pro** невозможно авторизоваться в доверенном домене при работе **ALD Pro** на версиях **Astra Linux 1.7.6** и **1.7.6uu1**.

Для решения проблемы необходимо добавить (вручную или создать ГП) конфигурацию в `/etc/krb5.conf` раздел `[capaths]` для доверенного домена, следующего формата:

```
[capaths]
<ЛОКАЛЬНЫЙ ДОМЕН ЗАГЛАВНЫМИ БУКВАМИ> = {
<ДОВЕРЕННЫЙ ДОМЕН ЗАГЛАВНЫМИ БУКВАМИ> = <ДОВЕРЕННЫЙ ДОМЕН ЗАГЛАВНЫМИ БУКВАМИ>
    <ДОВЕРЕННЫЙ ДОМЕН ЗАГЛАВНЫМИ БУКВАМИ> = <ЛОКАЛЬНЫЙ ДОМЕН ЗАГЛАВНЫМИ
↪БУКВАМИ>
}
```

Пример для конфигурации клиента домена `pool-19.aldpro-team.astralinux.ru`

```
[capaths]
DOMEN-01.ALDPRO.TEST.RU = {
DOMEN-02.ALDPRO.TEST.RU = DOMEN-02.ALDPRO.TEST.RU
    DOMEN-02.ALDPRO.TEST.RU = DOMEN-01.ALDPRO.TEST.RU
}
```

Конфигурации необходимо добавить на все машины в домене, включая серверы.

4.9.2. Настройка доверия между доменами ALD Pro

4.9.2.1. Групповая политика

Перед настройкой доверительных отношений, необходимо создать групповую политику, которая будет действовать на объекты, на которых происходит аутентификация пользователей другого домена (клиенты, контроллер домена).

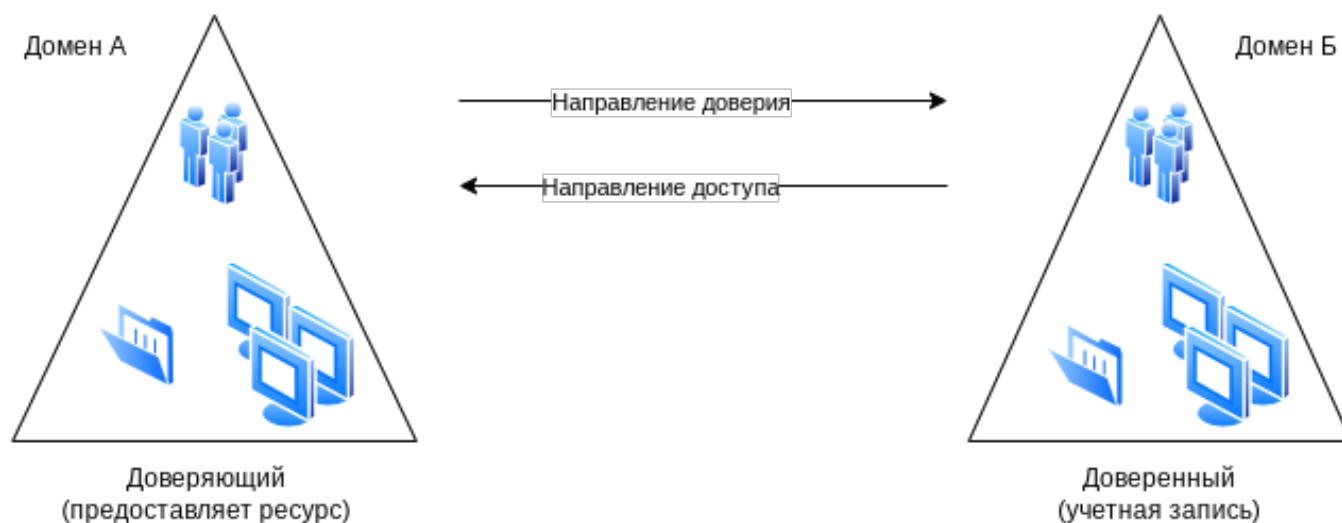
При создании групповой политики необходимо отключить FAST аутентификацию (Групповые политики -> имя групповой политики -> Параметры компьютера -> Безопасность -> FAST аутентификация).

4.9.2.2. Подключение к доменам ALD Pro

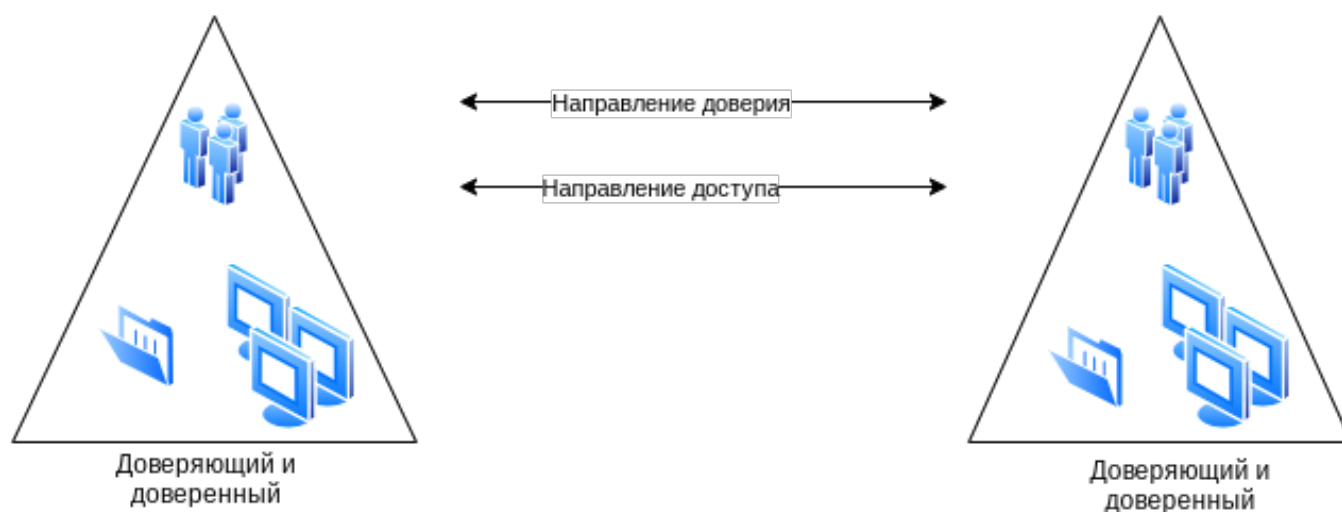
В подразделе представлены функции создания, удаления и просмотра доверительных отношений.

Создание нового подключения ALD Pro

Для создания нового подключения ALD Pro необходимо нажать на кнопку **[+ Новое подключение ALD Pro]**.



На открывшейся карточке необходимо заполнить обязательные поля **Домен, Тип доверия, Учетная запись для доверительных отношений** и **Пароль пользователя**.



Учетная запись для доверительных отношений должна принадлежать домену, с которым устанавливаются ДО и обладать одной из ролей: ALDPRO - IT Security Specialist, ALDPRO - Main Administrator.

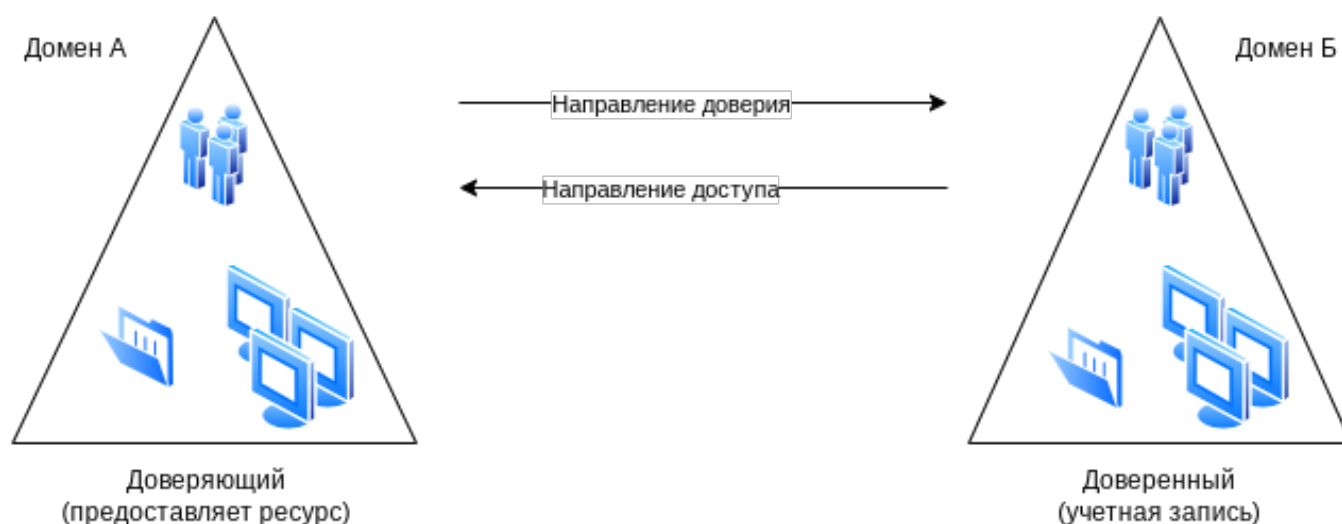
Для сохранения нового подключения ALD Pro необходимо нажать на кнопку сохранения. Будет выполнен переход к вкладке подключений доменов ALD Pro.

Для закрытия карточки создания нового подключения ALD Pro и возврата к вкладке подключений доменов ALD Pro нажать на кнопку **[Закрыть]**.

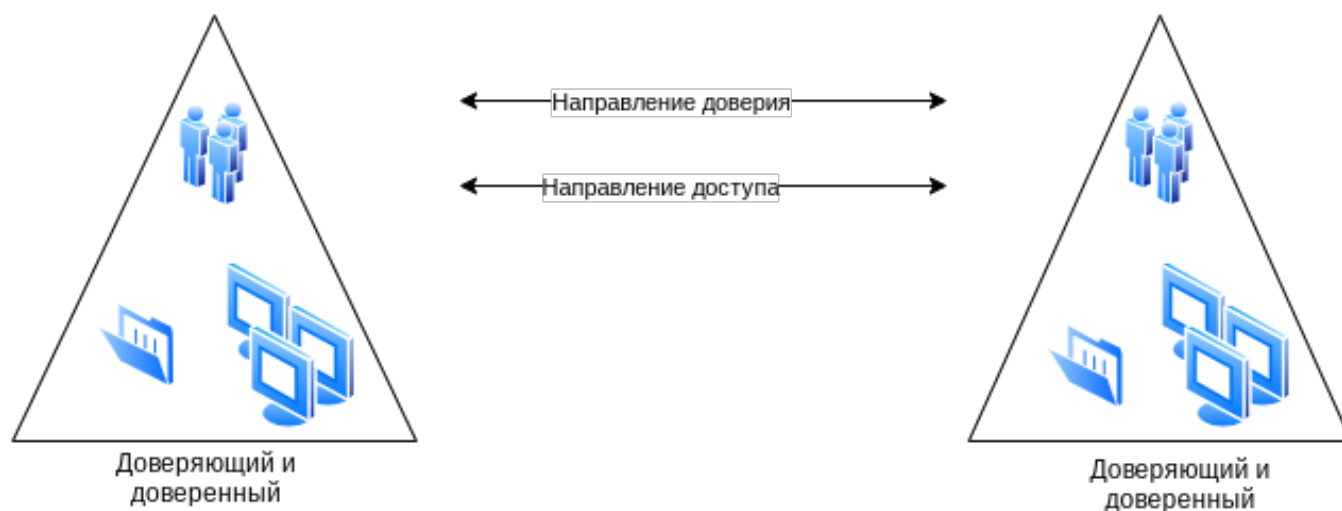
Важно: Существующие подключения между доменами ALD Pro недоступны для редактирования, так как при установке ДО логин и пароль используются единожды, в момент установки ДО. Все остальные поля доступны к просмотру в списке подключений ALD Pro.

Удаление подключения ALD Pro

Для удаления подключения ALD Pro необходимо в списке подключений ALD Pro напротив конкретного подключения нажать кнопку с иконкой корзины.



После, для подтверждения удаления подключения, необходимо ввести логин и пароль учетной записи, обладающей привилегией управления ДО для домена, с которым установлены доверительные отношения.



После подтверждения операции (нажатия кнопки **[Удалить]**) и удаления подключения ALD Pro произойдет переход к списку подключений ALD Pro. Удаление ДО на доверяющем домене так же удалит их и на стороне доверенного.

В случае выбора кнопки **[Отмена]** удаление подключения ALD Pro не будет выполнено и произойдет переход к списку подключений ALD Pro.

Дополнительные настройки файла конфигурации SSSD

После установления доверительных отношений между доменами ALD Pro для корректной обработки входа в графический интерфейс ОС необходимо внести в файл конфигурации дополнительные параметры. Изменения вносятся в файл конфигурации на каждом контроллере домена (включая все реплики), с которого выполняется запрос ресурсов доверяющих доменов. В случае двусторонних отношений изменяем файл конфигурации для обоих доменов.

На контроллере домена ALD Pro добавить раздел в файле `/etc/sss/sss.conf` в формате: `[domain/main_domain/trusted_domain]`, где `main_domain` - имя домена ALD Pro, `trusted_domain` - имя домена с которым установлены доверительные отношения. Раздел может содержать следующие параметры:

`ad_server` - имена хостов серверов домена, с которым установлены доверительные отношения, к которым может подключиться SSSD. Имена хостов перечисляются в одну строку, в порядке приоритета и разделяются запятыми.

Требования к формату записи строки параметров:

- между запятыми может быть любое количество пробелов
- переносить параметры на новую строку запрещено. в том числе запрещено использовать символ конкатенации строк \
- запрещено использовать символы шаблонов имен файлов (*, \$, и другие)

ad_backup_server (опционально) - данный список используется после того, как сервера из списка ad_server не отвечают.

Требования к формату аналогичны требованиям к ad_server.

ad_site - список сайтов, к которым клиент может подключаться.

Пример дополнительных параметров:

```
[domain/domain1.lan/domain2.test]
ad_server = dc01.domain2.test
ad_backup_server = dc01.domain2.test
ad_site = pool.domain2.test
```

После внесения изменений в файл конфигурации необходимо перезапустить службу sssd на каждом контроллере домена (включая все реплики).

4.9.2.3. Перечень ошибок, возникающих при работе с доверительными отношениями

Код	Текущий код ошибки	Текст ошибки
403	DeniedError	Отсутствуют права на выполнение данной операции
500	ProjectError	The DNS response does not contain an answer to the question
500	ProjectError	Нельзя создать/удалить доверие с самим собой
500	ProjectError	Домен для доверительных отношений не найден
500	ProjectError	NS-запись домена
500	ProjectError	Не удалось получить данные локального домена
500	ProjectError	Не удалось получить записи LDAP для контроллеров удаленного домена
500	ProjectError	Диапазон id объектов для
500	ProjectError	IP
500	ProjectError	При создании принципала
500	ProjectError	При создании принципала
500	ProjectError	При создании привилегированной УЗ
500	ProjectError	Сущность уже существует
424	FailedDependency	Ошибка на удаленном сервере [имя сервера]: Сущность уже существует
424	FailedDependency	Не удалось подключиться ни к одному доступному серверу удаленного домена
424	FailedDependency	Ошибка на удаленном сервере
424	FailedDependency	Ошибка на удаленном сервере
424	FailedDependency	Ошибка на удаленном сервере

Пользователи и компьютеры

В разделе осуществляется управление организационными единицами, учетными записями пользователей и групп пользователей, а также учетными записями компьютеров и групп компьютеров.

5.1. Организационная структура

5.1.1. Общие сведения

В подразделе осуществляется создание и управление организационной структурой подразделений домена. Также в подразделе выполняется назначение прав и ролей структурным подразделениям и управление учетными записями, входящими в состав структурного подразделения.

В подразделе в качестве корневого подразделения отображается домен. Структурные подразделения добавляются в домен в иерархическом виде.

При переходе в подраздел отображается поле поиска подразделений и контроллер домена.

Для поиска подразделения начать вводить в поле поиска название, результат поиска будет выводиться по мере ввода.

Для раскрытия структуры подразделений нажать на подразделение.

При выделении подразделения вверху страницы отобразятся кнопки управления структурой подразделений (см. [Добавление нового подразделения](#), [Редактирование подразделения](#)), а также кнопки добавления нового пользователя (см. [Пользователи](#)), новой группы пользователей (см. [Группы пользователей](#)) и новой группы компьютеров (см. [Группы компьютеров](#)) в состав подразделения.

5.1.2. Добавление нового подразделения

Для добавления нового подразделения в структуру нажать кнопку **[Подразделение]**, будет открыта карточка нового подразделения.

На карточке на вкладке **Основное** необходимо заполнить обязательные поля **Наименование подразделения**, **Родительское подразделение** и **Руководитель подразделения**. В поле **Расположение подразделения в организационной структуре** автоматически указывается полный путь выбранного структурного подразделения. В поле **Родительское подразделение** по умолчанию указывается подразделение, которое было выбрано при нажатии кнопки добавления нового подразделения. Данное значение можно изменить вручную. Также можно заполнить необязательное поле **Описание**.

Остальные вкладки для редактирования станут доступны после сохранения подразделения (см. [Редактирование подразделения](#)).

Для сохранения нового подразделения необходимо нажать на кнопку сохранения в правом верхнем углу. После сохранения подразделения будет выполнен переход к структуре подразделений.

5.1.3. Редактирование подразделения

Для редактирования подразделения необходимо выделить его в структуре и нажать кнопку **[Редактировать]** для открытия карточки подразделения.

На карточке подразделения информация приводится на вкладках:

- **Основное;**
- **Пользователи;**
- **Компьютеры;**
- **Дочерние подразделения;**
- **Групповые политики;**
- **Политики ПО.**

Для закрытия карточки подразделения и возврата к структуре подразделений нажать на кнопку закрытия.

5.1.3.1. Основное

На вкладке отображается основная информация о подразделении: наименование подразделения, родительское подразделение, руководитель подразделения, описание и расположение.

Поля **Наименование подразделения** и **Расположение подразделения в организационной структуре** не могут быть изменены, остальные поля доступны для редактирования.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

Для изменения родительского подразделения требуется наличие привилегии Organization units - Modify. Области действия активных ролей с этой привилегией должны включать:

- Подразделение, для которого выполняется изменение родительского подразделения;
- Старое родительское подразделение;
- Новое родительское подразделение.

К подразделению, над которым выполняется операция, не должны быть привязаны роли. Если к подразделению привязаны роли, для него нельзя изменить родительское подразделение. Для выполнения операции требуется отвязать от подразделения все роли, и выполнить назначение ролей после перемещения (требуется привилегия Roles - Modify)

Если требуется отвязать от подразделения роли и выполнить привязку после перемещения, то необходима привилегия Roles - Modify. Области действия активных ролей с этой привилегией должны включать подразделение, для которого выполняется изменение родительского подразделения.

5.1.3.2. Пользователи

На вкладке осуществляется управление штатным составом подразделения.

В списках **Выбранные пользователи** и **Выбранные группы** указаны пользователи и группы пользователей, входящие в состав подразделения.

В списках **Все пользователи** и **Все группы** указаны все пользователи и группы пользователей, зарегистрированные в домене.

Во всех списках доступен поиск по названию. Для этого в соответствующем поле поиска начать вводить название пользователя/группы, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для добавления пользователей в подразделение необходимо в блоке **Пользователи** в списке **Все пользователи** отметить требуемые записи и перенести их в список **Выбранные пользователи** нажатием кнопки [**<-**].

Для добавления пользователя в подразделение требуется наличие привилегии Users - Set organization unit. Области действия активных ролей с этой привилегией должны включать:

- Подразделение пользователя до выполнения операции;
- Подразделение, в которое переводится пользователь.

Если на пользователя назначены роли, исполнителю операции потребуются привилегии: Roles — Modify или Roles Membership — Manage. При наличии ролей, назначенных на пользователя: области действия активных ролей пользователя должны включать новое подразделение, в которое переводится пользователь. Пользователя нельзя добавить в подразделение, если область действия хотя бы одной из его активных ролей не включает новое подразделение. При возникновении ошибки о несоответствии областей действия роли пользователя и нового подразделения требуется выполнить одно из действий в отношении роли, вызвавшей ошибку:

- изменить привязку роли к подразделению таким образом, чтобы она включала новое подразделение (исполнитель операции должен обладать привилегией Roles - Modify), и повторить операцию добавления пользователя в подразделение;
- исключить пользователя из участников роли (исполнитель операции должен обладать привилегией Roles Membership - Manage) и повторить операцию добавления пользователя в подразделение.

Для исключения пользователей из подразделения необходимо в списке **Выбранные пользователи** отметить требуемые записи и перенести их в список **Все пользователи** нажатием кнопки [**->**].

Для удаления пользователя из подразделения требуется наличие привилегии Users - Set organization unit. Области действия активных ролей с этой привилегией должны включать:

- Подразделение пользователя до выполнения операции
- Корневое подразделение (пользователь при удалении из подразделения)

автоматически переносится в корень домена)

Если на пользователя назначены роли, исполнителю операции потребуются привилегии: Roles - Modify или Roles Membership - Manage. При наличии ролей, назначенных на пользователя: области действия активных ролей пользователя должны распространяться на корень домена. Пользователя нельзя удалить из подразделения, если область действия хотя бы одной из его активных ролей не распространяется на корень домена. При возникновении ошибки о несоответствии областей действия роли пользователя и нового подразделения требуется выполнить одно из действий в отношении роли, вызвавшей ошибку:

- изменить привязку роли к подразделению таким образом, чтобы она включала родительское подразделение (исполнитель операции должен обладать привилегией Roles - Modify), и повторить операцию удаления пользователя из подразделения;
- исключить пользователя из участников роли (исполнитель операции должен обладать привилегией Roles Membership - Manage) и повторить операцию удаления пользователя из подразделения.

При нажатии на кнопку **[Новый пользователь]** будет выполнен переход на карточку добавления нового пользователя в подразде [Пользователи](#).

Добавление/исключение группы пользователей выполняется в блоке **Группы пользователей** аналогично добавлению/исключению пользователей.

Для добавления группы пользователей в подразделение требуется наличие привилегии User groups - Set organization unit. Области действия активных ролей с этой привилегией должны включать:

- Подразделение группы до выполнения операции
- Подразделение, в которое переводится группа

Для удаление группы пользователей из подразделения требуется наличие привилегии User groups - Set organization unit. Области действия активных ролей с этой привилегией должны включать:

- Подразделение группы до выполнения операции
- Корневое подразделение (группа при удалении из подразделения автоматически переносится в корень домена)

При добавлении/удалении группы пользователей:

- Наличие ролей, назначенных на группу, не имеет значения;
- Подразделения пользователей, входящих в группу, не меняются в результате операции.

При нажатии на кнопку **[Новая группа]** будет выполнен переход на карточку создания новой группы в подразделе *Группы пользователей*.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

5.1.3.3. Компьютеры

На вкладке осуществляется управление составом компьютеров подразделения: выбор компьютеров и групп компьютеров, которые будут входить в состав данного подразделения.

В списках **Выбранные компьютеры** и **Выбранные группы** указаны компьютеры и группы компьютеров, входящие в состав подразделения.

В списках **Все компьютеры** и **Все группы** указаны все компьютеры и группы компьютеров, зарегистрированные в домене.

Список компьютеров соответствует списку в подразделе *Компьютеры*.

Во всех списках доступен поиск по названию. Для этого в соответствующем поле поиска начать вводить название компьютера/группы компьютеров, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для добавления компьютеров в подразделение необходимо в блоке **Компьютеры** в списке **Все компьютеры** отметить требуемые записи и перенести их в список **Выбранные компьютеры** нажатием кнопки **[<-]**.

Для добавления компьютера в подразделение требуется наличие привилегии Computers - Set organization unit. Области действия активных ролей с этой привилегией должны включать:

- Подразделение компьютера до выполнения операции;
- Подразделение, в которое переносится компьютер.

Для исключения компьютеров из подразделения необходимо в списке **Выбранные компьютеры** отметить требуемые записи и перенести их в список **Все компьютеры** нажатием кнопки **[->]**.

Для удаления компьютера из подразделения требуется наличие привилегии Computers - Set organization unit. Области действия активных ролей с этой привилегией должны включать:

- Подразделение компьютера до выполнения операции;
- Корневое подразделение (после удаления из подразделения компьютер автоматически переносится в корень домена).

Добавление/исключение группы компьютеров выполняется в блоке **Группы компьютеров** аналогично добавлению/исключению компьютеров.

Для добавления/удаления группы компьютеров требуется наличие привилегии Computer groups - Set organization unit. Для добавления группы компьютеров области действия активных ролей с этой привилегией должны включать:

- Подразделение группы компьютеров до выполнения операции;
- Подразделение, в которое переносится группа компьютеров.

Для удаления группы компьютеров области действия активных ролей с этой привилегией должны включать:

- Подразделение группы компьютеров до выполнения операции;
- Корневое подразделение (после удаления из подразделения группа компьютеров автоматически переносится в корень домена).

При нажатии на кнопку **[Новая группа]** будет выполнен переход на карточку создания новой группы компьютеров в подразделе *Группы компьютеров*.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

5.1.3.4. Дочерние подразделения

На вкладке приведен список дочерних подразделений выбранного подразделения.

Для списка доступен поиск по названию. Для этого в поле поиска начать вводить название подразделения, результат поиска будет выводиться по мере ввода.

Внизу списка указано количество дочерних подразделений данного подразделения.

При выборе дочернего подразделения из списка будет открыта карточка подразделения с возможностью редактирования (см. [Редактирование подразделения](#)).

При нажатии на кнопку **[Новое подразделение]** будет выполнен переход на карточку создания нового подразделения (см. [Добавление нового подразделения](#)).

5.1.3.5. Групповые политики

Список групповых политик

На вкладке приведен список групповых политик, которые были назначены на подразделение, с указанием их приоритета.

Флаг **Включить наследование** позволяет включить или отключить наследование параметров, определенных в объектах групповых политик, назначенных на родительские подразделения.

Для списка доступен поиск по названию. Для этого в поле поиска начать вводить название политики, результат поиска будет выводиться по мере ввода.

Внизу списка указано количество групповых политик, назначенных на подразделение.

Назначение групповой политики

Подразделению можно назначить групповые политики, созданные в подразделе [Групповые политики](#) (раздел [Групповые политики](#))

Назначенные групповые политики будут применяться к учетным записям пользователей, к компьютерам данного подразделения и объектам его дочерних подразделений.

Для назначения подразделению групповой политики нажать кнопку **[Добавить групповую политику]**, будет выполнен переход на карточку назначения групповой политики. На карточке необходимо из выпадающего списка **Групповая политика** выбрать групповую политику. В поле **Приоритет** задать приоритет ее применения. В поле **Расположение подразделения в организационной структуре** будет автоматически отображаться dn подразделения.

Флаг **Наследовать принудительно** делает наследование параметров выбранное ГПО

обязательным для подразделения и для всех дочерних подразделений, даже если где-то было отключено наследование. (см. инструкцию GP_sum)

Внимание: Приоритет групповой политики должен быть уникальным. Одному подразделению не может быть назначено несколько групповых политик с одинаковым приоритетом.

Для применения изменений нажать на кнопку сохранения в правом верхнем углу, будет выполнен переход к списку групповых политик.

Для закрытия карточки назначения групповой политики и возврата к списку групповых политик нажать на кнопку закрытия.

Изменение приоритета и порядка наследования назначенной групповой политики

Для изменения приоритета и порядка наследования назначенной групповой политики необходимо перейти в карточку политики, нажав на нее в списке.

Изменение приоритета определяет порядок применения групповых политик, т.е. какие настройки будут применены к объекту.

Для изменения приоритета применения групповой политики в поле **Приоритет групповой политики** задать новое значение.

Флаг **Наследовать принудительно** позволяет сделать наследование параметров соответствующего объекта обязательным для всех дочерних подразделений, даже если где-то наследование отключено. Связанные ГПО, отмеченные флагом **Принудительно**, применяются после обычных ГПО, поэтому переопределяют их значения.

Для включения принудительного наследования параметров ГПО, необходимо установить флаг **Наследовать принудительно**.

Для применения изменений нажать на кнопку сохранения в правом верхнем углу, будет выполнен переход к списку групповых политик.

Для закрытия карточки групповой политики и возврата к списку групповых политик нажать на кнопку закрытия.

Отмена назначения групповой политики

Для отмены назначения на подразделение групповой политики или одновременно нескольких групповых политик необходимо на вкладке **Групповые политики** в списке отметить требуемые групповые политики и нажать кнопку **[Удалить]**.

Также отменить назначение на подразделение групповой политики можно из ее карточки: нажать на групповую политику в списке для открытия ее карточки, затем на карточке нажать кнопку **[Удалить групповую политику]**. После подтверждения удаления будет выполнен переход к списку групповых политик.

5.1.3.6. Политики ПО

Список групповых политик

На вкладке приведен список политик ПО, которые были назначены на подразделение, с указанием их приоритета.

Для списка доступен поиск по названию. Для этого в поле поиска начать вводить название политики, результат поиска будет выводиться по мере ввода.

Внизу списка указано количество политик ПО, назначенных на подразделение.

Назначение политики ПО

Подразделению можно назначить политики ПО, созданные в подразделе [Политики ПО](#) (раздел [Установка и обновление ПО](#))

Политики ПО определяют перечень программного обеспечения, устанавливаемого на компьютеры данного подразделения и его дочерних подразделений.

Для назначения подразделению политики ПО нажать кнопку **[Назначить политику ПО]**, будет выполнен переход на карточку назначения политики. На карточке необходимо из выпадающего списка **Имя политики ПО** выбрать политику ПО и в поле **Приоритет политики ПО** задать приоритет ее применения.

Важно: Приоритет политики ПО должен быть уникальным. Одному подразделению не может быть назначено две (или более) политики ПО, которые имеют одинаковый

приоритет.

Для применения изменений нажать на кнопку сохранения в правом верхнем углу, будет выполнен переход к списку политик ПО.

Для закрытия карточки назначения политики ПО и возврата к списку политик ПО нажать на кнопку закрытия.

Изменение приоритета назначенной политики ПО

Для изменения приоритета назначенной политики ПО необходимо нажать на политику ПО в списке, затем на открывшейся карточке отредактировать поле **Приоритет политики ПО**.

Для применения изменений нажать на кнопку сохранения в правом верхнем углу, будет выполнен переход к списку политик ПО.

Для закрытия карточки политики ПО и возврата к списку политик ПО нажать на кнопку закрытия.

Отмена назначения политики ПО

Для отмены назначения на подразделение политики ПО или одновременно нескольких политик ПО необходимо на вкладке **Политики ПО** в списке отметить требуемые политики ПО и нажать кнопку **[Удалить]**.

Также отменить назначение на подразделение политики ПО можно из ее карточки: нажать на политику ПО в списке для открытия ее карточки, затем на карточке нажать кнопку **[Удалить политику ПО]**. После подтверждения удаления будет выполнен переход к списку групповых политик.

5.1.4. Удаление подразделения

Для удаления подразделения необходимо выделить его в иерархической структуре и нажать кнопку **[Редактировать]**. В открывшейся карточке подразделения нажать кнопку **[Удалить подразделение]**. После подтверждения удаления будет выполнен переход к структуре подразделений домена.

Для удаления подразделения требуется привилегия Organization Units — Delete. Области действия активных ролей с этой привилегией должны включать удаляемое подразделение.

В удаляемом подразделении должны отсутствовать объекты (пользователи, компьютеры, группы компьютеров, группы пользователей). К подразделению, над которым выполняется операция, не должны быть привязаны роли. Если к подразделению привязаны роли, его нельзя удалить.

Для удаления подразделения требуется выполнить одно из действий:

- переназначить роли на другое подразделение (требуется привилегия Roles — Modify с привязкой к подразделению, на которое выполняется перепривязка ролей);
- удалить роли, назначенные на удаляемое подразделение (требуется привилегия Roles — Delete с привязкой к удаляемому подразделению).

5.2. Пользователи

5.2.1. Список пользователей

В подразделе осуществляется управления учетными записями пользователей.

В подразделе приведен список всех учетных записей пользователей с указанием имени пользователя, имени учетной записи, подразделения, должности и состояния учетной записи.

Для списка доступен поиск по имени пользователя и логину. Для этого в поле поиска ввести значение от трех символов, результат поиска будет выводиться по мере ввода.

Внизу списка указано количество учетных записей.

5.2.2. Добавление пользователя

Для добавления нового пользователя необходимо нажать на кнопку **[+ Новый пользователь]**, будет выполнен переход на карточку нового пользователя.

На карточке на вкладке **Основное** ввести данные о пользователе и его учетной записи. Обязательные для заполнения поля отмечены соответствующим образом.

Остальные вкладки карточки пользователя станут доступны после сохранения информации (см. [Редактирование информации о пользователе](#))

Для добавления пользователя нажать на кнопку сохранения в правом верхнем углу. Будет выполнен переход к списку пользователей.

Для закрытия карточки и возврата к списку пользователей нажать на кнопку закрытия.

Важно: Учетная запись, которой не присвоен ни один системный тип администратора не имеет допуска к функциям Системы. Управление системными типами администратора осуществляется:

- из карточки типа администратора подраздел [Типы администратора в системе](#) раздела [Роли и права доступа](#);
- из карточки пользователя (вкладка “Назначенные роли”)

5.2.3. Редактирование информации о пользователе

Редактирование информации о пользователе осуществляется на его карточке. Для перехода на карточку необходимо в списке нажать на пользователя.

На карточке информация о пользователе размещается на вкладках:

- **Основное;**
- **Группы;**
- **Дополнительные сведения;**
- **Групповые политики;**
- **Расширенные настройки;**
- **Роли.**

Для закрытия карточки пользователя и возврата к списку пользователей нажать на кнопку закрытия.

Для изменения подразделения пользователя требуется наличие привилегии Users - Set organization unit. Области действия активных ролей с этой привилегией должны включать:

- Подразделение пользователя до выполнения операции;

- Подразделение, в которое переводится пользователь.

При наличии ролей, назначенных на пользователя: области действия активных ролей пользователя должны включать новое подразделение, в которое переводится пользователь.

Пользователю нельзя изменить подразделение, если область действия хотя бы одной из его активных ролей не включает новое подразделение. При возникновении ошибки о несоответствии областей действия роли пользователя и нового подразделения требуется выполнить одно из действий в отношении роли, вызвавшей ошибку:

- изменить привязку роли (исполнитель операции должен обладать привилегией Roles - Modify) и повторить операцию изменения подразделения пользователя;
- отменить назначение роли пользователю (исполнитель операции должен обладать привилегией Roles Membership - Manage) и повторить операцию изменения подразделения пользователя.

Области действия активных ролей с этими привилегиями также должны включать:

- Подразделение пользователя до выполнения операции;
- Подразделение, в которое переводится пользователь.

5.2.3.1. Основное

Информация о пользователе

На вкладке приведена информация о пользователе и о его учетной записи. Не доступно для редактирования имя учетной записи (логин) и дата окончания действия пароля, остальные поля доступны для изменения.

Информация о пользователе размещается в соответствующих блоках:

- **Персональные данные** — имя пользователя и его фотография;
- **Учетная запись** — имя и идентификатор учетной записи, сброса пароля и управление состоянием учетной записи;
- **Организационные данные** — подразделение и должность пользователя, а также его руководитель;
- **Контактная информация** — адрес электронной почты и телефон пользователя;
- **Расположение** — адрес пользователя;

- **Сертификаты пользователя** — управление сертификатами пользователя;
- **Открытые ключи SSH** — управление открытыми ключами пользователя.

Для применения внесенных изменений нажать на кнопку сохранения в правом верхнем углу.

Сброс пароля пользователя

На карточке пользователя на вкладке **Основное** задать новый пароль в полях **Пароль** и **Подтверждение пароля** и нажать кнопку **[Сбросить пароль]**.

Управление сертификатами пользователя

Для добавления сертификата необходимо ввести его в поле **Сертификат в формате base64 или PEM** и нажать на кнопку **[Добавить]**.

Для пользователя можно добавить несколько сертификатов. Для добавление второго и последующих сертификатов необходимо в пустом поле **Сертификат в формате base64 или PEM** ввести новый сертификат и нажать на кнопку **[Добавить еще]**.

Для удаления сертификата нажать кнопку **[Удалить]** рядом с соответствующим сертификатом.

Управление открытыми ключами пользователя

Для добавления открытого ключа SSH необходимо ввести его в поле **Ключ в формате SSH** и нажать на кнопку **[Добавить]**.

Для пользователя можно добавить несколько открытых ключей SSH. Для добавление второго и последующих открытых ключей необходимо в пустом поле **Ключ в формате SSH** ввести новый открытый ключ SSH и нажать на кнопку **[Добавить еще]**.

Для удаления открытого ключа SSH нажать кнопку **[Удалить]** рядом с соответствующим ключом.

5.2.3.2. Группы

На вкладке задаются группы пользователей, в которых будет состоять учетная запись пользователя.

В блоке **Состоит в группах** в списке **Выбранные группы** указаны группы пользователей, в которых состоит данная учетная запись. В списке **Все группы** указаны все группы пользователей домена.

Во всех списках доступен поиск по названию. Для этого в соответствующем поле поиска начать вводить название группы, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для включения пользователя в состав группы необходимо в списке **Все группы** отметить группы, в состав которых требуется включить пользователя, и перенести их в список **Выбранные группы** нажатием кнопки [**<-**].

Для добавление пользователя в группу требуется наличие привилегии User groups - Set group membership. Области действия активных ролей с этой привилегией должны включать:

- Подразделение пользователя;
- Подразделение группы, в которую добавляется пользователь.

Если на группу назначены роли, исполнителю операции потребуются привилегия Roles Membership - Manage. Области действия активных ролей с этой привилегией должны включать:

- Подразделение пользователя;
- Подразделения всех ролей, назначенных на группу.

При добавлении в группу пользователь наследует все роли, назначенные на группу.

Для исключения пользователя из состава групп необходимо в списке **Выбранные группы** отметить требуемые записи и перенести их в список **Все группы** нажатием кнопки [**->**].

Для удаления пользователя из группы требуется наличие привилегии User groups - Set group membership. Области действия активных ролей с этой привилегией должны включать:

- Подразделение пользователя;

- Подразделение группы, из которой исключается пользователь.

Если на группу, из которой удаляется пользователь, назначены роли, исполнителю операции потребуется привилегия Roles Membership - Manage. Области действия активных ролей с этой привилегией должны включать:

- Подразделение пользователя;
- Подразделения всех ролей, назначенных на группу.

При исключении из группы пользователь лишается ролей, унаследованных от группы (требуется привилегия Roles Membership - Manage с привязкой к подразделению пользователя)

При нажатии на кнопку **[Новая группа]** будет выполнен переход на карточку создания новой группы в подразделе *Группы пользователей*.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

В блоке **Состоит в группах** **непрямое наследование** приведен список всех групп, которые входят в состав групп, в которые включена просматриваемая группа.

5.2.3.3. Дополнительные сведения

На вкладке приводятся дополнительные сведения о пользователе. Поля дополнительных сведений настраиваются на вкладке **Атрибуты пользователей** в подразделе *Пользователи и группы* (раздел *Управление доменом*)

Все поля на вкладке доступны для редактирования.

Для сохранения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

5.2.3.4. Групповые политики

На левой вкладке приводится список назначенных параметров групповых политик, которые могут быть применены к данному пользователю. Групповые политики назначаются на подразделение в подразделе *Групповые политики* (раздел *Групповые политики*) или на вкладке **Групповые политики** карточки подразделения в подразделе *Организационная структура* (раздел *Пользователи и компьютеры*).

Внимание: Данный список представляет собой моделирование результатов применения групповых политик. Это значит, что не все политики из данного списка могут быть применены к конкретному пользователю и не все параметры могут быть отображены в данном списке. Чтобы групповая политика применилась к пользователю, необходимо соблюдать требования к операционной системе и заполнять значения атрибутов.

Внизу списка указано количество параметров групповых политик, применяемых к данному пользователю.

Настройки параметра выводятся в правой панели **Настройка параметра <имя параметра>**. Здесь отображается общая информация о параметре: объект групповой политики, подразделение, расположение подразделения в организационной структуре, требования к ОС и настройки атрибутов.

5.2.3.5. Расширенные настройки

Заполнение информации на вкладке формирует псевдонимы почтового ящика пользователя: основной адрес почты и дополнительные адреса (proxyAddresses).

Данные атрибуты используются для взаимодействия с почтовым сервисом.

Для заполнения информации о дополнительных адресах (proxyAddresses) необходимо заполнить поле **Основной адрес**. Данное поле заполняется в SMTP формате:
SMTP:<регистрационное имя>@<домен получателя>

Пример

SMTP:a.ivanov@ald.pro

Для добавления дополнительных адресов необходимо перейти в блок **Дополнительные адреса (proxyAddresses)** и заполнить поле **Адрес**. Данное поле доступно для заполнения в одном из следующих форматов:

- для формата smtp: smtp:<регистрационное имя>@<домен получателя>

Пример

smtp:alex_ivanov@ald.pro

- для формата x500: x500:/o=<имя организации>/ou=<имя сайта>/cn=Recipients/cn=<псевдоним>

Пример

x500:/o=ALDPro/ou=Департамент разработки/cn=Recipients/cn=a.ivanov

- Для формата sip:

1) sip:<имя пользователя>@<имя домена>

Пример

sip:a.ivanov@ald.pro

2) sip:<регистрационное имя>@<имя хоста>

Пример

sip:a.ivanov@client01.aldpro

3) sip:<регистрационное имя>@<IP-адрес хоста>

Пример

sip:a.ivanov@10.11.1.8

4) sip:<№ телефона пользователя>@<имя шлюза>

Пример

sip:+74952232343@192.168.31.254

После заполнения поля необходимо нажать на кнопку **[Добавить]**. Для сохранения внесенных изменений нажать на кнопку сохранения в правом верхнем углу.

5.2.3.6. Типы администратора

На вкладке задаются типы администратора, которыми будет наделена учетная запись пользователя, и отображаются наследуемые типы.

В блоке **Содержит роли** в списке **Выбранные роли** указаны типы администратора, которыми будет наделена учетная запись пользователя. В списке **Все роли** указаны все типы администратора в системе. В списке **Все роли** отображаются не только

предустановленные роли, но и те, которые создали сами пользователи.

Во всех списках доступен поиск по названию. Для этого в соответствующем поле поиска начать вводить название типа администратора, результат поиска будет выводиться по мере ввода.

Во всех списках доступна фильтрация по значению поля **Состояние**. Для этого необходимо кликнуть на значок фильтрации и выбрать значение, по которому список будет отфильтрован.

Внизу каждого списка указано количество записей в данном списке.

Для наделения пользователей возможностями соответствующего типа администратора необходимо в списке **Все роли** отметить типы, которыми требуется наделить пользователя, и перенести их в список **Выбранные роли** нажатием кнопки [**<-**].

Для исключения пользователей из списка обладателей соответствующего типа администратора необходимо в списке **Выбранные роли** отметить требуемые записи и перенести их в список **Все роли** нажатием кнопки [**->**].

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

В блоке **Наследует роли** указаны типы администратора, которые наследуются учетной записью пользователя.

В списке доступен поиск по названию. Для этого в соответствующем поле поиска начать вводить название типа администратора, результат поиска будет выводиться по мере ввода.

В списке доступна фильтрация по значению поля **Состояние**. Для этого необходимо кликнуть на значок фильтрации и выбрать значение, по которому список будет отфильтрован.

Внизу списка указано количество записей в данном списке.

Управление типами администратора также осуществляется в подразделе [Роли и права доступа](#) раздела [Управление доменом](#)

5.2.4. Блокировка и разблокировка пользователя

Пользователя или одновременно нескольких пользователей возможно заблокировать или разблокировать. Для этого необходимо в списке отметить пользователя и нажать,

соответственно, кнопку **[Заблокировать]** или **[Разблокировать]**.

Для снятия отметки с пользователя можно нажать кнопку закрытия в правом верхнем углу.

Также заблокировать или разблокировать пользователя можно из его карточки: открыть карточку нажатием на пользователя в списке, затем на карточке на вкладке **Основное** нажать, соответственно, кнопку **[Заблокировать УЗ]** или **[Разблокировать УЗ]**.

Для блокировки/разблокировки учетной записи пользователя требуется наличие привилегий: Users Block - Manage или Users - Modify. Области действия активных ролей с этой привилегией должны включать подразделение пользователя.

Если на заблокированного пользователя назначены роли, он полностью теряет делегированные ему права на время блокировки.

Разблокированный пользователь имеет доступ, полностью соответствующий привилегиям в составе его ролей.

Для закрытия карточки пользователя и возврата к списку нажать на кнопку закрытия.

5.2.5. Удаление пользователя

Пользователя или одновременно нескольких пользователей можно удалить. Для этого необходимо отметить пользователя в списке и нажать кнопку **[Удалить]**.

Для снятия отметки с пользователя можно нажать кнопку закрытия в правом верхнем углу.

Также удалить пользователя можно из его карточки: открыть карточку нажатием на пользователя в списке, затем на карточке на вкладке **Основное** нажать кнопку **[Удалить учетную запись]**. После подтверждения удаления учетная запись будет перенесена в *Корзину* и будет выполнен переход к списку пользователей.

Для переноса пользователя в Корзину требуется привилегия Users - Move to trash. Области действия активных ролей с этой привилегией должны включать подразделение пользователя.

Пользователь, перенесенный в Корзину, теряет доступ, соответствующий назначенным ему ролям.

5.3. Группы пользователей

В подразделе осуществляется управление группами пользователей.

5.3.1. Список групп пользователей

В подразделе приведен список групп пользователей домена с указанием названия группы, подразделения, в которое входит группа, и описания группы.

Если группа входит в состав другой группы и напрямую (прямое наследование), и как участник другой группы (непрямое наследование), то отражается только прямое участие группы (**Состоит в группах**), а участие в составе другой группы (**Состоит в группах не прямое наследование**) не отражается.

Группа пользователей может входить в состав только одного подразделения, при этом в состав одного подразделения может входить несколько групп пользователей.

Для списка доступен поиск. Для этого в поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Внизу списка указано количество групп в домене.

5.3.2. Добавление новой группы

Для добавления новой группы нажать кнопку **[Новая группа]**, будет выполнен переход на карточку новой группы пользователей.

На карточке на вкладке **Основное** заполнить обязательные поля **Название группы** и **Подразделение**. В поле **Расположение подразделения в организационной структуре** автоматически указывается полный путь выбранного структурного подразделения. Также можно заполнить поле **Описание**.

Остальные вкладки станут доступны после сохранения группы пользователей (см. [Редактирование информации о группе пользователей](#)).

Для сохранения группы пользователей нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку групп пользователей нажать на кнопку закрытия.

Для добавление родительской группы пользователей (состоит в группах) требуется наличие привилегии User groups - Set group membership. Области действия активных ролей с этой привилегией должны включать:

- Подразделение группы, для которой выполняется добавление родительской;
- Подразделение группы, которая добавляется в качестве родительской.

Если на родительскую группу назначены роли, исполнителю операции потребуются привилегия Roles Membership - Manage. При наличии активных ролей, назначенных на группу, которая добавляется в качестве родительской группы: подразделения всех без исключения пользователей дочерней группы должны попадать в области действия всех ролей, назначенных на родительскую группу.

После операции:

- дочерняя группа наследует роли, назначенные на родительскую группу;
- все пользователи в составе дочерней группы наследуют роли, назначенные на родительскую группу.

При добавление дочерней группы пользователей (содержит группы) требуется наличие привилегии User groups - Set group membership. Области действия активных ролей с этой привилегией должны включать:

- Подразделение группы, в которую выполняется добавление дочерней группы;
- Подразделение группы, которая добавляется в качестве дочерней.

Если на родительскую группу назначены роли, исполнителю операции потребуются привилегия Roles Membership - Manage. При наличии активных ролей, назначенных на группу, в которую выполняется добавление дочерней группы: подразделения всех без исключения пользователей дочерней группы должны попадать в области действия всех ролей, назначенных на родительскую группу.

После операции:

- дочерняя группа наследует роли, назначенные на родительскую группу;
- все пользователи в составе дочерней группы наследуют роли, назначенные на родительскую группу.

5.3.3. Редактирование информации о группе пользователей

Редактирование информации о группе пользователей осуществляется на ее карточке. Для перехода на карточку необходимо нажать на группу пользователей в списке.

На карточке информация о группе пользователей размещается на вкладках:

- **Основное;**
- **Пользователи;**
- **Группы;**
- **Роли.**

Для закрытия карточки группы пользователей и возврата к списку групп нажать на кнопку закрытия.

5.3.3.1. Основное

На вкладке приведена информация о группе пользователей, а также указывается UID группы, присвоенный автоматически при создании группы.

На вкладке можно изменить подразделение, в которое будет входить группа пользователей, и описание группы.

Для изменения подразделения группы пользователей требуется наличие привилегии User groups - Set organization unit. Области действия активных ролей с этой привилегией должны включать:

- Подразделение группы до выполнения операции;
- Подразделение, в которое переводится группа.

Наличие ролей, назначенных на группу, не имеет значения.

Для применения внесенных изменений нажать на кнопку сохранения в правом верхнем углу.

5.3.3.2. Пользователи

На вкладке в списке **Выбранные пользователи** приведен список пользователей, включенных в состав данной группы. В списке **Все пользователи** приведен список всех

пользователей домена.

Во всех списках доступен поиск по имени пользователя и по должности. Для этого в соответствующем поле поиска начать вводить имя/должность, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для добавления пользователей в группу необходимо в списке **Все пользователи** отметить требуемые записи и перенести их в список **Выбранные пользователи** нажатием кнопки [**<-**].

Для добавления пользователя в группу требуется наличие привилегии User groups - Set group membership. Области действия активных ролей с этой привилегией должны включать:

- Подразделение пользователя;
- Подразделение группы, в которую добавляется пользователь.

Если на группу назначены роли, исполнителю операции потребуются привилегия Roles Membership - Manage. Области действия активных ролей с этой привилегией должны включать:

- Подразделение пользователя;
- Подразделения всех ролей, назначенных на группу.

При добавлении в группу пользователь наследует все роли, назначенные на группу.

Для исключения пользователей из группы необходимо в списке **Выбранные пользователи** отметить требуемые записи и перенести их в список **Все пользователи** нажатием кнопки [**->**].

Для удаления пользователя из группы требуется наличие привилегии User groups - Set group membership. Области действия активных ролей с этой привилегией должны включать:

- Подразделение пользователя;
- Подразделение группы, из которой исключается пользователь.

Если на группу назначены роли, исполнителю операции дополнительно требуется привилегия Roles Membership - Manage. Области действия активных ролей с этой привилегией должны включать:

- Подразделение пользователя;
- Подразделения всех ролей, назначенных на группу.

После исключения из группы пользователь лишается ролей, унаследованных им от группы.

При нажатии на кнопку **[Новый пользователь]** будет выполнен переход на карточку добавления нового пользователя в подразделе *Пользователи*.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

5.3.3.3. Группы

В разделе **Содержит группы** на вкладке в списке **Выбранные группы** приведен список групп, включенных в состав данной группы (прямое наследование). В списке **Все группы** приведен список всех групп пользователей домена.

Внимание: Использование циклических (замнутых) наследований групп пользователей может привести к нежелательному поведению системы в различных ее частях. Не рекомендуется использовать данную архитектуру групп.

Во всех списках доступен поиск по названию группы. Для этого в соответствующем поле поиска начать вводить название группы, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для включения групп пользователей в состав данной группы необходимо в списке **Все группы** отметить группы пользователей и перенести их в список **Выбранные группы** нажатием кнопки **[<-]**. При этом все пользователи из добавляемых групп будут добавлены в список **Выбранные пользователи** на вкладке *Пользователи*.

Для добавления группы пользователей в данную группу требуется наличие привилегии User groups - Set group membership. Области действия активных ролей с этой привилегией должны включать:

- Подразделение данной группы;
- Подразделение группы пользователей, которая добавляется в качестве дочерней.

При наличии активных ролей, назначенных на группу, в которую выполняется добавление

дочерней группы, исполнителю операции требуется дополнительная привилегия Roles Membership — Manage. Области действия активных ролей с этой привилегией должны включать:

- Подразделения всех ролей, назначенных на родительскую группу
- Подразделения всех пользователей из дочерней группы

Также подразделения всех без исключения пользователей дочерней группы должны попадать в области действия всех ролей, назначенных на родительскую группу. По результатам операции:

- Дочерняя группа наследует роли, назначенные на родительскую группу;
- Все пользователи в составе дочерней группы наследуют роли, назначенные на родительскую группу.

Для исключения групп пользователей из состава данной группы необходимо в списке **Выбранные группы** отметить требуемые записи и перенести их в список **Все группы** нажатием кнопки [->]. При этом все пользователи из исключаемых групп будут исключены из списка **Выбранные пользователи** на вкладке *Пользователи*.

Для удаления дочерней группы пользователей из данной группы требуется наличие привилегии User groups - Set group membership. Области действия активных ролей с этой привилегией должны включать:

- Подразделение данной группы;
- Подразделение дочерней группы пользователей, которая удаляется из данной группы.

При наличии активных ролей, назначенных на группу, из которой выполняется удаление дочерней группы, исполнителю операции требуется дополнительная привилегия Roles Membership — Manage. Области действия активных ролей с этой привилегией должны включать:

- Подразделения всех ролей, назначенных на родительскую группу;
- Подразделения всех пользователей из дочерней группы.

По результатам операции все пользователи дочерней группы теряют роли, которые наследовали от родительской группы.

Для включения данной группы пользователей в состав других групп пользователей необходимо в блоке **Состоит в группах** в списке **Все группы** отметить группы

пользователей и перенести их в список **Выбранные группы** нажатием кнопки [<-]. Для включения данной группы в состав группы пользователей (состоит в группах) требуется наличие привилегии User groups - Set group membership. Области действия активных ролей с этой привилегией должны включать:

- Подразделение данной группы;
- Подразделение группы пользователей, добавляемой в качестве родительской группы.

При наличии активных ролей, назначенных на группу, которая добавляется в качестве родительской группы, исполнителю операции требуется дополнительная привилегия Roles Membership — Manage. Области действия активных ролей с этой привилегией должны включать:

- Подразделения всех ролей, назначенных на родительскую группу;
- Подразделения всех пользователей из дочерней группы.

Также подразделения всех без исключения пользователей дочерней группы должны попадать в области действия всех ролей, назначенных на родительскую группу. По результатам операции:

- Дочерняя группа наследует роли, назначенные на родительскую группу;
- Все пользователи в составе дочерней группы наследуют роли, назначенные на родительскую группу.

Для исключения данной группы пользователей из состава группы пользователей необходимо в блоке **Состоит в группах** в списке **Выбранные группы** отметить группу пользователей и перенести ее в список **Все группы** нажатием кнопки [->]. Для удаления родительской группы для данной группы пользователей (состоит в группах) требуется наличие привилегии User groups - Set group membership. Области действия активных ролей с этой привилегией должны включать:

- Подразделение данной группы;
- Подразделение родительской группы пользователей, из которой удаляется данная группа.

При наличии активных ролей, назначенных на удаляемую родительскую группу, исполнителю операции требуется дополнительная привилегия Roles Membership — Manage. Области действия активных ролей с этой привилегией должны включать:

- Подразделения всех ролей, назначенных на родительскую группу;
- Подразделения всех пользователей из дочерней группы.

По результатам операции все пользователи дочерней группы теряют роли, которые наследовали от родительской группы.

При нажатии на кнопку **[Новая группа]** будет выполнен переход на карточку добавления новой группы (см. [Добавление новой группы](#)).

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

В разделе **Содержит группы не прямое наследование** приведен список всех групп, которые входят в состав групп, которые включены в состав просматриваемой группы.

В разделе **Состоит в группах** приведен список групп, в которых состоит просматриваемая группа.

В разделе **Состоит в группах не прямое наследование** приведен список всех групп, которые входят в состав групп, в которые включена просматриваемая группа.

5.3.3.4. Типы администратора

На вкладке задаются типы администратора, которыми будут наделены группы пользователей, и отображаются наследуемые типы.

В блоке **Содержит роли** в списке **Выбранные роли** указаны типы администратора, которыми будут наделены группы пользователей. В списке **Все роли** указаны все типы администратора в системе. В списке **Все роли** отображаются не только предустановленные роли, но и те, которые создали сами пользователи.

Во всех списках доступен поиск по названию. Для этого в соответствующем поле поиска начать вводить название типа администратора, результат поиска будет выводиться по мере ввода.

Во всех списках доступна фильтрация по значению поля **Состояние**. Для этого необходимо кликнуть на значок фильтрации и выбрать значение, по которому список будет отфильтрован.

Внизу каждого списка указано количество записей в данном списке.

Для наделения групп пользователей возможностями при администрировании соответствующему типу администратора необходимо в списке **Все роли** отметить типы, которыми требуется наделить группу пользователей, и перенести их в список **Выбранные**

роли нажатием кнопки [**<-**].

Для исключения групп пользователей из списка обладателей соответствующего типа необходимо в списке **Выбранные роли** отметить требуемые записи и перенести их в список **Все роли** нажатием кнопки [**->**].

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

В блоке **Наследует роли** указаны типы администратора, которые наследуются группами пользователей.

В списке доступен поиск по названию. Для этого в соответствующем поле поиска начать вводить название типа администратора, результат поиска будет выводиться по мере ввода.

В списке доступна фильтрация по значению поля **Состояние**. Для этого необходимо кликнуть на значок фильтрации и выбрать значение, по которому список будет отфильтрован.

Внизу списка указано количество записей в данном списке.

Управление типами администратора также осуществляется в подразделе *[Роли и права доступа](#)* раздела *[Управление доменом](#)*

5.3.4. Удаление группы пользователей

Группу пользователей или одновременно несколько групп пользователей можно удалить. Для этого необходимо отметить группу пользователей в списке и нажать кнопку **[Удалить]**.

Для снятия отметки с группы пользователей можно нажать кнопку закрытия в правом верхнем углу.

Также удалить группу пользователей можно из ее карточки: открыть карточку нажатием на группу в списке, затем на карточке на вкладке **Основное** нажать кнопку **[Удалить группу]**. После подтверждения удаления будет выполнен переход к списку групп пользователей.

5.4. Компьютеры

5.4.1. Список компьютеров

В подразделе осуществляется управления компьютерами, введенными в домен.

В подразделе приведен список компьютеров, введенных в домен, с указанием имени компьютера и его IP-адреса.

Для списка доступен поиск по имени компьютера. Для этого в поле поиска начать вводить имя, результат поиска будет выводиться по мере ввода.

Внизу списка указано количество записей в списке.

5.4.2. Добавление компьютера

Для добавления нового компьютера в домен необходимо нажать на кнопку **[Новый компьютера]**, будет выполнен переход на карточку нового компьютера.

На карточке на вкладке **Основное** необходимо указать обязательные атрибуты **Имя компьютера**, **Зона DNS**, **IP-адрес**, **Подразделение**. В поле **Расположение подразделения в организационной структуре** автоматически указывается полный путь выбранного структурного подразделения. Остальные вкладки станут доступны после сохранения компьютера (см. [Редактирование информации о компьютере](#)).

Для сохранения нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку компьютеров нажать на кнопку закрытия.

5.4.3. Редактирование информации о компьютере

Редактирование информации о компьютере осуществляется на его карточке. Для перехода на карточку необходимо нажать на компьютер в списке.

На карточке информация о компьютере размещается на вкладках:

- **Основное;**
- **Группы;**

- Групповые политики;
- Назначение ПО;
- Политики обновления;
- Удаленный доступ.

Для изменение подразделения компьютера требуется наличие привилегия Computers - Set organization unit. Области действия активных ролей с этой привилегией должны включать:

- Подразделение компьютера до выполнения операции;
- Подразделение, в которое переносится компьютер.

Для закрытия карточки компьютера и возврата к списку компьютеров нажать на кнопку закрытия.

5.4.3.1. Основное

На вкладке приведена информация о компьютере и о его местоположении.

Для редактирования не доступно имя компьютера и псевдоним учетной записи компьютера. Остальные поля возможно изменить.

Для применения внесенных изменений нажать на кнопку сохранения в правом верхнем углу.

5.4.3.2. Группы

На вкладке задаются группы компьютеров, в которые будет входить компьютер.

В блоке **Состоит в группах** в списке **Выбранные группы** указаны группы компьютеров, в которые входит данный компьютер. В списке **Все группы** указаны все группы компьютеров домена.

Во всех списках доступен поиск по названию группы. Для этого в соответствующем поле поиска начать вводить название группы, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для добавления компьютера в состав группы необходимо в списке **Все группы** отметить группы, в которые требуется добавить компьютер, и перенести их в список **Выбранные**

группы нажатием кнопки [**<-**].

Для добавления компьютера в группу требуется наличие привилегии Computer groups - Set group membership. Области действия активных ролей с этой привилегией должны включать:

- Подразделение компьютера;
- Подразделение группы, в которую добавляется компьютер.

Для исключения компьютера из состава групп необходимо в списке **Выбранные группы** отметить требуемые записи и перенести их в список **Все группы** нажатием кнопки [**->**].

Для удаление компьютера из группы требуется наличие привилегии Computer groups - Set group membership. Области действия активных ролей с этой привилегией должны включать:

- Подразделение компьютера;
- Подразделение группы, из которой исключается компьютер.

Создание новой группы компьютеров осуществляется в подразделе *Группы компьютеров*.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

В блоке **Состоит в группах непрямоe наследование** приведен список всех групп, которые входят в состав групп, в которые включена просматриваемая группа.

5.4.3.3. Групповые политики

На левой вкладке приводится список назначенных параметров групповых политик, которые могут быть применены к данному компьютеру. Групповые политики назначаются на подразделение в подразделе *Групповые политики* (раздел *Групповые политики*) или на вкладке **Групповые политики** карточки подразделения в подразделе *Организационная структура* (раздел *Пользователи и компьютеры*).

Внимание: Данный список представляет собой моделирование результатов применения групповых политик. Это значит, что не все политики из данного списка могут быть применены на конкретном компьютере и не все политики могут быть отображены в данном списке. Чтобы групповая политика применилась на компьютере,

необходимо соблюдать требования к операционной системе и заполнить значения атрибутов.

Внизу списка указано количество параметров групповых политик, применяемых к данному компьютеру.

Настройки параметра выводятся в правой панели **Настройка параметра <имя параметра>**. Здесь отображается общая информация о параметре: объект групповой политики, подразделение, расположение подразделения в организационной структуре, требования к ОС и настройки атрибутов.

5.4.3.4. Назначение ПО

На вкладке в табличном виде отображается информация о ПО, устанавливаемом на данный компьютер в соответствии с политиками ПО.

Для устанавливаемого ПО указывается статус установки, значения параметров устанавливаемого ПО, а также информация об изменении на данном компьютере параметров, заданных политикой.

Для списка доступен поиск по наименованию ПО. Для этого в поле поиска начать вводить наименование, результат поиска будет выводиться по мере ввода.

Для списка ПО доступна фильтрация по значениям столбцов **Статус установки** и **Переопределено на хосте**, для этого необходимо нажать на значок фильтра рядом с названием соответствующего столбца и отметить требуемые значения для фильтрации.

Внизу списка указано количество записей в списке.

Назначение политики ПО осуществляется на карточке политики ПО в подразделе *Политики ПО* (раздел *Установка и обновление ПО*)

5.4.3.5. Политики обновления

На вкладке в табличном виде отображается информация о политиках обновления ALD Pro, назначенных на данный компьютер: имя политики обновления и статус.

Для списка доступен поиск по наименованию политики обновления. Для этого в поле

поиска начать вводить наименование, результат поиска будет выводиться по мере ввода.

Для списка политик обновления доступна фильтрация по значению столбца **Статус**, для этого необходимо нажать на значок фильтра рядом с названием соответствующего столбца и отметить требуемые значения для фильтрации.

Внизу списка указано количество записей в списке.

Назначение политики обновления ALD Pro осуществляется на карточке политики обновления ALD Pro в подразделе *Политики обновления ALD Pro*.

5.4.3.6. Удаленный доступ

Вкладка предоставляет возможность удаленного подключения к данному компьютеру.

Для удаленного подключения к компьютеру необходимо из выпадающего списка **Активные сессии** выбрать сессию, запущенную на компьютере, в поле **Пароль** ввести пароль для выбранной сессии и затем нажать кнопку **[Подключиться]**.

После успешного подключения на вкладке будет предоставлен доступ к удаленному рабочему столу компьютера.

5.4.4. Добавление компьютера в домен

Добавление компьютера в домен ALD Pro возможно двумя способами:

- путем подготовки компьютера и установки на нем клиентской части (см. `install_ALD_client`)
- путем установки на компьютер ОС по сети с использованием портала управления ПК «ALD Pro» в соответствии с описанием подраздела *Установка ОС по сети* (раздел *Автоматизация*).

5.4.5. Удаление компьютера

Компьютер или одновременно несколько компьютеров возможно удалить. Для этого необходимо отметить компьютер в списке и нажать кнопку **[Удалить]**.

Также удалить компьютер можно из его карточки: открыть карточку нажатием на компьютер

в списке, затем на карточке нажать кнопку **[Удалить компьютер]**. После подтверждения удаления будет выполнен переход к списку компьютеров.

5.5. Группы компьютеров

В подразделе осуществляется управления группами компьютеров.

5.5.1. Список групп компьютеров

В подразделе приведен список групп компьютеров домена с указанием названия группы, подразделения, в которое входит группа, и описания группы.

Если группа входит в состав другой группы и напрямую (прямое наследование), и как участник другой группы (непрямое наследование), то отражается только прямое участие группы (**Состоит в группах**), а участие в составе другой группы (**Состоит в группах не прямое наследование**) не отражается.

Группа компьютеров может входить в состав только одного подразделения, при этом в состав одного подразделения может входить несколько групп компьютеров.

Для списка доступен поиск. Для этого в поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Внизу списка указано количество групп в домене.

5.5.2. Добавление новой группы компьютеров

Для добавления новой группы компьютеров нажать кнопку **[Новая группа]**, будет выполнен переход на карточку новой группы компьютеров.

На карточке на вкладке **Основное** заполнить обязательные поля **Имя группы компьютеров** и **Название подразделения**. В поле **Расположение подразделения в организационной структуре** автоматически указывается полный путь выбранного структурного подразделения. Также можно заполнить поле **Описание**.

Остальные вкладки станут доступны после сохранения группы компьютеров (см. [Редактирование информации о группе компьютеров](#)).

Для сохранения группы компьютеров нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку групп компьютеров нажать на кнопку закрытия.

Для добавление родительской группы компьютеров (состоит в группах) требуется наличие привилегии Computer groups - Set group membership. Области действия активных ролей с этой привилегией должны включать:

- Подразделение дочерней группы компьютеров;
- Подразделение группы компьютеров, добавляемой в качестве родительской группы.

Для добавление дочерней группы компьютеров (состоит в группах) требуется наличие привилегии Computer groups - Set group membership. Области действия активных ролей с этой привилегией должны включать:

- Подразделение родительской группы компьютеров;
- Подразделение группы компьютеров, которая добавляется в качестве дочерней.

5.5.3. Редактирование информации о группе компьютеров

Редактирование информации о группе компьютеров осуществляется на ее карточке. Для перехода на карточку необходимо нажать на группу компьютеров в списке.

На карточке информация о группе компьютеров размещается на вкладках:

- **Основное;**
- **Компьютеры;**
- **Группы;**
- **Политики обновления**

Для изменения подразделения группы компьютеров требуется наличие привилегии Computer groups - Set organization unit. Области действия активных ролей с этой привилегией должны включать:

- Подразделение группы компьютеров до выполнения операции;
- Подразделение, в которое переносится группа компьютеров.

Для закрытия карточки группы компьютеров и возврата к списку нажать на кнопку закрытия.

5.5.3.1. Основное

На вкладке приведена информация о группе компьютеров. Поле **Имя группы компьютеров** недоступно для редактирования, остальные поля можно изменить.

Для применения внесенных изменений нажать на кнопку сохранения в правом верхнем углу.

5.5.3.2. Компьютеры

На вкладке в списке **Выбранные компьютеры** приведен список компьютеров, включенных в состав данной группы. В списке **Все компьютеры** приведен список всех компьютеров домена.

Во всех списках доступен поиск по имени компьютера. Для этого в соответствующем поле поиска начать вводить имя, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для добавления компьютера в группу необходимо в списке **Все компьютеры** отметить компьютеры и перенести их в список **Выбранные компьютеры** нажатием кнопки [**<-**].

Для добавления компьютера в группу требуется наличие привилегии Computer groups - Set group membership. Области действия активных ролей с этой привилегией должны включать:

- Подразделение группы компьютеров;
- Подразделение компьютера, добавляемого в группу.

Для исключения компьютеров из состава группы необходимо в списке **Выбранные компьютеры** отметить требуемые компьютеры и перенести их в список **Все компьютеры** нажатием кнопки [**->**].

Для удаления компьютера из группы требуется наличие привилегии Computer groups - Set group membership. Области действия активных ролей с этой привилегией должны включать:

- Подразделение группы компьютеров;
- Подразделение компьютера, удаляемого из группы.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем

углу.

5.5.3.3. Группы

В разделе **Содержит группы** в списке **Выбранные группы** приведены группы компьютеров, которые включены в данную группу.

Внимание: Использование циклических (замнутых) наследований групп компьютеров может привести к нежелательному поведению системы в различных ее частях. Не рекомендуется использовать данную архитектуру групп.

В разделе **Состоит в группах** в списке **Выбранные группы** приведены группы компьютеров, в которые входит данная группа.

В каждом разделе приведен список **Все группы**, в котором указаны все группы компьютеров домена.

Во всех списках доступен поиск по названию группы. Для этого в соответствующем поле поиска ввести значение от трех символов, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для включения групп компьютеров в состав данной группы компьютеров необходимо в разделе **Содержит группы** в списке **Все группы** отметить группы компьютеров и перенести их в список **Выбранные группы** нажатием кнопки [**<-**].

Для добавления группы компьютеров в данную группу требуется наличие привилегии Computer groups - Set group membership. Области действия активных ролей с этой привилегией должны включать:

- Подразделение данной группы;
- Подразделение группы компьютеров, которая добавляется в качестве дочерней.

Для исключения групп компьютеров из состава данной группы компьютеров необходимо в разделе **Содержит группы** в списке **Выбранные группы** отметить требуемые записи и перенести их в список **Все группы** нажатием кнопки [**->**].

Для удаления группы компьютеров из данной группы требуется наличие привилегии

Computer groups - Set group membership. Области действия активных ролей с этой привилегией должны включать:

- Подразделение данной группы;
- Подразделение дочерней группы компьютеров, которая удаляется из данной группы.

Для включения данной группы компьютеров в состав других групп компьютеров необходимо в разделе **Состоит в группах** в списке **Все группы** отметить группы компьютеров и перенести их в список **Выбранные группы** нажатием кнопки [**<-**].

Для включения данной группы в состав группы компьютеров (состоит в группах) требуется наличие привилегии Computer groups - Set group membership. Области действия активных ролей с этой привилегией должны включать:

- Подразделение данной группы;
- Подразделение группы компьютеров, добавляемой в качестве родительской группы.

Для исключения данной группы компьютеров из состава группы компьютеров необходимо в разделе **Состоит в группах** в списке **Выбранные группы** отметить группу компьютеров и перенести ее в список **Все группы** нажатием кнопки [**->**].

Для удаления данной группы из состава группы компьютеров (состоит в группах) требуется наличие привилегии Computer groups - Set group membership. Области действия активных ролей с этой привилегией должны включать:

- Подразделение данной группы;
- Подразделение родительской группы компьютеров, из которой удаляется данная группа.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

В разделе **Содержит группы непрямоe наследование** приведен список всех групп, которые входят в состав групп, которые включены в состав просматриваемой группы.

В разделе **Состоит в группах** приведен список групп, в которых состоит просматриваемая группа.

В разделе **Состоит в группах непрямоe наследование** приведен список всех групп, которые входят в состав групп, в которые включена просматриваемая группа.

5.5.3.4. Политики обновления

На вкладке в табличном виде отображается информация о политиках обновления ALD Pro, назначенных на группу компьютеров: имя политики обновления и статус.

Для списка доступен поиск по наименованию политики обновления. Для этого в поле поиска начать вводить наименование, результат поиска будет выводиться по мере ввода.

Для списка политик обновления доступна фильтрация по значению столбца **Статус**, для этого необходимо нажать на значок фильтра рядом с названием соответствующего столбца и отметить требуемые значения для фильтрации.

Внизу списка указано количество записей в списке.

Назначение политики обновления ALD Pro осуществляется на карточке политики обновления ALD Pro в подразделе *Политики обновления ALD Pro*.

5.5.4. Удаление группы компьютеров

Удаление группы компьютеров осуществляется из ее карточки. Для открытия карточки нажать на группу в списке, затем на карточке нажать кнопку **[Удалить группу]**. После подтверждения удаления будет выполнен переход к списку групп компьютеров.

5.6. Корзина

В разделе осуществляется управления учетными записями пользователей, которые были перемещены в корзину.

5.6.1. Список пользователей, перемещенных в корзину

В подразделе приведен список всех учетных записей пользователей с указанием имени пользователя, имени учетной записи, даты перемещения в корзину и даты окончательного удаления.

Для списка доступен поиск по имени пользователя. Для этого в поле поиска начать вводить имя, результат поиска будет выводиться по мере ввода.

Внизу списка указано количество учетных записей.

Важно: Срок хранения удаленных учетных записей составляет 180 календарных дней. По истечению этого периода учетные записи будут удалены окончательно.

5.6.2. Восстановление пользователя из корзины

Восстановить пользователя можно из его карточки: открыть карточку нажатием на пользователя в списке, затем на карточке на вкладке **Основное** нажать кнопку **[Восстановить учетную запись]**. Далее необходимо задать новый пароль для восстанавливаемой учетной записи после чего будет выполнен переход к списку пользователей, перемещенных в корзину.

Для восстановления пользователя из Корзины требуется наличие привилегии Users - Return from trash. Области действия активных ролей с этой привилегией должны включать привязку к корневому подразделению.

Пользователь восстанавливается в корень домена. Восстановленному из Корзины пользователю автоматически не возвращаются назначенные ему ранее роли.

5.6.3. Окончательное удаление пользователя

Пользователя или одновременно нескольких пользователей можно удалить. Для этого необходимо отметить пользователя в списке и нажать кнопку **[Удалить]**.

Для снятия отметки с пользователя можно нажать кнопку закрытия в правом верхнем углу.

Также удалить пользователя можно из его карточки: открыть карточку нажатием на пользователя в списке, затем на карточке на вкладке **Основное** нажать кнопку **[Удалить учетную запись]**. После подтверждения удаления будет выполнен переход к списку пользователей, перемещенных в корзину.

Также удалить пользователя можно из его карточки: открыть карточку нажатием на пользователя в списке, затем на карточке на вкладке **Основное** нажать кнопку **[Удалить учетную запись]**. После подтверждения удаления будет выполнен переход к списку пользователей, перемещенных в корзину.

Автоматизация

В разделе представлены функции автоматизации управления рабочими станциями и серверами. Включает в себя подразделы:

6.1. Задания автоматизации

Задача автоматизации это Bash-скрипт, который портал управления может принудительно запустить на одном из включенных в домен компьютеров или группе компьютеров. Скрипт может выполнять самые разные операции на конечной машине – от установки пакетов до запуска и управления процессами в операционной системе.

Подраздел предоставляет функции запуска заданий автоматизации и сведения о запущенных заданиях.

6.1.1. Журнал заданий

6.1.1.1. Список заданий

На вкладке в табличном виде приведена информация о запущенных заданиях автоматизации с указанием даты запуска, названия задания, инициатора задания и статуса задания.

В столбце **Статус** отображается статус выполнения задания.

В списке доступен поиск по названию. Для этого в соответствующем поле поиска ввести значение. Также доступна фильтрация по дате запуска задания и статусу задания, для этого нажать на значок фильтра рядом с названием соответствующего столбца и выбрать значения для фильтрации.

При выборе задания будет отображена карточка с полной информацией о запуске задания.

В левом нижнем углу списка указано количество записей, а в правом нижнем углу кнопки переключения страниц.

Для закрытия вкладки нажать на кнопку закрытия.

6.1.1.2. Карточка задания

Для открытия карточки задания нажать на соответствующую строку в списке заданий.

На карточке задания приводится вся информация о задании.

В системе используются задания двух типов:

- кастомные задания;
- миграции.

Для закрытия карточки и возврата к списку заданий нажать на кнопку закрытия.

Основное

На вкладке отображается следующая основная информация о задании:

- **Название задания;**
- **Статус задания;**
- **Дата запуска задания;**
- **Дата завершения задания;**
- **Инициатор запуска задания;**
- **Узел;**
- **Отчет о выполнении задания;**
- **Лог ошибки исполнения.**

Параметры задания

На вкладке отображаются параметры задания и их значения, с которыми было запущено задание автоматизации.

В левом нижнем углу списка указано количество записей, а в правом нижнем углу кнопки переключения страниц.

6.1.2. Каталог заданий автоматизации

На вкладке в структурированном виде представлены задания автоматизации, созданные в подразделе *Каталог заданий автоматизации* (раздел *Управление доменом*). Для просмотра содержимого папки необходимо выбрать ее.

6.1.2.1. Выбор и просмотр задания

В каталоге доступен поиск по названию папки или задания. Для этого в соответствующем поле поиска ввести значение.

При выборе задания будет отображена форма **Задание автоматизации** в правой части вкладки, которой приведено описание задания автоматизации.

6.1.2.2. Запуск задания

Для запуска задания необходимо выбрать его в каталоге и нажать кнопку **[Запустить задание]**.

В открывшейся карточке запуска задания необходимо заполнить поле **Параметры задания автоматизации** (например, *Hello world*) и выбрать компьютеры, на которых требуется запустить задание.

Значения полей **Наименование задания автоматизации** и **Каталог заданий** заполняются автоматически (параметры заданию задаются на карточке задания в подразделе *Каталог заданий автоматизации* (раздел *Управление доменом*))

Для выбора компьютеров, на которых необходимо запустить задание, в блоке **Запустить на компьютер** в списке **Все компьютеры** отметить требуемые записи и перенести их в список **Выбранные компьютеры** нажатием кнопки **[<-]**.

Для исключения компьютеров из списка выбранных необходимо в списке **Выбранные компьютеры** отметить требуемые записи и перенести их в список **Все компьютеры** нажатием кнопки **[->]**.

Выбор группы компьютеров выполняется в блоке **Запустить на группу компьютеров** аналогично выбору компьютеров.

Выбор компьютеров подразделений выполняется в блоке **Запустить на компьютеры**

подразделения аналогично выбору компьютеров.

Во всех списках доступен поиск по названию. Для этого в соответствующем поле поиска ввести значение от трех символов, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для запуска задания необходимо нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки без запуска задания нажать на кнопку закрытия.

6.2. Установка ОС по сети

В подразделе выполняется управление серверами для установки ОС по сети, а также:

- определение перечня компьютеров для установки ОС по сети;
- выполнение установки ОС по сети и ввод компьютеров в домен;
- управление сценариями автоматической установки ОС и конфигурирования рабочей станции после установки ОС.

6.2.1. Список серверов установки ОС

В подразделе на вкладке **Серверы установки ОС** приведен список серверов установки ОС с указанием имени сервера, его IP-адреса и имени сайта.

В списке доступен поиск по названию и по IP-адресу сервера. Для этого в поле поиска ввести значение. Внизу списка указано количество записей в списке.

6.2.2. Создание сервера установки ОС

Для создания сервера установки ОС нажать кнопку **[Новый сервер]**, будет выполнен переход на карточку нового сервера.

На карточке на вкладке **Основное** заполнить обязательные поля:

- **Имя компьютера** — из перечня компьютеров, добавленных в ALD Pro выбрать компьютер, который будет выполнять функции сервера для установки ОС по сети;

- **Имя сайта** — из выпадающего списка выбрать сайт;
- **DHCP-сервер** — из списка развернутых в ALD Pro DHCP-серверов выбрать сервер для данного сервера установки ОС (поле для выбора доступно, если не отмечен пункт **Использовать внешний DHCP-сервер**).

Пункт **Использовать внешний DHCP-сервер** необходимо отметить, если планируется использовать внешний DHCP-сервер. При отмеченном пункте выбор DHCP-сервера не доступен.

Остальные вкладки станут доступны после сохранения сервера.

Для сохранения сервера необходимо нажать на кнопку сохранения. Будет выполнен переход к списку серверов.

Для закрытия карточки и возврата к списку серверов нажать на кнопку закрытия.

6.2.3. Редактирование сервера установки ОС

Редактирование сервера осуществляется на его карточке. Для перехода на карточку необходимо нажать на сервер в списке.

Для закрытия карточки сервера и возврата к списку нажать на кнопку закрытия.

6.2.3.1. Основное

На вкладке указана основная информация о сервере: имя компьютера, имя сайта и DHCP-сервер (если не установлен флаг **Использовать внешний DHCP-сервер**).

Для редактирования доступно имя сайта и DHCP-сервер см. [Создание сервера установки ОС](#).

Для применения внесенных изменений нажать на кнопку сохранения в правом верхнем углу.

6.2.3.2. Перечень компьютеров

На вкладке осуществляется управление компьютерами, на которые будет выполняться установка ОС с данного сервера.

Список компьютеров

На вкладке приведен список компьютеров, которые подключены к данному серверу, с указанием имени компьютера, его MAC-адреса, операционной системы и профиля.

В списке доступен поиск по названию и MAC-адресу компьютера. Для этого в поле поиска ввести значение.

Внизу списка указано количество записей в списке.

Добавление компьютера

Для добавления в перечень нового компьютера нажать кнопку **[+ Новый компьютер]**, будет выполнен переход на карточку нового компьютера.

На карточке заполнить обязательные поля:

- **Имя компьютера** — задать имя, которое будет использоваться для идентификации компьютера в ALD Pro;

Важно: В названии имени компьютера можно использовать только строчные латинские буквы[a-z], цифры [1-9] и дефис[-]

- **Имя сайта** — из списка выбрать имя сайта для данного добавляемого компьютера;
- **Профиль загрузки** — из выпадающего списка выбрать профиль, в соответствии с которым будет установлено и настроено программное обеспечение на добавляемом компьютере. Профили загрузок формируются на вкладке [Профили загрузок](#)
- **MAC-адрес** — указать MAC-адрес добавляемого компьютера.

Также можно заполнить поле **Модель**, указав в нем дополнительную информацию о добавляемом компьютере.

Поле **Домен** заполняется автоматически, в нем указан домен, в который будет введен добавляемый компьютер после установки на нем ОС.

Для добавления компьютера нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки без добавления компьютера нажать на кнопку закрытия.

Редактирование информации о компьютере

Редактирование информации о компьютере осуществляется на его карточке. Для перехода на карточку необходимо нажать на компьютер в списке.

На карточке приведена основная информация о компьютере. Для редактирования доступны поля **Имя сайта**, **Профиль загрузки** и **Модель** (см. [Добавление компьютера](#)).

Для применения изменений нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку компьютеров нажать на кнопку закрытия.

Удаление компьютера

Компьютер или одновременно несколько компьютеров можно удалить из перечня подключенных к серверу. Для этого необходимо отметить компьютер в списке и нажать кнопку **[Удалить]**.

Также удалить компьютер из перечня можно из его карточки: открыть карточку нажатием на компьютер в списке, затем на карточке нажать кнопку **[Удалить компьютер]**. После подтверждения удаления будет выполнен переход к списку компьютеров.

6.2.3.3. Профили загрузок

На вкладке осуществляется управление профилями установки ОС и ПО на компьютеры, подключаемые к данному серверу.

Список профилей загрузки

На вкладке приведен список профилей для установки ОС и ПО на компьютеры с указанием названия профиля.

В списке доступен поиск по названиям профиля. Для этого в поле поиска ввести значение.

Внизу списка указано количество записей в списке.

Создание профиля загрузки

Для создания нового профиля загрузки нажать кнопку **[Новый профиль]**, будет выполнен переход на карточку нового профиля.

На карточке на вкладке **Основные свойства** заполнить обязательное поле:

- **Название профиля** — отображаемое имя профиля.

После сохранения профиля станут доступны для редактирования остальные вкладки (см. [Редактирование профиля загрузки](#)).

Для сохранения профиля нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки профиля без сохранения нажать на кнопку закрытия.

Редактирование профиля загрузки

Редактирование профиля осуществляется на его карточке. Для перехода на карточку необходимо нажать на профиль в списке.

Для закрытия карточки и возврата к списку профилей нажать на кнопку закрытия.

Основные свойства

На вкладке указана основная информация о профиле загрузки - название профиля, доступное для редактирования.

Для применения внесенных изменений нажать на кнопку сохранения в правом верхнем углу.

Preseed

На вкладке **Preseed** осуществляется управление файлом конфигурации для автоматической установки ОС на клиентах ALD Pro.

На вкладке отображается актуальный текст файла конфигурации.

Пример

```

# Подключение сетевого репозитория
d-i mirror/protocol string http
d-i mirror/http/hostname string download.astralinux.ru
d-i mirror/http/directory string /astra/frozen/1.7_x86-64/1.7.3/repository-
↳base
# Установка локали и языка
d-i mirror/country string manual
d-i debian-installer/locale string ru_RU
d-i debian-installer/locale select ru_RU.UTF-8
d-i debian-installer/language string ru
d-i debian-installer/country string RU
d-i debian-installer/keymap string ru
# Выбор клавиатуры
d-i console-tools/archs select at
d-i console-keymaps-at/keymap select ru
d-i console-setup/toggle string Alt+Shift
d-i console-setup/layoutcode string ru
d-i keyboard-configuration/toggle select Alt+Shift
d-i keyboard-configuration/layoutcode string ru
d-i keyboard-configuration/xkb-keymap select ru
d-i languagechooser/language-name select Russian
d-i countrychooser/country-name select Russia
# Автоматический выбор сетевого интерфейса
d-i netcfg/choose_interface select auto
# Подключение non-free, contrib компонентов в репозитории
d-i apt-setup/non-free boolean true
d-i apt-setup/contrib boolean true
d-i apt-setup/services-select none
# Установка часового пояса UTC
d-i clock-setup/utc boolean true
# Временная зона
d-i time/zone string Europe/Moscow
# Не обновлять время
d-i clock-setup/ntp boolean false
# Автоматическая разметка дисков
d-i partman-base partman/default_filesystem string ext4
d-i partman-auto/init_automatically_partition \
select Авто - использовать весь диск
d-i partman-auto/method string regular
d-i partman-auto/purge_lvm_from_device boolean true

```

(продолжение на следующей странице)


```

d-i partman-lvm/confirm boolean true
# Разметка для режима bios
#d-i partman-auto/choose_recipe select atomic
# для UEFI режима:
#d-i partman-auto/choose_recipe select /lib/partman/recipes-amd64-efi/
↪30atomic
# Не задавать вопросов при разметке
d-i partman/confirm_write_new_label boolean true
d-i partman/choose_partition select finish
d-i partman/confirm boolean true
d-i partman-auto-crypto/erase_disks boolean true
d-i partman-basicfilesystems/no_swap boolean false
d-i partman-target/mount_failed boolean true
d-i partman-partitioning/unknown_label boolean true
d-i partman-auto/purge_lvm_from_device string true
d-i partman-lvm/vgdelete_confirm boolean true
d-i partman/confirm_write_new_label string true
d-i partman-lvm/confirm boolean true
d-i partman/confirm_nooverwrite boolean true
d-i anna/no_kernel_modules boolean true
d-i base-installer/kernel/image string linux-image-generic
# Создание пользователя при установке
d-i passwd/make-user boolean true
# Имя пользователя
d-i passwd/user-fullname string astra
d-i passwd/username string astra
# Пароль пользователя
d-i passwd/user-password password 12345678
d-i passwd/user-password-again password 12345678
d-i debian-installer/allow_unauthenticated string true
# Выбор рабочего стола Fly
tasksel tasksel/first multiselect Fly, Fly-ssh
tasksel tasksel/astra-feat-setup multiselect
# Дополнительные пакеты
# Специфические настройки Астры
d-i astra-additional-setup/os-check select Base security level 0rel
d-i astra-additional-setup/additional-settings-0rel multiselect
astra-additional-setup astra-additional-setup/automatic-network-disable
↪multiselect

```

```

d-i astra-additional-setup/automatic-network-disable multiselect
d-i desktop-tablet-mode-switch/tablet-mode multiselect
popularity-contest popularity-contest/participate boolean false
# В GRUB будет только 1 операционная система
d-i grub-installer/only_debian boolean true
# Установка в mbr
d-i grub-installer/with_other_os boolean true
# Установка пароля Grub
d-i grub-installer/password password 12345678
d-i grub-installer/password-again password 12345678
grub-installer grub-installer/password-mismatch error
# Не показывать диалог окончания установки
d-i finish-install/reboot_in_progress note
d-i finish-install/exit/poweroff boolean true
# Команды, выполняемые после установки ОС
d-i preseed/late_command string in-target systemctl enable ssh; \
    in-target bash -c "echo -e \"astra:astra\" | chpasswd"; \
    in-target bash -c "apt-get -y purge linux-image-*-hardened"; \
    in-target bash -c "apt-get -y autoremove --purge"; \
    in-target bash -c "sed -i 's/deb-src/#deb-src/g' /etc/apt/sources.list"; \
    in-target bash -c "/usr/bin/wget -O /tmp/postinstall.sh http://192.168.17.
5/tftp/{PROFILE_UNIQ_NAME}/{POSTINSTALL_FILE_NAME}"; \
    in-target bash -c "/bin/sh -x /tmp/postinstall.sh"; \
    echo

```

Важно: Репозиторий `/astra/frozen/1.7_x86-64/1.7.3/repository-base` - это стандартный репозиторий Astra Linux, использованный в качестве примера. Для установки ОС по сети необходимо вместо базового репозитория указать репозиторий установочного диска.

Добавить или изменить файл конфигурации можно двумя способами:

- добавить текст из файла на компьютере;
- вручную ввести или изменить текст файла конфигурации на вкладке.

Для добавления текста конфигурации из файла необходимо нажать кнопку **[Загрузить из файла]**, в окне навигации выбрать на компьютере необходимый файл в формате *.cfg и

нажать **[Открыть]**.

Содержимое файла отобразится в форме **Редактировать скрипт вручную**, при этом предыдущее содержимое файла конфигурации будет заменено. При необходимости добавленный текст можно отредактировать.

Для сохранения файла конфигурации необходимо ввести комментарий и нажать кнопку сохранения. Для отмены внесения изменений в файл конфигурации нажать кнопку **[Отменить]**.

Для добавления или редактирования файла конфигурации вручную необходимо нажать на кнопку **[Редактировать файл]**, после чего форма **Редактировать скрипт вручную** станет доступна для редактирования.

Для сохранения файла конфигурации необходимо ввести комментарий и нажать кнопку сохранения. Для отмены внесения изменений в файл конфигурации нажать кнопку **[Отменить]**.

Для просмотра истории изменений файла конфигурации необходимо нажать на кнопку **[История изменений]**. Откроется карточка с отображением списка изменений с указанием даты изменения, автора изменения и комментария. В списке доступен поиск, для этого в верхнем левом углу вкладки в поле поиска ввести значение. В левом нижнем углу указано количество записей, а в правом нижнем углу кнопки переключения страниц.

Postinstall

На вкладке **Postinstall** осуществляется управление скриптом настройки ОС после ее установки на клиентах ALD Pro.

На вкладке отображается актуальный текст скрипта.

Пример

```
#!/bin/bash
set -x

sudo systemctl enable ssh
#Добавление репозитория Astra Linux
cat <<EOL > /etc/apt/sources.list
deb http://download.astralinux.ru/astra/frozen/1.7_x86-64/1.7.3/repository-
```

(продолжение на следующей странице)

```

↪base 1.7_x86-64 main non-free contrib
deb http://download.astralinux.ru/astra/frozen/1.7_x86-64/1.7.3/repository-
↪extended 1.7_x86-64 main contrib non-free
EOL
#Добавление репозитория ALD Pro
cat <<EOL > /etc/apt/sources.list.d/aldpro.list
deb http://download.astralinux.ru/aldpro/stable/repository-main/ 1.4.0 main
deb http://download.astralinux.ru/aldpro/stable/repository-extended/ generic
↪main
EOL
#Установка приоритетов репозитория
cat <<EOL > /etc/apt/preferences.d/aldpro
Package: *
Pin: release n=generic
Pin-Priority: 900
EOL
# Скачать скрипт первого запуска
# Необходимо заменить IP адрес на ваш сервер ОС
wget http://192.168.17.5/tftp/{PROFILE_UNIQ_NAME}/{FIRSTSTART_FILE_NAME} -O /
↪usr/bin/firststart.sh
# Подготовка сервиса первого запуска ОС
cat <<EOL > /etc/systemd/system/firststart.service
[Unit]
Wants=network-online.target
After=network-online.target

[Service]
Type=oneshot
RemainAfterExit=yes
ExecStart=/usr/bin/firststart.sh start

[Install]
WantedBy=multi-user.target
EOL
# Запуск сервиса
chmod 774 /usr/bin/firststart.sh
systemctl enable firststart || true

```

Добавить или изменить скрипт можно двумя способами:

- добавить текст скрипта из файла на компьютере;
- вручную ввести или изменить текст скрипта на вкладке.

Для добавления текста скрипта из файла необходимо нажать кнопку **[Загрузить из файла]**, в окне навигации выбрать на компьютере необходимый файл в формате *.sh и нажать **[Открыть]**.

Содержимое файла отобразится в форме **Редактировать скрипт вручную**, при этом предыдущее содержимое скрипта будет заменено. При необходимости добавленный текст скрипта можно отредактировать.

Для сохранения изменений в скрипте необходимо ввести комментарий и нажать кнопку сохранения. Для отмены внесения изменений в скрипт нажать кнопку **[Отменить]**.

Для добавления или редактирования скрипта вручную необходимо нажать кнопку **[Редактировать файл]**, после чего форма **Редактировать скрипт вручную** станет доступна для редактирования.

Для сохранения изменений в скрипте необходимо ввести комментарий и нажать кнопку сохранения. Для отмены внесения изменений в скрипт нажать кнопку **[Отменить]**.

Для просмотра истории изменений скрипта необходимо нажать кнопку **[История изменений]**. Откроется карточка с отображением списка изменений с указанием даты изменения, автора изменения и комментария. В списке доступен поиск, для этого в верхнем левом углу вкладки в поле поиска ввести значение. В левом нижнем углу указано количество записей, а в правом нижнем углу кнопки переключения страниц.

Первый запуск

На вкладке **Первый запуск** осуществляется управление скриптом конфигурирования клиента ALD Pro при первом запуске ОС после ее установки и настройки.

На вкладке отображается актуальный текст скрипта.

Пример

```
#!/bin/bash
set -x
# Установка клиента ALD Pro и ввод компьютера в домен
case $1 in
```

(продолжение на следующей странице)

```

start)
    apt-get update
    export DEBIAN_FRONTEND=noninteractive
    apt-get install -yq aldpro-client wget
    mkdir -p /etc/ssl/freeipa
    wget -O /root/token http://192.168.17.5/tftp/tokens/$(hostname -f).
↪pwd # Указать IP адрес вашего сервера установки ОС
    ipa-client-install --hostname=$(hostname -f) --domain=$(hostname -d) -
↪-mkhomedir --password=$(cat /root/token) -U
    rm -f /etc/aldpro-salt/minion_id
    /usr/bin/python3 /opt/rbta/aldpro/client/bin/aldpro-service-discovery.
↪py single
    systemctl restart aldpro-salt-minion
    ln -s /usr/bin/astra-freeipa-domains-ctl /etc/domains.list.d/
    sed -e "s/^astra-admin.*/&,admin,admin@$(hostname -d)/" -i /etc/
↪group 2>/dev/null >/dev/null
    systemctl disable firststart
    reboot
    ;;
stop)
    systemctl disable firststart
    ;;
*)
    echo "$Usage: $0 {start|stop}"
    ;;
esac

```

Добавить или изменить скрипт можно двумя способами:

- добавить текст скрипта из файла на компьютере;
- вручную ввести или изменить текст скрипта на вкладке.

Для добавления текста скрипта из файла необходимо нажать кнопку **[Загрузить из файла]**, в окне навигации выбрать на компьютере необходимый файл в формате *.sh и нажать **[Открыть]**.

Содержимое файла отобразится в форме **Редактировать скрипт вручную**, при этом предыдущее содержимое скрипта будет заменено. При необходимости добавленный текст скрипта можно отредактировать.

Для сохранения изменений в скрипте необходимо ввести комментарий и нажать кнопку сохранения. Для отмены внесения изменений в скрипт нажать кнопку **[Отменить]**.

Для добавления или редактирования скрипта вручную необходимо нажать кнопку **[Редактировать файл]**, после чего форма **Редактировать скрипт вручную** станет доступна для редактирования.

Для сохранения изменений в скрипте необходимо ввести комментарий и нажать кнопку сохранения. Для отмены внесения изменений в скрипт нажать кнопку **[Отменить]**.

Для просмотра истории изменений скрипта необходимо нажать кнопку **[История изменений]**. Откроется карточка с отображением списка изменений с указанием даты изменения, автора изменения и комментария. В списке доступен поиск, для этого в верхнем левом углу вкладки в поле поиска ввести значение. В левом нижнем углу указано количество записей, а в правом нижнем углу кнопки переключения страниц.

Настройка boot-меню

На вкладке **Настройка boot-меню** осуществляется управление файлом настройки boot-меню на клиентах ALD Pro.

На вкладке отображается актуальный текст файла настройки.

Пример

```
UI vesamenu.c32

# 0 - отключение приглашения командной строки. Загрузка начнется сразу
PROMPT 0

# Автоматический выбор меню по таймеру. Секунды вычисляются делением на 10
→ введенного значения
TIMEOUT 100

DEFAULT bootlocal # Выбор по умолчанию загрузки с диска
#DEFAULT pxeinstall # Выбор по умолчанию загрузки по сети

menu background isolinux/aldpro_bios.png
menu title User Management Portal Boot Menu
```

(продолжение на следующей странице)

```

# Локальная загрузка с диска
LABEL bootlocal
    menu label Boot from first HDD
    kernel chain.c32
    append hd0 0
TEXT HELP
Normal boot from HDD
ENDTEXT

# Загрузка из сети
LABEL pxeinstall
    menu label PXE operation system install
    kernel linux
    append initrd=initrd.gz vga=788 auto=true priority=critical debian-
    ↪installer/locale=ru_RU console-keymaps-at/keymap=ru hostname={HOSTNAME}
    ↪domain={DOMAIN_REALM} astra-license/license=true url=http://192.168.17.5/
    ↪tftp/{PROFILE_UNIQ_NAME}/{PRESEED_FILE_NAME} interface=auto netcfg/dhcp_
    ↪timeout=60 # Необходимо указать IP адрес Вашего сервера установи ОС по сети
TEXT HELP
Install AstraLinux Operating System
ENDTEXT

```

Добавить или изменить файл настройки можно двумя способами:

- добавить текст из файла на компьютере;
- вручную ввести или изменить текст файла на вкладке.

Для добавления текста из файла необходимо нажать кнопку **[Загрузить из файла]**, в окне навигации выбрать на компьютере необходимый файл в формате *.conf или *.txt и нажать **[Открыть]**.

Содержимое файла отобразится в форме **Редактировать скрипт вручную**, при этом предыдущее содержимое файла настройки будет заменено. При необходимости добавленный текст можно отредактировать.

Для сохранения файла настройки необходимо ввести комментарий и нажать кнопку сохранения. Для отмены внесения изменений в файл настройки нажать кнопку **[Отменить]**.

Для добавления или редактирования файла настройки вручную необходимо нажать на

кнопку **[Редактировать файл]**, после чего форма **Редактировать скрипт вручную** станет доступна для редактирования.

Для сохранения файла настройки необходимо ввести комментарий и нажать кнопку сохранения. Для отмены внесения изменений в файл конфигурации нажать кнопку **[Отменить]**.

Для просмотра истории изменений файла конфигурации необходимо нажать на кнопку **[История изменений]**. Откроется карточка с отображением списка изменений с указанием даты изменения, автора изменения и комментария. В списке доступен поиск, для этого в верхнем левом углу вкладки в поле поиска ввести значение. В левом нижнем углу указано количество записей, а в правом нижнем углу кнопки переключения страниц.

GRUB.

На вкладке **GRUB** осуществляется управление скриптом настройки GRUB для клиента ALD Pro.

На вкладке отображается актуальный текст скрипта.

Пример

```
if loadfont $prefix/font.pf2 ; then
    set gfxmode=800x600
    set gfxpayload=keep
    insmod efi_gop
    insmod efi_uga
    insmod video_bochs
    insmod video_cirrus
    insmod gfxterm
    insmod png
    terminal_output gfxterm
fi

if background_image /isolinux/aldpro.png; then
    set color_normal=light-gray/black
    set color_highlight=white/black
else
    set menu_color_normal=cyan/blue
    set menu_color_highlight=white/blue
```

(продолжение на следующей странице)

```

fi

# Установка Astra Linux Special Edition
menuentry 'Install AstraLinux Operating System' {
    set background_color=black
    linux      (http,192.168.17.5)/tftp/linux modprobe.blacklist=evbug debian-
    ↪installer/allow_unauthenticated=true auto=true priority=critical debian-
    ↪installer/locale=en_US console-keymaps-at/keymap=ru hostname={HOSTNAME}
    ↪domain={DOMAIN_REALM} astra-license/license=true url=http://192.168.17.5/
    ↪tftp/{PROFILE_UNIQ_NAME}/{PRESEED_FILE_NAME} interface=auto netcfg/dhcp_
    ↪timeout=60
    initrd     (http,192.168.17.5)/tftp/initrd.gz
}

```

Добавить или изменить файл настройки можно двумя способами:

- добавить текст из файла на компьютере;
- вручную ввести или изменить текст файла на вкладке.

Для добавления текста конфигурации из файла необходимо нажать кнопку **[Загрузить из файла]**, в окне навигации выбрать на компьютере необходимый файл в формате *.cfg и нажать **[Открыть]**.

Содержимое файла отобразится в форме **Редактировать скрипт вручную**, при этом предыдущее содержимое файла настройки будет заменено. При необходимости добавленный текст можно отредактировать.

Для сохранения файла настройки необходимо ввести комментарий и нажать кнопку сохранения. Для отмены внесения изменений в файл настройки нажать кнопку **[Отменить]**.

Для добавления или редактирования файла настройки вручную необходимо нажать на кнопку **[Редактировать файл]**, после чего форма **Редактировать скрипт вручную** станет доступна для редактирования.

Для сохранения файла настройки необходимо ввести комментарий и нажать кнопку сохранения. Для отмены внесения изменений в файл конфигурации нажать кнопку **[Отменить]**.

Для просмотра истории изменений файла конфигурации необходимо нажать на кнопку

[История изменений]. Откроется карточка с отображением списка изменений с указанием даты изменения, автора изменения и комментария. В списке доступен поиск, для этого в верхнем левом углу вкладки в поле поиска ввести значение. В левом нижнем углу указано количество записей, а в правом нижнем углу кнопки переключения страниц.

Удаление профиля загрузки

Профиль загрузки или одновременно несколько профилей можно удалить. Для этого необходимо отметить профиль в списке и нажать кнопку **[Удалить]**.

Также удалить профиль можно из его карточки: открыть карточку нажатием на профиль в списке, затем на карточке нажать кнопку **[Удалить профиль]**. После подтверждения удаления будет выполнен переход к списку профилей.

6.2.3.4. Операционные системы

На вкладке приведен список операционных систем, доступных для использования в профилях загрузки при установке ОС по сети. Для каждой записи указано название операционной системы, ее архитектура, путь к установочному дистрибутиву и число профилей, в которых участвует ОС.

В списке доступен поиск, для этого в поле поиска ввести значение. Внизу списка указано количество записей в списке.

6.2.4. Удаление сервера установки ОС

Для удаления сервера установки ОС открыть его карточку, нажав на сервер в списке, затем на карточке нажать кнопку **[Удалить сервер установки ОС]**. После подтверждения удаления будет выполнен переход к списку серверов.

Мониторинг

В разделе доступен просмотр журнала событий мониторинга и мониторинг подсистем ALD Pro.

7.1. Журнал событий мониторинга

В подразделе приводится информация о мониторинге событий.

Подраздел состоит из вкладок:

- **Журнал событий;**
- **Серверы мониторинга.**

7.1.1. Журнал событий

На вкладке в табличном виде приводится перечень событий мониторинга. Настройка сбора событий выполняется в подразделе *Настройка сбора журналов событий* (раздел *Журнал событий*)

Для событий указывается:

- дата и время появления;
- критичность события — предупреждение, ошибка и т.д.;
- сервер, на котором произошло событие;
- описание события;
- длительность события.

Для поиска или фильтрации событий необходимо в блоке **Фильтр** в соответствующих полях задать значения для поиска или фильтрации и нажать кнопку **[Применить]**.

Поиск или фильтрация доступны по одному или нескольким атрибутам:

- **Сервер;**

- **Описание события;**
- **Дата начала;**
- **Дата окончания.**

Дополнительно в списке событий доступна фильтрация по критичности события, для этого в столбце **Критичность** нажать на значок фильтра и указать значения для фильтрации.

В левом нижнем углу указано количество правил, а в правом нижнем углу кнопки переключения страниц.

Внизу списка событий в левом углу указано количество записей в журнале, в правом углу размещены кнопки смены страниц журнала.

Если не установлен глобальный каталог, то в портале управления будут на постоянной основе отображаться ошибки, не влияющие на работу Системы, при этом в журнале событий мониторинга будут зафиксированы события чрезвычайной критичности на контроллере домена:

- о неактивности глобального каталога (globalcatalog)
- о неактивности службы синхронизации объектов с глобальным каталогом (ipa-gcsyncd)

7.1.2. Серверы мониторинга

На вкладке осуществляется управление серверами мониторинга.

7.1.2.1. Список серверов мониторинга

На вкладке в табличном виде приведен список серверов мониторинга с указанием имени сервера, IP-адреса сервера, функций сервера и имени сайта.

В списке доступен поиск по всем значениям. Для этого в поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

В левом нижнем углу указано количество записей в списке, а в правом нижнем углу кнопки переключения страниц.

7.1.2.2. Развертывание сервера мониторинга

Для развертывания нового сервера мониторинга необходимо нажать на кнопку **[Развернуть сервер мониторинга]**, будет выполнен переход на карточку нового сервера мониторинга.

На карточке заполнить обязательные поля **Имя компьютера**, **Роль** и **Имя сайта**.

Для поля **Роль** доступен выбор из двух значений:

- **Основной сервер** — сервер будет выполнять мониторинг компонентов домена и собирать результаты мониторинга с локальных серверов;
- **Локальный сервер** — сервер будет выполнять функции локального мониторинга.

Для сохранения нового сервера мониторинга необходимо нажать на кнопку сохранения в правом верхнем углу. Будет выполнен переход к списку серверов мониторинга.

Для закрытия карточки и возврата к списку серверов мониторинга нажать на кнопку закрытия.

7.1.2.3. Редактирование сервера мониторинга

Редактирование сервера мониторинга выполняется на его карточке. Для открытия карточки необходимо в списке нажать на соответствующий сервер мониторинга.

Для редактирования доступны функции сервера и имя сайта.

Для применения изменений нажать на кнопку сохранения в правом верхнем углу. Будет выполнен переход к списку серверов мониторинга.

Для закрытия карточки и возврата к списку серверов мониторинга нажать на кнопку закрытия.

7.1.2.4. Удаление сервера мониторинга

Удаление сервера мониторинга выполняется из его карточки: открыть карточку нажатием в списке на соответствующий сервер мониторинга, затем на карточке нажать кнопку **[Удалить сервер мониторинга]**. После подтверждения удаления будет выполнен переход к списку серверов мониторинга.

7.2. Витрины мониторинга домена

Витрина мониторинга – это UI-виджет (дашборд) который отображает некоторую информацию о состоянии ALD Pro, её подсистем или подмодулей. Серве(а) мониторинга занимается сбором информации о состоянии ALD Pro и выводит их пользователю в графическом интерфейсе браузера в виде набора витрин мониторинга, что позволяет пользователю оценить состояние системы.

В подразделе осуществляется:

- просмотр виджетов событий мониторинга и графиков производительности;
- просмотр шаблонов мониторинга;
- контроль доступности, работоспособности и утилизации ресурсов компонентов системы.

Список серверов формируется автоматически из серверов, развернутый в домене. Требуется порядка 30 минут с момента развертывания, чтобы сервер попал в данный список.

Витрина из выпадающего списка **Каталог витрин** выводит данные в виде виджетов на панели ниже. С помощью витрины отслеживаются системные показатели каждой подсистемы:

- **Динамическая настройка узла**
- **Мониторинг**
- **Общий доступ к файлам**
- **Печать**
- **Портал управления**
- **Разрешение имен**
- **Репозитории программного обеспечения**
- **Синхронизация времени**
- **Служба каталогов**
- **Установка ОС по сети**

7.2.1. Просмотр витрины

Для просмотра информации необходимо выбрать значения из выпадающих списков **Сервер** и **Каталог витрин**, после чего будет отображена соответствующая информация о сервере. Для поиска сервера или витрины необходимо начать вводить название по соответствующему полю.

По умолчанию выводится информация за последние 6 часов. Для вывода информации за более или менее продолжительный период необходимо выбрать период в выпадающем меню в правом верхнем углу панели виджетов.

Информация на виджетах может быть обновлена вручную или может быть настроено обновление через заданный период. По умолчанию обновление через заданный период отключено. Для обновления данных или задания периода обновления необходимо кликнуть кнопку **Refresh dashboard** в правом верхнем углу панели виджетов.

Каждый из отображаемых на панели статусов может быть раскрыт. Для этого необходимо выбрать пункт "View" из выпадающего меню названия виджета. Для возврата к панели используется стрелка рядом с названием панели.

Для каждой витрины подсистемы отображаются виджеты со статусом используемых на выбранном сервере служб. Доступные статусы:

- **Доступно:** служба установлена на сервере, работает в штатном режиме;
- **Авария:** служба недоступна, но установлена на сервере;
- **Нет данных:** служба не установлена на сервере.

Витрина **Мониторинг подсистемы "Портал управления"** также отображает данные по использованию памяти и ЦП процессами служб.

Витрина **Мониторинг подсистемы "Служба каталогов"** также отображает срок действия используемых сертификатов.

Витрина **Мониторинг системных показателей** отображает системные показатели каждого сервера.

Витрина **Мониторинг подсистемы «Глобальный каталог»** отображает состояние целостности глобального каталога и служб контроля целостности и синхронизации глобального каталога. Целостность глобального каталога - соответствие объектов контроллера домена объектам глобального каталога. На панели **Целостность глобального каталога** отображается количество ошибок.

Примечание: Если не установлен глобальный каталог, на витринах мониторинга подсистемы «Глобальный каталог» контроллера домена будет зафиксирован статус ГК «Авария».

7.3. Расширение функционала мониторинга

Мониторинг событий ALD Pro реализован с использованием решения Zabbix. ALD Pro позволяет подключиться к web-интерфейсу Zabbix. Использование web-интерфейса Zabbix позволяет:

- расширить перечень событий, подлежащих мониторингу;
- использовать полный перечень функций Zabbix.

Для доступа к web-интерфейсу Zabbix необходимо ввести в браузере адрес сервера мониторинга ALD Pro в формате: `https://<адрес сервера мониторинга>/zabbix`

Пример `https://mon.aldpro.astralinux.ru/zabbix`

Далее в открывшемся окне авторизации необходимо ввести логин и пароль системной учетной записи администрирования Zabbix.

Модуль синхронизации

В разделе осуществляется управление модулем синхронизации объектов MS AD и ALD Pro.

Модуль синхронизации является отдельным от портала управления модулем. Основная задача модуля синхронизации – миграция в реальном времени изменений отслеживаемых LDAP-объектов в подключенном сервере Active Directory в контроллер домена ALD Pro, за которым закреплен модуль синхронизации.

Синхронизация может быть односторонней (AD -> ALD Pro) и двусторонней (AD <-> ALD Pro).

Односторонняя синхронизация доступна объектам:

- User (Пользователи);
- OU (Подразделения);
- User Groups (Группы пользователей).

Двусторонняя синхронизация реализована только для паролей пользователей.

Важно: Для работы модуля синхронизации на контроллере домена Windows Active Directory необходимо выполнить конфигурирование групповой политики для фильтра паролей (см.Руководство администратора, Инструкция по дополнительной настройке модуля синхронизации)

Модуль синхронизации имеет ряд ограничений в части синхронизации объектов, имеющих в своем составе специальные символы. Для удобства работы предоставлен инструмент обработки запрещенных символов (см. раздел **Полезные инструкции** special_characters_instruction)

8.1. Настройки

В подразделе представлены функции управления синхронизацией паролей и контроллерами домена, участвующими в синхронизации.

8.1.1. Контроллеры домена AD

8.1.1.1. Создание нового контроллера AD

Для создания нового контроллера AD необходимо нажать на кнопку **Новый контроллер AD**. Откроется карточка создания контроллера AD.

Все поля в карточке являются обязательными для заполнения.

В поле **Имя сервера** необходимо ввести наименование контроллера домена AD. В названии допустимо использовать строчные буквы латинского алфавита a-z и символы . и -.

В поле **Имя пользователя** необходимо ввести логин пользователя в формате логин@домен_AD. В названии допустимо использовать строчные буквы латинского алфавита a-z и символы @, . и -. Учетная запись пользователя должна обладать правами администратора домена в домене AD или ограниченными правами на контейнер **Delete Object** (Корзина) в домене AD и организационное подразделение (OU), задействованное для процесса синхронизации (см.Руководство администратора, Инструкция по дополнительной настройке модуля синхронизации).

В поле **Пароль** ввести пароль от учетной записи.

Для заполнения поля **Сертификат** необходимо нажать на кнопку **Выбрать файл** и загрузить сертификат в формате **.pem**. Данный сертификат должен быть сформирован и выгружен с помощью Центра сертификации AD.

Для сохранения нового контроллера AD нажать на кнопку сохранения. Будет выполнен переход к вкладке контроллеров домена AD.

Для закрытия карточки создания нового контроллера AD и возврата к вкладке контроллеров домена AD нажать на кнопку закрытия.

8.1.1.2. Редактирование контроллера AD

Для редактирования контроллера AD необходимо нажать на запись контроллера AD в списке. Откроется карточка контроллера AD, для редактирования доступны все поля.

Для применения изменений нажать на кнопку сохранения.

Для закрытия карточки редактирования контроллера AD и возврата к вкладке контроллеров домена AD нажать на кнопку закрытия.

8.1.1.3. Удаление контроллера AD

Контроллер домена AD можно удалить:

- на вкладке контроллеров домена AD, выделив нужный домен и нажав кнопку **-Удалить**;
- на карточке контроллера домена AD, нажав кнопку **Удалить контроллер AD**.

После удаления контроллера AD будет выполнен переход на вкладку контроллеров домена AD.

8.1.2. Контроллеры домена ALD

8.1.2.1. Создание нового контроллера ALD

Модуль синхронизации всегда устанавливается на первый контроллер домен. При установке модуля синхронизации контроллер домена **ALD** добавляется в карточку **Контроллеры домена ALD** автоматически.

При установке модуля синхронизации создается учетная запись имеющая вид `syncset/<имя сервера>@<имя домена>`. Данная учетная запись является сервисной и используется для работы модуля синхронизации. Пароль данной учетной записи является бессрочным, что делает работу модуля синхронизации более стабильной и устойчивой.

Внимание: При обновлении до 2.4.0 учетная запись текущего подключения изменится на сервисную.

Для создания нового контроллера ALD необходимо нажать на кнопку **Новый контроллер ALD**. Откроется карточка создания контроллера ALD.

Все поля в карточке являются обязательными для заполнения.

В поле **Имя сервера** необходимо ввести имя компьютера в формате FQDN («имя_сервера.полное_имя_домена»), который выполняет роль первого контроллера домена ALD Pro. В названии допустимо использовать строчные буквы латинского алфавита «a-z» и символы . и «-».

В поле **Имя пользователя** необходимо ввести служебную учетную запись, которая создается на контроллере домена и имеет вид syncer/<имя сервера>@<имя домена>.

Использование служебной учетной записи избавляет от необходимости смены пароля по истечению срока его действия.

Для заполнения поля **Сертификат** необходимо нажать на кнопку **Выбрать файл** и загрузить сертификат в формате **.pem**. Данный сертификат можно получить на web-сайте ALD Pro средствами стандартного браузера.

Для сохранения нового контроллера ALD нажать на кнопку сохранения. Будет выполнен переход к вкладке контроллеров домена ALD.

Для закрытия карточки создания нового контроллера ALD и возврата к вкладке контроллеров домена ALD нажать на кнопку закрытия.

8.1.2.2. Редактирование контроллера ALD

Для редактирования контроллера ALD необходимо нажать на запись контроллера ALD в списке. Откроется карточка контроллера ALD, для редактирования доступны все поля.

Для применения изменений нажать на кнопку сохранения.

Для закрытия карточки редактирования контроллера ALD папки и возврата к вкладке контроллеров домена ALD нажать на кнопку закрытия.

8.1.2.3. Удаление контроллера ALD

Контроллер домена ALD можно удалить:

- на вкладке контроллеров домена ALD, выделив нужный домен и нажав кнопку

-Удалить;

- на карточке контроллера домена ALD, нажав кнопку **Удалить контроллер ALD**.

После удаления контроллера ALD будет выполнен переход на вкладку контроллеров домена ALD.

8.1.3. Синхронизация паролей

Вкладка синхронизации паролей содержит поле получения пароля для сервиса отправки паролей.

Для получения открытого ключа необходимо нажать на кнопку **Получить ключ**.

Результатом будет файл открытого ключа public.gpg, скачанный на устройство. В поле **Номер ключа** после нажатия кнопки обновиться порядковый номер сгенерированного открытого ключа.

После необходимо добавить файл public.gpg на каждую реплику ALD Pro в расположение /opt/rbta/aldpro/syncser. При каждом выпуске нового файла public.gpg, его необходимо тиражировать по всем репликам.

8.2. Источники

В подразделе представлены функции управления структурой синхронизации.

8.2.1. Сопоставление подразделений

8.2.1.1. Создание нового сопоставления

Для создания нового сопоставления подразделений необходимо нажать на кнопку **+ Новое сопоставление**. Будет открыта карточка создания сопоставления.

На карточке необходимо заполнить обязательные поля из выпадающих списков **Источник** и **Получатель**. Для каждого поля из структуры подразделений необходимо выбрать одно, для которых будет выполнена синхронизация.

Список поля **Источник** содержит перечень подразделений AD.

Список поля **Получатель** содержит перечень подразделений ALD, свернутый до родительского.

После выбора значений для полей **Источник** и **Получатель** для проверки возможных конфликтов синхронизации необходимо нажать кнопку **Проверить наличие конфликтов**.

На данном этапе проверяется наличие конфликтов синхронизации между **Источником** и **Получателем** до создания сопоставления подразделений.

Если конфликты не будут обнаружены, появится всплывающее уведомление об отсутствии конфликтов.

Если конфликты будут обнаружены, сообщение об их наличии будет отображено во всплывающем окне. Так же появится возможность скачать файл на вкладке **Структура дерева синхронизации**, содержащий список конфликтов. Решение о разрешении конфликтов вручную или их игнорировании принимает администратор.

Важно: Если проигнорировать возникшие конфликты и сохранить сопоставление подразделений, объекты ALD Pro, конфликтующие с объектами AD, не будут изменены.

Для сохранения нового сопоставления нажать на кнопку сохранения. Будет выполнен переход к вкладке сопоставления подразделений.

Для закрытия карточки создания сопоставления и возврата к вкладке сопоставления подразделений нажать на кнопку закрытия.

8.2.1.2. Удаление сопоставления

Для удаления сопоставления подразделений необходимо выделить запись в списке и на карточке нажать кнопку - **Удалить**. После удаления сопоставления подразделений будет выполнен переход к вкладке сопоставления подразделений.

8.2.2. Структура дерева синхронизации

Вкладка содержит информацию о структуре подразделений виртуального дерева, через которое проходит синхронизация изменений, объектах и конфликтах синхронизации.

8.2.2.1. Конфликты синхронизации

Для просмотра списка конфликтов необходимо нажать на кнопку **Проверить конфликты синхронизации**. По нажатию кнопки запускается проверка наличия конфликтов синхронизации для всех сопоставлений подразделений AD и ALD Pro.

На данном этапе проверяется наличие конфликтов синхронизации оставшихся в процессе синхронизации сопоставлений подразделений.

Результатом будем всплывающее уведомление об отсутствии конфликтов или их наличии. При наличии конфликтов можно будет скачать файл, содержащий список конфликтов. Решение о разрешении конфликтов вручную или их игнорировании принимает администратор.

При выборе подразделения для просмотра объектов синхронизации становится доступен функционал ручного разрешения конфликтов:

- кнопка **Решить конфликт подразделения** разрешает конфликты синхронизации подразделения и появляется опционально при наличии конфликта синхронизации выбранного подразделения.
- кнопка **Решить**, имеющаяся у каждого объекта синхронизации, разрешает конфликты синхронизации конкретного объекта и делает его доступным для всех последующих синхронизаций.

Важно: Если кнопка **Решить конфликт подразделения** отображается в интерфейсе. Необходимо в первую очередь разрешить конфликты синхронизации подразделения, во вторую - конфликты синхронизации конкретных объектов.

8.3. Сопоставление атрибутов

В подразделе Сопоставление атрибутов представлен функционал управления атрибутами LDAP объектов синхронизации.

8.3.1. Карта сопоставлений

8.3.1.1. Сопоставления по умолчанию

В модуле синхронизации имеется список сопоставлений атрибутов, синхронизирующихся по умолчанию.

Сопоставления отражаются на вкладке **Карта сопоставлений** и не доступны для удаления.

8.3.1.2. Создание нового сопоставления

Для создания нового сопоставления атрибутов необходимо нажать на кнопку **+ Новое сопоставление**. Будет открыта карточка создания сопоставления.

В карточке необходимо заполнить обязательные поля из выпадающих списков **Тип объекта синхронизации**: **Подразделение**, **Пользователь**, **Группа**, **Атрибут AD** и **Атрибут ALD**.

Для сохранения нового сопоставления нажать на кнопку сохранения. Будет выполнен переход к вкладке карты сопоставления.

Для закрытия карточки создания сопоставления и возврата к вкладке карты сопоставления нажать на кнопку закрытия.

8.3.1.3. Удаление сопоставления

Для удаления сопоставления необходимо выделить запись в списке и в карточке нажать кнопку **- Удалить**. После удаления сопоставления будет выполнен переход к вкладке карты сопоставлений.

8.3.2. Атрибуты AD

8.3.2.1. Атрибуты AD по умолчанию

В модуле синхронизации имеется список атрибутов синхронизирующихся по умолчанию.

Атрибуты отражаются на вкладке Атрибуты AD и не доступны для удаления.

8.3.2.2. Создание нового атрибута AD

Для создания нового атрибута AD необходимо нажать на кнопку **+ Новый атрибут**. Будет открыта карточка создания атрибута AD.

В карточке необходимо заполнить обязательные поля **Имя атрибута** и **Атрибут LDAP**.

В значении поля **Имя атрибута** допустимо использовать строчные и прописные буквы латинского алфавита **a-z, A-Z** и цифры **0-9**.

В значении поля **Атрибут LDAP** допустимо использовать строчные и прописные буквы латинского алфавита **a-z, A-Z**, цифры **0-9** и символ **-**.

Для сохранения нового атрибута нажать на кнопку сохранения. Будет выполнен переход к вкладке атрибуты AD.

Для закрытия карточки создания атрибута и возврата к вкладке атрибуты AD нажать на кнопку закрытия.

8.3.2.3. Удаление атрибута AD

Для удаления атрибута AD необходимо выделить запись в списке и в карточке нажать кнопку **- Удалить**. После удаления атрибута AD будет выполнен переход к вкладке атрибуты AD.

8.3.3. Атрибуты ALD

8.3.3.1. Атрибуты ALD по умолчанию

В модуле синхронизации имеется список атрибутов синхронизирующихся по умолчанию.

Атрибуты отражаются на вкладке Атрибуты ALD и не доступны для удаления.

8.3.3.2. Создание нового атрибута ALD

Для создания нового атрибута ALD необходимо нажать на кнопку **+ Новый атрибут**. Будет открыта карточка создания атрибута ALD.

В карточке необходимо заполнить обязательные поля **Имя атрибута** и **Атрибут LDAP**.

В значении поля **Имя атрибута** допустимо использовать строчные и прописные буквы латиницы и кириллицы **a-z, A-Z, а-я, А-Я** и цифры **0-9**.

В значении поля **Атрибут LDAP** допустимо использовать строчные и прописные буквы латинского алфавита **a-z, A-Z**, цифры **0-9** и символ **-**.

Для сохранения нового атрибута нажать на кнопку сохранения. Будет выполнен переход к вкладке атрибуты ALD.

Для закрытия карточки создания атрибута и возврата к вкладке атрибуты ALD нажать на кнопку закрытия.

8.3.3.3. Удаление атрибута ALD

Для удаления атрибута ALD необходимо выделить запись в списке и в карточке нажать кнопку **- Удалить**. После удаления атрибута ALD будет выполнен переход к вкладке атрибуты ALD.

8.4. Особенности работы модуля синхронизации

1. При настройке модуля синхронизации рекомендуется поддерживать соотношение доменов один к одному, то есть выполнять синхронизацию объектов из одного домена MS AD в один домен ALD Pro. Настройка синхронизации из нескольких доменов MS AD в один домен ALD Pro увеличивает риски возникновения конфликтов синхронизации (так как конфликты могут возникать и между объектами доменов MS AD).
2. Нельзя производить переименование подразделений, добавленных в **Сопоставление подразделений**. Если возникла такая необходимость, корректно будет удалить сопоставление, произвести переименование и создать новое сопоставление подразделений.

3. Нельзя создавать сопоставления подразделений для дочерних подразделений подразделения, уже участвующего в синхронизации.
4. В домене ALD Pro в разделе **Управление доменом -> Пользователи и группы** содержится настройка **Максимальная длина имени пользователя**. Для успешной синхронизации длина имени пользователя AD должна быть меньше установленного значения, в противном случае возникнет ошибка синхронизации.
5. Необходимо учесть, что в момент синхронизации учетная запись синхронизируемого пользователя временно блокируется. Блокировка не превышает 30 секунд.
6. Атрибуты по умолчанию и соответствующие им сопоставления ограничены перечнем обязательных атрибутов для объектов ALD Pro
 - Пользователи: **Логин, Пароль, Подразделение, Фамилия** либо **Имя**
 - Группы пользователей: **Название группы, Подразделение**
 - Подразделения: **Наименование подразделения, Родительское подразделение**.

Однако не все эти атрибуты явно указаны на карточке **Атрибуты AD, Атрибуты ALD**, так как их синхронизация происходит внутренними процессами модуля синхронизации.

Добавляя эти атрибуты в явном виде в **Карте сопоставления**, есть риск нарушить логику работы модуля синхронизации

7. Наименование подразделений, наименования групп, логины пользователей не должны содержать специальных символов, за исключением “.”, “-”, “_”.
8. Модуль синхронизации может быть установлен при первичной установке или в процессе обновления контроллера домена. Ограничением настоящей версии является установка модуля синхронизации только на первый контроллер домена. В случае отключения первого контроллера домена, синхронизация новых данных, добавленных после отключения первого контроллера домена, выполняться не будет. Ранее синхронизированные данные сохранятся и будут реплицироваться между контроллерами домена, для которых созданы соглашения о репликации.
9. Для успешной синхронизации учетную запись администратора, которая используется для подключения к контроллеру домена, необходимо добавить в группу admins.
10. При изменении пароля синхронизированного пользователя через интерфейс FreeIPA, синхронизация пароля **ALD Pro -> AD** не произойдет. Для изменения пароля с последующей успешной синхронизацией необходимо использовать интерфейс ALD Pro.

11. Процесс изменения пароля пользователя через личный кабинет с последующей синхронизацией **ALD Pro -> AD** проходит успешно, только при использовании личного кабинета, на котором был развернут модуль синхронизации.
12. При сбросе пароля пользователя через интерфейс ALD Pro временный пароль не синхронизируется. После сброса пароля пользователя необходимо залогиниться в домене, изменить пароль с временного на постоянный и только тогда произойдет синхронизация пароля **ALD Pro -> AD**.
13. Пароли пользователей MS AD, установленные до настройки модуля синхронизации, синхронизированы не будут. Синхронизация паролей пользователей после настройки модуля синхронизации и сопоставлений подразделений происходит по логике:
- синхронизирован пользователь в домен ALD Pro -> изменен пароль пользователя в домене MS AD -> синхронизирован пароль пользователя в домен ALD Pro
 - создан пользователь в домене MS AD -> синхронизирован пользователь в домен ALD Pro
14. При изменении расположения синхронизированного подразделения через MS AD , групповые политики, привязанные к подразделению в домене ALD Pro не сохраняются. Варианты решения:
- Планировать иерархию подразделений таким образом, чтобы перенос подразделений не сказывался на работе групповых политик: добавление еще одного уровня вложенности, на который будут применяться ГП.
 - Повторно привязывать групповые политики после переноса подразделения.

Журнал событий

В разделе осуществляется настройка журнала событий (система аудита). Сервера журнала событий занимаются сбором ограниченного (но настраиваемого) набора событий с определённого набора компьютеров домена ALD Pro с помощью инструмента syslog-ng.

9.1. Серверы журнала событий

В подразделе выполняется развертывание серверов журнала событий.

9.1.1. Список серверов журнала событий

В подразделе на вкладке **Серверы журнала событий** приводится список серверов с указанием имени сервера, IP-адреса и имени сайта.

В списке доступен поиск по имени сервера, IP-адресу сервера и имени сайта. Для этого в поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

В левом нижнем углу указано количество серверов, а в правом нижнем углу кнопки переключения страниц.

9.1.2. Развертывание сервера журнала событий

Для создания нового сервера необходимо нажать на кнопку **[+ Развернуть сервер журнала событий]**, будет выполнен переход на карточку нового сервера.

На карточке выбрать из выпадающего списка значения полей **Имя компьютера** и **Имя сайта**. Оба поля являются обязательными для заполнения. Управление сервером осуществляется после его сохранения (см. [Управление сервером журнала событий](#)).

Важно: В выпадающем списке предлагаются только те компьютеры, которые не заняты

под серверы в других подсистемах и в системе журнала событий.

Для сохранения сервера нажать на кнопку сохранения в правом верхнем углу. Будет выполнен переход к списку серверов.

Важно: Развертывание сервера занимает некоторое время. Отслеживать процесс развертывания можно одним из следующих вариантов:

- через всплывающие сообщения, которые появляются по мере наступления очередного события;
- на вкладке **Журнал заданий (Автоматизация->Задания автоматизации)** по названию **audit_install**.

Система не имеет ограничений на количество серверов журнала событий и на количество серверов на одном сайте.

Для закрытия карточки и возврата к списку серверов нажать на кнопку закрытия.

9.1.3. Управление сервером журнала событий

Управление сервером журнала событий выполняется на его карточке. Для открытия карточки необходимо в списке серверов нажать на соответствующий сервер.

На карточке сервера доступно для редактирования поле **Имя сайта**.

Для сохранения изменений нажать на кнопку сохранения в правом верхнем углу. Будет выполнен переход к списку серверов.

Для закрытия карточки и возврата к списку серверов нажать на кнопку закрытия.

9.1.4. Удаление сервера журнала событий

Удаление сервера журнала событий осуществляется из его карточки: открыть карточку, нажав в списке серверов на соответствующий сервер, затем на карточке нажать кнопку **[Удалить сервер журнала событий]**. После подтверждения удаления будет выполнен переход к списку серверов журнала событий.

9.2. Настройка сбора журналов событий

В подразделе выполняется настройка правил сбора информации о событиях.

9.2.1. Список правил

В подразделе на вкладке **Правила сбора событий** приводится список правил сбора информации о событиях с указанием имени правила и его состояния (включено или выключено). Журнал собранных событий отображается в подразделе *Журнал событий мониторинга* (раздел *Мониторинг*)

Важно: При обновлении Системы до версии 2.0.0 все добавленные правила, у которых не настроен параметр состояния и/или сервер сбора логов, отобразятся в таблице, но будут недоступны для работы в этой версии Системы. Для корректной работы правил, их нужно удалить, развернуть и настроить.

В списке доступен поиск по имени правила. Для этого в верхнем левом углу вкладки в поле поиска начните вводить значение.

В списке доступна фильтрация по значению **Состояние**, для этого необходимо нажать на значок фильтра рядом с названием столбца и отметить требуемые значения для фильтрации.

В левом нижнем углу указано количество правил, а в правом нижнем углу кнопки переключения страниц.

9.2.2. Добавление нового правила сбора информации о событиях

Для добавления нового правила необходимо нажать на кнопку **[+ Новое правило]**, будет выполнен переход на карточку нового правила.

В карточке на вкладке **Основное** заполнить обязательные поля **Имя правила**, **Тип логов**, **Сервер сбора логов**.

В поле **Тип логов** задается тип событий, информация о которых будет собираться. Доступны следующие значения:

- **Логи авторизации Fly** — сбор информации о входе пользователей в графический интерфейс клиентов домена;
- **Логи удаленного подключения** — сбор информации обо всех удаленных подключениях к клиентам домена по протоколу ssh;
- **Логи состояния подключения к сети** — сбор информации о состоянии подключения к сети всех клиентов домена.

Важно: Версия 2.0.0 Системы поддерживает использование уникального типа логов для одного сервера логов. Т.е. создание двух правил с типом логов, например, **Логи авторизации Fly** на одном сервере сбора логов запрещено.

Также можно заполнить поле **Описание**.

Для включения или выключения правила, соответственно, установить флаг **Включено** или **Выключено**.

Для сохранения правила нажать на кнопку сохранения в правом верхнем углу.

Важно: Создание правила занимает некоторое время. Отслеживать процесс создания можно одним из следующих вариантов:

- через всплывающие сообщения, которые появляются по мере наступления очередного события;
- на вкладке Журнал заданий (Автоматизация->Задания автоматизации) по названию add_rule.

Для применения внесенных изменений нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку правил нажать на кнопку закрытия.

9.2.3. Просмотр информации о правиле

Просмотр информации о правиле доступен на его карточке. Для открытия карточки правила необходимо в списке правил нажать на соответствующее правило.

На вкладке **Основное** можно изменить описание правила. Для применения внесенных изменений нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку правил нажать на кнопку закрытия.

9.2.4. Редактирование правила сбора информации о событии

Для редактирования доступно поле **Описание** на вкладке **Основное** карточки правила. Правило можно включать и выключать - изменять его состояние.

Важно: Начиная с версии 2.0.0 не предусмотрена возможность настройки правил сбора логов.

Важно: При внесении изменений в правило сбора информации о событии, его версия меняется автоматически.

9.2.4.1. Управление состоянием правила

Управление состоянием правила осуществляется из его карточки на вкладке **Основное**.

Для включения или выключения правила отметить, соответственно, пункт **Включено** или **Выключено**.

Для применения внесенных изменений нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку правил нажать на кнопку закрытия.

9.2.5. Удаление правила

Для удаления правила или одновременно несколько правил необходимо в списке правил отметить требуемое правило и нажать кнопку **[Удалить]**.

Чтоб отметить все записи — отметить пункт **Имя правила**. Для снятия отметок со всех

правил — нажать кнопку закрытия в правом верхнем углу.

Также удалить правило можно из его карточки: открыть карточку, нажав в списке правил на соответствующее правило, затем на карточке на вкладке **Основное** нажать кнопку **[- Удалить правило]**. После подтверждения удаления будет выполнен переход к списку правил.

Групповые политики

В разделе осуществляется настройка и управление групповыми политиками. Групповая политика – это набор правил, в соответствии с которыми отдельный компьютер домена ALD Pro выполняет настройку рабочей среды. Настройка рабочей среды производится с помощью запуска скриптов групповой политики. Групповые политики используются для массовой настройки однотипной рабочей среды на компьютерах, подключенных в домен. Группу компьютеров можно выбрать разными способами.

10.1. Групповые политики

В подразделе осуществляется управление групповыми политиками: создание, настройка и удаление групповых политик, назначение политик на подразделение и др.

10.1.1. Список групповых политик

В подразделе приведен список групповых политик с указанием имени, версии, даты изменения и имени пользователя, внесшего изменения.

В списке доступен поиск по имени политики, версии и автору изменений. Для этого в поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Для просмотра информации о политике нажать на соответствующую политику в списке. Будет открыта карточка политики с информацией о ней.

В левом нижнем углу указано количество групповых политик, а в правом нижнем углу кнопки переключения страниц.

10.1.2. Создание групповой политики

Для создания новой групповой политики нажать кнопку **[Новая групповая политика]**, будет открыта карточка создания новой групповой политики.

На карточке на вкладке **Основное** заполнить обязательно поле **Имя групповой политики**, а также при необходимости добавить ее описание в поле **Описание групповой политики**.

Остальные вкладки станут доступны для редактирования после сохранения групповой политики (см. [Настройка групповой политики](#)).

Для сохранения новой групповой политики необходимо нажать на кнопку сохранения в правом верхнем углу. После сохранения групповой политики на вкладке **Основное** отобразится информация о датах создания и изменения политики, версии политики и авторе изменений.

Для закрытия карточки и возврата к списку групповых политик нажать на кнопку закрытия.

10.1.3. Настройка групповой политики

Настройка групповой политики выполняется на ее карточке. Для открытия карточки необходимо в списке групповых политик нажать на соответствующую политику.

Важно: При внесении изменений в настройку групповой политики, ее версия меняется автоматически.

На карточке управление групповой политикой осуществляется на вкладках:

- **Основное;**
- **Конфигурация политики;**
- **Параметры компьютеров;**
- **Параметры пользователей;**
- **Подразделения.**

Для закрытия карточки и возврата к списку групповых политик нажать на кнопку закрытия.

10.1.3.1. Основное

На вкладке отображается информация о групповой политике: ее название, описание, дата создания, дата изменения, версия изменения и имя пользователя, внесшего последние изменения.

Для редактирования доступны имя групповой политики и ее описание.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

10.1.3.2. Конфигурация политики

На вкладке приведен в табличном виде список параметров пользователей и параметров компьютеров, применяемых в данной групповой политике. Для каждого параметра указывается его название, тип (параметр пользователя или компьютера), папка хранения параметра (в каталоге параметров пользователей или в каталоге параметров компьютеров), и состояние параметра.

В списке доступен поиск по названию параметра и каталогу параметра. Для этого в верхнем левом углу вкладки в поле поиска ввести значение.

В списке доступна фильтрация по значениям столбцов **Тип** и **Состояние**, для этого необходимо нажать на значок фильтра рядом с названием соответствующего столбца и отметить требуемые значения для фильтрации.

При нажатии на параметр будет выполнен переход на вкладку **Параметры пользователя** или **Параметры компьютера** (в зависимости от типа параметра), к форме настройки данного параметра.

Для удаления из групповой политики параметра или одновременно нескольких параметров необходимо в списке отметить требуемые параметры и нажать кнопку **[Удалить]**.

Чтоб отметить все имеющиеся параметры — отметить пункт **Название параметра**.

В левом нижнем углу указано количество параметров, а в правом нижнем углу кнопки переключения страниц.

10.1.3.3. Параметры компьютеров

На вкладке осуществляется настройка параметров компьютеров и их включение в состав данной групповой политики.

На вкладке приведены папки с параметрами компьютеров в иерархическом виде.

Доступен поиск папки или параметра. Для этого в соответствующем поле поиска начать

вводить название параметра/папки, результат поиска будет выводиться по мере ввода.

В папке **Дополнительные параметры** отображаются параметры, созданные на вкладке *Параметры компьютеров* (раздел *Управление доменом*, подраздел *Дополнительные параметры групповых политик*).

При выборе параметра будет отображена форма настройки параметра. В форме указывается значение обязательного поля **Состояние**, можно добавить описание параметра в поле **Комментарий**. В соответствующих полях задаются значения настроек параметра. Информация о параметре и его атрибутах описана в справке (знак ? в правом верхнем углу).

В разделе **Требования к ОС** задается информация о том, с какими версиями ОС совместим данный параметр.

Для определения требований к ОС необходимо выбрать в выпадающем списке **Параметр ОС** один из атрибутов, задать значение параметра и выбрать один из следующих операторов сравнения:

- = - точное соответствие;
- ~ - указанная подстрока присутствует в значении;
- ; - задать несколько требований в ОС, читается через ИЛИ.

Если фильтр не указан, то проверка не выполняется.

Если поля заполнены, проверяется выполнение условия. Параметр применяется, только если условие выполнено.

Для каждого параметра можно указать собственный фильтр **Совместимой версии**, в том числе и для дополнительных параметров групповой политики.

Значения атрибутов выбранного параметра можно настроить в блоке **Настройки атрибутов**.

Параметры бывают простые и составные. Простые параметры имеют один список атрибутов. Атрибуты составного параметра представлены массивом списков. Если необходимо добавить список атрибутов для составного параметра, необходимо нажать кнопку **[+]** справа от названия блока **Настройка параметра**.

Для удаления списка атрибутов из массива нажать кнопку **[-]** справа над блоком продублированных полей.

Для сохранения настроек параметра необходимо в форме нажать кнопку **[Применить]**, при этом параметр будет добавлен в конфигурацию групповой политики.

10.1.3.4. Параметры пользователей

На вкладке осуществляется настройка параметров пользователей и их включение в состав данной групповой политики.

Доступен поиск папки или параметра. Для этого в соответствующем поле поиска начать вводить название параметра/папки, результат поиска будет выводиться по мере ввода.

В папке **Дополнительные параметры** отображены параметры, созданные на вкладке *Параметры пользователей* (раздел *Управление доменом*, подраздел *Дополнительные параметры групповых политик*).

При выборе параметра будет отображена форма настройки параметра. В форме указывается значение обязательного поля **Состояние**, можно добавить описание параметра в поле **Комментарий**.

В разделе **Требования к ОС** задается информация о том, с какими версиями ОС совместим данный параметр.

Для определения требований с ОС необходимо выбрать в выпадающем списке **Параметр ОС** один из атрибутов, задать значение параметра и выбрать один из следующих операторов сравнения:

- = - точное соответствие;
- ~ - указанная подстрока присутствует в значении;
- ; - задать несколько требований в ОС, читается через ИЛИ.

Если фильтр не указан, то проверка не выполняется.

Если поля заполнены, проверяется выполнение условия. Параметр применяется, только если условие выполнено.

Для каждого параметра можно указать собственный фильтр **Совместимой версии**, в том числе и для дополнительных параметров групповой политики.

Значения атрибутов выбранного параметра можно настроить в блоке **Настройки атрибутов**.

Параметры бывают простые и составные. Простые параметры имеют один список атрибутов. Атрибуты составного параметра представлены массивом списков. Если необходимо добавить список атрибутов для составного параметра, необходимо нажать кнопку **[+]** справа от названия блока **Настройка параметра**.

Для удаления списка атрибутов из массива нажать кнопку **[-]** справа над блоком продублированных полей.

Для сохранения настроек параметра необходимо в форме нажать кнопку **[Применить]**, при этом параметр будет добавлен в конфигурацию групповой политики.

10.1.3.5. Подразделения

На вкладке настраивается список подразделений, к пользователям и компьютерам которых будет применяться данная групповая политика. При этом групповая политика также будет применяться к пользователям и компьютерам дочерних подразделений.

Список подразделений с назначенными групповыми политиками

На вкладке приведен список подразделений, на которые назначена данная групповая политика, с указанием названия подразделения, приоритетом политики и принудительного наследования ее параметров.

В списке доступен поиск по названию подразделения. Для этого в поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Для доступа к функционалу нужно настроить привилегии. Список необходимых привилегий приведен в таблице 1.

Таблица 1. Привилегии

Привилегия	Описание	На что распространяется
Group Policies - Read	Привилегия позволяет: Видеть список групповых политик (Групповые политики/Групповые политики); Видеть карточки групповых политик (Групповые политики/Групповые политики/<Групповая политика>)	На весь домен
Group Policies User Parameters - Manage	Привилегия позволяет: Видеть список групповых политик в карточке подразделения (Пользователи и компьютеры/Организационная структура/<Подразделение>/вкладка Групповые политики); Видеть карточки групповых политик в карточке подразделения (Пользователи и компьютеры/Организационная структура/<Подразделение>/вкладка Групповые политики/<Групповая политика>)	На весь домен
Group Policy Membership - Manage	Привилегия позволяет: Добавлять и удалять политики для подразделений (Групповые политики/Групповые политики/<Групповая политика>/вкладка Подразделения); Добавлять, удалять и изменять приоритет политик для подразделений (Пользователи и компьютеры/Организационная структура/<Подразделение>/вкладка Групповые политики)	Выбранное подразделение

В левом нижнем углу указано количество подразделений, которым назначена данная групповая политика.

Назначение групповой политики на подразделение

Для назначения на подразделение групповой политики с заданными параметрами нажать кнопку **[Добавить подразделение]**. Будет открыта карточка подразделения. На карточке необходимо выбрать подразделение, на которое будет назначена данная групповая политика, а также приоритет применения групповой политики. Поле **Расположение подразделения в организационной структуре** заполняется автоматически при выборе подразделения.

Если необходимо, чтобы дочерние подразделения наследовали параметры данной

групповой политики, даже если где-то наследование отключено, необходимо установить флаг **Наследовать принудительно**.

На одно подразделение может быть назначено несколько групповых политик, но с разным приоритетом — приоритет должен быть уникальным числовым значением. Значение приоритета не может быть больше количества групповых политик, назначенных на это подразделение. Если на выбранное подразделение уже назначены другие групповые политики, то они и их приоритет будут отображены в блоке **Групповые политики, ранее назначенные на подразделения**.

Если каждая из групповых политик, назначенных одному подразделению, задает непересекающийся набор параметров, то к подразделению применяются все параметры назначенных политик.

Если несколько политик, назначенных одному подразделению, то применяется алгоритм разрешения конфликтов (см. GP_sum).

Для применения изменений нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку подразделений нажать на кнопку закрытия.

Изменение приоритета и порядка наследования назначенной групповой политики

Изменение приоритета и порядка наследования назначенной на подразделение групповой политики осуществляется на карточке подразделения. Для открытия карточки необходимо на вкладке **Подразделения** нажать на соответствующее подразделение.

Изменение приоритета определяет порядок применения групповых политик, т.е. какие настройки будут применены к объекту.

Для изменения приоритета применения групповой политики в поле **Приоритет групповой политики** задать новое значение.

Флаг **Наследовать принудительно** позволяет сделать наследование параметров соответствующего объекта обязательным для всех дочерних подразделений, даже если где-то наследование отключено. Связанные ГПО, отмеченные флагом **Принудительно**, применяются после обычных ГПО, поэтому переопределяют их значения.

Для включения принудительного наследования параметров ГПО, необходимо установить флаг **Наследовать принудительно**.

Для применения изменений нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку подразделений нажать на кнопку закрытия.

Удаление назначения групповой политики на подразделение

Удаление назначения групповой политики на подразделение выполняется путем удаления подразделения из списка.

Удалить подразделение или одновременно несколько подразделений из списка можно, отметив требуемые подразделения и нажав кнопку **[Удалить]**.

Чтоб отметить все имеющиеся подразделения — отметить пункт **Название подразделения**.

Также удалить назначение групповой политики можно на карточке подразделения. Для открытия карточки на вкладке **Подразделения** нажать на соответствующее подразделение, затем на карточке нажать кнопку **[Удалить подразделение]**. После подтверждения удаления будет выполнен переход к списку подразделений.

10.1.4. Удаление групповой политики

Удаления групповой политики осуществляется из ее карточки на вкладке **Основное**. Для открытия карточки необходимо в списке групповых политик нажать на политику. Затем на карточке нажать кнопку **[Удалить групповую политику]**. После подтверждения удаления будет выполнен переход к списку групповых политик.

10.2. Политики доступа к узлу

В подразделе, на соответствующих вкладках, выполняется настройка правил доступа пользователей к компьютерам с использованием определенных служб HBAC (Host-based access control) FreeIPA.

10.2.1. Правила НВАС

На вкладке Правила НВАС выполняется создание, настройка и удаление правил НВАС, а также определяется порядок их применения.

10.2.1.1. Список правил НВАС

На вкладке приведен список правил НВАС с указанием имени правила, его состояния и описания.

В списке доступен поиск по имени или описанию правила. Для этого в поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Для просмотра информации о правиле НВАС нажать на соответствующее правило в списке. Будет открыта карточка правила НВАС.

В левом нижнем углу указано количество правил НВАС, а в правом нижнем углу кнопки переключения страниц.

10.2.1.2. Создание нового правила НВАС

Для создания нового правила необходимо нажать на кнопку **[Новое правило]**, будет выполнен переход на карточку нового правила.

На карточке на вкладке **Основное** заполнить обязательное поле **Имя правила**.
Остальные вкладки станут доступны для заполнения после сохранения правила (см. [Управление правилом НВАС](#)).

Важно: В имени правила можно использовать a-z, A-Z, 0-9, -_

Для сохранения нового правила необходимо нажать на кнопку сохранения в правом верхнем углу. Будет выполнен переход к карточке управления правилом.

Для закрытия карточки и возврата к списку правил нажать на кнопку закрытия.

10.2.1.3. Управление правилом НВАС

Управление правилом НВАС выполняется на его карточке. Для открытия карточки необходимо на вкладке **Правила НВАС** нажать на соответствующее правило в списке.

На карточке управление правилом НВАС осуществляется на вкладках:

- **Основное;**
- **Пользователи;**
- **Компьютеры;**
- **Службы НВАС.**

Для закрытия карточки и возврата к списку правил нажать на кнопку закрытия.

Основное

На вкладке отображается информация о правиле НВАС: его название, описание, а также состояние (включено/выключено).

Описание правила доступно для редактирования.

Для включения или выключения правила НВАС отметить, соответственно, **Включено** или **Выключено**.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

Пользователи

На вкладке настраивается каким категориям пользователей разрешено запускать службы НВАС из данного правила.

Список служб НВАС, которые будет разрешено запускать, настраивается на вкладке [Службы НВАС](#).

Список компьютеров, на которых будет разрешено запускать службы, настраивается на вкладке [Компьютеры](#).

Для разрешения всем пользователям запускать службы НВАС из данного правила

необходимо в поле **Категория пользователей, к которой применяется правило** выбрать значение **Любой пользователь**.

Для разрешения отдельным пользователям и группам пользователей запускать службы НВАС из данного правила необходимо в поле **Категория пользователей, к которой применяется правило** выбрать значение **Указанные пользователи и группы** (при создании правила значение по умолчанию).

Для выбора пользователей, которым будет разрешено запускать службы НВАС из данного правила, необходимо в блоке **Пользователи** в списке **Все пользователи** отметить требуемые записи и перенести их в список **Выбранные пользователи** нажатием кнопки [**<-**].

Для исключения пользователей необходимо в списке **Выбранные пользователи** отметить требуемые записи и перенести их в список **Все пользователи** нажатием кнопки [**->**].

Выбор и исключение групп пользователей выполняется в блоке **Группы пользователей** аналогично выбору/исключению пользователей.

Во всех списках доступен поиск по имени/должности(названию). Для этого в соответствующем поле поиска ввести значение от трех символов, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

Компьютеры

На вкладке настраивается на каких компьютерах разрешено запускать службы НВАС.

Список служб НВАС, которые будет разрешено запускать, настраивается на вкладке [Службы НВАС](#).

Список пользователей, которым будет разрешено запускать службы НВАС, настраивается на вкладке [Пользователи](#).

Для разрешения запускать службы НВАС из данного правила на всех компьютерах необходимо в поле **Категория пользователей, к которой применяется правило** выбрать значение **Любой компьютер**.

Для разрешения запускать службы НВАС из данного правила на отдельных компьютерах и группах компьютеров необходимо в поле **Категория компьютеров, к которой применяется правило** выбрать значение **Указанные компьютеры и группы** (при создании правила значение по умолчанию).

Для выбора компьютеров, на которых будет разрешено запускать службы НВАС из данного правила, необходимо в блоке **Компьютеры** в списке **Все компьютеры** отметить требуемые записи и перенести их в список **Выбранные компьютеры** нажатием кнопки [**<-**].

Для исключения компьютеров необходимо в списке **Выбранные компьютеры** отметить требуемые записи и перенести их в список **Все компьютеры** нажатием кнопки [**->**].

Выбор и исключение групп компьютеров выполняется в блоке **Группы компьютеров** аналогично выбору/исключению компьютеров.

Во всех списках доступен поиск по имени(названию). Для этого в соответствующем поле поиска ввести значение от трех символов, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

Службы НВАС

На вкладке настраивается какие службы НВАС разрешает запускать данное правило.

Список пользователей, которым будет разрешено запускать службы НВАС, настраивается на вкладке *Пользователи*.

Список компьютеров, на которых будет разрешено запускать службы, настраивается на вкладке *Компьютеры*.

Для разрешения запускать все службы НВАС необходимо в поле **Категория служб, к которой применяется правило** выбрать значение **Любая служба**.

Для разрешения запускать отдельные службы НВАС и группы служб необходимо в поле **Категория служб, к которой применяется правило** выбрать значение **Указанные службы и группы** (при создании правила значение по умолчанию).

Для выбора служб НВАС, которые будет разрешено запускать, необходимо в блоке **Службы** в списке **Все службы** отметить требуемые записи и перенести их в список **Выбранные службы** нажатием кнопки [**<-**].

Для исключения служб НВАС необходимо в списке **Выбранные службы** отметить требуемые записи и перенести их в список **Все службы** нажатием кнопки [**->**].

Выбор и исключение групп служб выполняется в блоке **Группы служб** аналогично выбору/исключению служб НВАС.

Список служб НВАС настраивается на вкладке *Службы НВАС* (подраздел *Политики доступа к узлу*).

Список групп служб настраивается на вкладке *Группы служб НВАС* (подраздел *Политики доступа к узлу*).

Во всех списках доступен поиск по имени(названию). Для этого в соответствующем поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

10.2.1.4. Удаление правила НВАС

Для удаления правила НВАС или одновременно несколько правил НВАС необходимо на вкладке **Правила НВАС** в списке отметить требуемые правила и нажать кнопку [**Удалить**].

Чтоб отметить все имеющиеся правила — отметить пункт **Имя правила**.

Также удалить правило НВАС можно из его карточки: открыть карточку нажатием на правило в списке, затем на карточке нажать кнопку [**Удалить правило**]. После подтверждения удаления будет выполнен переход к списку правил.

10.2.2. Службы НВАС

На вкладке Службы НВАС осуществляется управление службами НВАС: создание, настройка и удаление служб НВАС.

10.2.2.1. Список служб НВАС

На вкладке приведен список служб с указанием имени службы и описания.

В списке доступен поиск по имени и описанию службы. Для этого в поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Для просмотра информации о службе нажать на соответствующую службу в списке. Будет открыта карточка службы с информацией о ней.

В левом нижнем углу указано количество служб.

10.2.2.2. Создание службы НВАС

Для создания новой службы необходимо нажать на кнопку **[Новая служба]**, будет выполнен переход на карточку новой службы.

На карточке заполнить обязательное поле **Имя службы**. Также можно добавить описание службы в соответствующем поле.

Важно: В имени службы можно использовать а - z, А - Z, 0 - 9, ! - _

Вкладка **Группы** станет доступна для заполнения после сохранения службы (см. [Управление службой НВАС](#)).

Для сохранения новой службы необходимо нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку служб нажать на кнопку закрытия.

10.2.2.3. Управление службой НВАС

Управление службой выполняется на ее карточке. Для открытия карточки необходимо на вкладке **Службы НВАС** нажать на соответствующую службу в списке.

На карточке управление службой осуществляется на вкладках:

- **Основное;**

- **Группы.**

На вкладке **Основное** отображается информация о службе: ее название и описание.

Для редактирования доступно описание службы.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

На вкладке **Группы** осуществляется добавление данной службы НВАС в состав групп служб.

Для выбора групп служб, в которые будет входить данная служба НВАС, необходимо в списке **Все группы** отметить требуемые записи и перенести их в список **Выбранные группы** нажатием кнопки [**<-**].

Для исключения данной службы НВАС из групп служб необходимо в списке **Выбранные группы** отметить требуемые записи и перенести их в список **Все группы** нажатием кнопки [**->**].

Список групп служб задается на вкладке *Группы служб НВАС* (подраздел *Политики доступа к узлу*).

Во всех списках доступен поиск по названию. Для этого в поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку служб нажать на кнопку закрытия.

10.2.2.4. Удаление службы НВАС

Для удаления службы или одновременно несколько служб необходимо на вкладке **Службы НВАС** в списке отметить требуемые службы и нажать кнопку **[Удалить]**.

Чтоб отметить все имеющиеся службы — отметить пункт **Имя службы**.

Также удалить службу НВАС можно из ее карточки: открыть карточку нажатием на службу в списке служб, затем на карточке нажать кнопку **[Удалить службу]**. После подтверждения удаления будет выполнен переход к списку служб.

10.2.3. Группы служб НВАС

На вкладке осуществляется управление группами служб НВАС: создание, настройка и удаление групп служб НВАС.

10.2.3.1. Список групп служб НВАС

На вкладке приведен список групп служб с указанием имени группы и описания.

В списке доступен поиск по имени и описанию группы. Для этого в поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Для просмотра информации о группе служб нажать на соответствующую группу в списке. Будет открыта карточка группы служб с информацией о ней.

В левом нижнем углу указано количество групп служб.

10.2.3.2. Создание группы служб НВАС

Для создания новой группы служб необходимо нажать на кнопку **[Новая группа]**, будет выполнен переход на карточку новой группы.

На карточке заполнить обязательное поле **Имя группы**. Также можно добавить описание группы в соответствующем поле.

Важно: В имени группы можно использовать а - z, А - Z, 0 - 9, - _

Вкладка **Службы** станет доступна для заполнения после сохранения группы (см. [Управление группой служб НВАС](#)).

Для сохранения новой группы служб необходимо нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку групп нажать на кнопку закрытия.

10.2.3.3. Управление группой служб НВАС

Управление группой служб выполняется на ее карточке. Для открытия карточки необходимо на вкладке **Группы служб НВАС** нажать на соответствующую группу в списке.

На карточке управление группой служб осуществляется на вкладках:

- **Основное;**
- **Службы.**

На вкладке **Основное** отображается информация о группе служб: ее название и описание.

Для редактирования доступно описание группы.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

На вкладке **Службы** осуществляется добавление служб НВАС в состав данной группы служб.

Для добавления служб НВАС в состав данной группы необходимо в списке **Все службы** отметить требуемые записи и перенести их в список **Выбранные службы** нажатием кнопки [**<-**].

Для исключения служб НВАС из состава данной группы необходимо в списке **Выбранные службы** отметить требуемые записи и перенести их в список **Все службы** нажатием кнопки [**->**].

Список служб НВАС задается на вкладке [Службы НВАС](#) (подраздел [Политики доступа к узлу](#)).

Во всех списках доступен поиск по названию. Для этого в поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку групп служб нажать на кнопку закрытия.

10.2.3.4. Удаление группы служб НВАС

Для удаления группы служб или одновременно несколько групп необходимо на вкладке **Группы служб НВАС** в списке отметить требуемые группы и нажать кнопку **[Удалить]**.

Чтоб отметить все имеющиеся группы — отметить пункт **Имя группы**.

Также удалить группу служб можно из ее карточки: открыть карточку нажатием на группу служб в списке групп, затем на карточке нажать кнопку **[Удалить группу]**. После подтверждения удаления будет выполнен переход к списку групп.

10.3. Политики повышения привилегий

С помощью политик повышения привилегий (возможностей при администрировании) доступна возможность предоставления возможности обычным пользователям выполнять конкретные команды на целевом компьютере с привилегиями root-пользователя (или конкретного пользователя).

Повышение возможностей при администрировании работает через sssd-службу, которая в момент выполнения команды sudo запрашивает правила из LDAP-каталога.

10.3.1. Правила Sudo

На вкладке выполняется создание, настройка и удаление правил выполнения команд sudo, а также определяется порядок их применения.

10.3.1.1. Список правил sudo

Вкладка содержит правила для выполнения команд sudo.

В списке доступен поиск по имени и описанию правила. Для этого в поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

В списке доступна фильтрация по значению **Состояние**, для этого необходимо нажать на значок фильтра рядом с названием столбца и отметить требуемые значения для фильтрации.

10.3.1.2. Создание правила sudo

Для создания правила sudo нажать кнопку **[Новое правило]**, будет выполнен переход на карточку нового правила.

На карточке на вкладке **Основное** заполнить обязательное поле **Имя правила**.

Важно: В имени правила можно использовать a - z, A - Z, 0 - 9, - _

Остальные вкладки станут доступны после сохранения правила (см. [Редактирование правила sudo](#)).

Для сохранения правила sudo нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку правил sudo нажать на кнопку закрытия.

10.3.1.3. Редактирование правила sudo

Редактирование правила sudo осуществляется на его карточке. Для перехода на карточку необходимо нажать на правило sudo в списке.

На карточке информация о правиле sudo размещается на вкладках:

- **Основное;**
- **Параметры;**
- **Пользователи;**
- **Компьютеры;**
- **Команды Sudo;**
- **Запуск от имени.**

Для закрытия карточки правила sudo и возврата к списку нажать на кнопку закрытия.

Основное. Управление состоянием правила

На вкладке указана основная информация о правиле sudo: имя правила, описание и состояние.

Для редактирования доступно описание правила и порядок его выполнения.

Для включения или выключения правила, соответственно, установить флаг **Включено** или **Выключено**.

Для применения внесенных изменений нажать на кнопку сохранения в правом верхнем углу.

Параметры

На вкладке приведен список параметров правила sudo.

В списке доступен поиск, для этого в верхнем левом углу вкладки в поле поиска ввести значение.

Для добавления нового параметра нажать кнопку **[Новый параметр]**, будет открыта карточка нового параметра. В карточке необходимо указать добавляемый параметр.

Для сохранения параметра нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку параметров нажать на кнопку закрытия.

Для удаления параметра правила или одновременно несколько параметров необходимо отметить параметр в списке и нажать кнопку **[Удалить параметр]**.

Пользователи

На вкладке настраивается каким категориям пользователей разрешено/запрещено выполнение команд sudo из данного правила.

Список разрешенных/запрещенных команд sudo настраивается на вкладке [Команды Sudo](#).

Список компьютеров, на которых разрешено/запрещено выполнять команды sudo, настраивается на вкладке [Компьютеры](#).

Для разрешения всем пользователям выполнять команды sudo из данного правила необходимо в поле **Категория пользователей, к которой применяется правило** выбрать значение **Любой пользователь**.

Для разрешения отдельным пользователям и группам пользователей выполнять команды sudo из данного правила необходимо в поле **Категория пользователей, к которой**

применяется правило выбрать значение **Указанные пользователи и группы** (при создании правила значение по умолчанию).

Для выбора пользователей, которым будет разрешено выполнять команды sudo из данного правила, необходимо в блоке **Пользователи** в списке **Все пользователи** отметить требуемые записи и перенести их в список **Выбранные пользователи** нажатием кнопки [**<-**].

Для исключения пользователей необходимо в списке **Выбранные пользователи** отметить требуемые записи и перенести их в список **Все пользователи** нажатием кнопки [**->**].

Выбор и исключение групп пользователей выполняется в блоке **Группы пользователей** аналогично выбору/исключению пользователей.

Во всех списках доступен поиск по имени/должности(названию). Для этого в соответствующем поле поиска ввести значение от трех символов, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

Компьютеры

На вкладке настраивается на каких компьютерах разрешено/запрещено выполнение команд sudo.

Список разрешенных/запрещенных команд sudo настраивается на вкладке *Команды Sudo* .

Список пользователей, которым разрешено/запрещено выполнять команды sudo, настраивается на вкладке *Пользователи*.

Для разрешения выполнять команды sudo из данного правила на всех компьютерах необходимо в поле **Категория компьютеров, к которой применяется правило** выбрать значение **Любой компьютер**.

Для разрешения выполнять команды sudo из данного правила на отдельных компьютерах и группах компьютеров необходимо в поле **Категория компьютеров, к которой применяется правило** выбрать значение **Указанные компьютеры и группы** (при создании правила значение по умолчанию).

Для выбора компьютеров, на которых будет разрешено выполнять команды sudo из данного правила, необходимо в блоке **Компьютеры** в списке **Все компьютеры** отметить требуемые записи и перенести их в список **Выбранные компьютеры** нажатием кнопки [**<-**].

Для исключения компьютеров необходимо в списке **Выбранные компьютеры** отметить требуемые записи и перенести их в список **Все компьютеры** нажатием кнопки [**->**].

Выбор и исключение групп компьютеров выполняется в блоке **Группы компьютеров** аналогично выбору/исключению компьютеров.

Во всех списках доступен поиск по имени(названию). Для этого в соответствующем поле поиска ввести значение от трех символов, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

Команды Sudo

На вкладке настраивается какие команды sudo разрешено/запрещено выполнять.

Список пользователей, которым разрешено/запрещено выполнять команды sudo, настраивается на вкладке *Пользователи*.

Список компьютеров, на которых разрешено/запрещено выполнять команды sudo, настраивается на вкладке *Компьютеры*.

Для разрешения выполнять все команды sudo необходимо в поле **Категория команд, к которой применяется правило** выбрать значение **Любая команда**.

Для разрешения выполнять отдельные команды sudo и группы команд необходимо в поле **Категория команд, к которой применяется правило** выбрать значение **Указанные команды и группы** (при создании правила значение по умолчанию).

Для выбора команд sudo, которые будет разрешено выполнять, необходимо в блоке **Разрешенные команды** в списке **Все команды** отметить требуемые записи и перенести их в список **Выбранные команды** нажатием кнопки [**<-**].

Для исключения команд из списка разрешенных необходимо в списке **Выбранные**

команды отметить требуемые записи и перенести их в список **Все команды** нажатием кнопки **[->]**.

Выбор и исключение разрешенных групп команд sudo выполняется аналогично выбору и исключению команд sudo.

Для выбора команд sudo, которые будет запрещено выполнять, необходимо в блоке **Запрещенные команды** в списке **Все команды** отметить требуемые записи и перенести их в список **Выбранные команды** нажатием кнопки **[<-]**.

Для исключения команд из списка запрещенных необходимо в списке **Выбранные команды** отметить требуемые записи и перенести их в список **Все команды** нажатием кнопки **[->]**.

Выбор и исключение запрещенных групп команд sudo выполняется аналогично выбору и исключению команд sudo.

Команды, выполняемые с sudo, добавляются на вкладке *Команды Sudo* (подраздел *Политики повышения привилегий*).

Группы команд, выполняемых с sudo, настраиваются на вкладке *Группы команд Sudo* (подраздел *Политики повышения привилегий*).

Во всех списках доступен поиск по имени. Для этого в соответствующем поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

Запуск от имени

На вкладке дополнительно настраиваются права выполнения команд sudo из данного правила от имени другого пользователя.

Для разрешения выполнять команды sudo из данного правила от имени любого пользователя необходимо в поле **Категория запуска от имени пользователей, к которой применяется правило** выбрать значение **Любой пользователь**.

Для разрешения выполнять команды sudo из данного правила от имени определенных пользователей и групп пользователей необходимо в поле **Категория запуска от имени**

пользователей, к которой применяется правило выбрать значение **Указанные пользователи и группы** (при создании правила значение по умолчанию).

Если на вкладке выбран пункт **Указанные пользователи и группы**, но пользователи и группы не выбраны, то команды sudo из данного правила возможно будет выполнять только от имени суперпользователя root.

Для выбора пользователей, от имени которых будет разрешено выполнять команды sudo из данного правила, необходимо в блоке **От имени пользователей** в списке **Все пользователи** отметить требуемые записи и перенести их в список **Выбранные пользователи** нажатием кнопки [**<-**].

Для исключения пользователей необходимо в списке **Выбранные пользователи** отметить требуемые записи и перенести их в список **Все пользователи** нажатием кнопки [**->**].

Для добавления локального пользователя, от имени которого будет разрешено выполнять команды sudo из данного правила, необходимо в поле **Имя локального пользователя** ввести имя локальной учетной записи пользователя и нажать кнопку [**Добавить**].

Для исключения локального пользователя необходимо нажать кнопку [**Удалить**] рядом с соответствующей учетной записью.

Выбор и исключение групп пользователей выполняется в блоке **От имени группы пользователей** аналогично выбору и исключению пользователей.

Во всех списках доступен поиск по имени(названию). Для этого в соответствующем поле поиска ввести значение от трех символов, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

10.3.1.4. Удаление правила sudo

Для удаления правила sudo или одновременно нескольких правил sudo необходимо на вкладке **Правила Sudo** отметить правило в списке и нажать кнопку [**Удалить**].

Чтоб отметить все имеющиеся правила — отметить пункт **Имя правила**.

Также удалить правило sudo можно из его карточки: открыть карточку нажатием на

правило sudo в списке, затем на карточке на вкладке **Основное** нажать кнопку **[Удалить правило]**. После подтверждения удаления будет выполнен переход к списку правил sudo.

10.3.2. Команды Sudo

На вкладке осуществляется управление командами, выполняемыми с sudo.

10.3.2.1. Список команд sudo

На вкладке приведен список команд, выполняемых с sudo.

В списке доступен поиск по имени или описанию команды. Для этого в поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Внизу списка указано количество записей в списке.

10.3.2.2. Добавление команды

Для добавления команды нажать кнопку **[Новая команда]**, будет выполнен переход на карточку новой команды.

На карточке на вкладке **Основное** заполнить обязательное поле **Команда Sudo**.

Важно: В имени команды можно использовать a-z, A-Z, 0-9, -_./~ и пробелы (кроме первого и последнего)

Вкладка **Группы** станет доступна после сохранения команды (см. [Редактирование команды](#)).

Для сохранения команды sudo нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку команд sudo нажать на кнопку закрытия.

10.3.2.3. Редактирование команды

Редактирование команды sudo осуществляется на ее карточке. Для перехода на карточку необходимо нажать левой кнопкой мыши на команду sudo в списке.

На карточке информация о команде sudo размещается на вкладках:

- **Основное;**
- **Группы.**

Для закрытия карточки команды sudo и возврата к списку нажать на кнопку закрытия.

Основное

На вкладке указана команда и ее описание. Описание команды можно изменить.

Для применения внесенных изменений нажать на кнопку сохранения в правом верхнем углу.

Группы

На вкладке задаются группы команд, в состав которых будет входить данная команда.

Для выбора групп команд, в которые будет включена данная команда sudo, необходимо в списке **Все группы** отметить требуемые записи и перенести их в список **Выбранные группы** нажатием кнопки [**<-**].

Для исключения данной команды sudo из групп команд необходимо в списке **Выбранные группы** отметить требуемые записи и перенести их в список **Все группы** нажатием кнопки [**->**].

Список групп команд sudo задается на вкладке *Группы команд Sudo* (подраздел *Политики повышения привилегий*).

Во всех списках доступен поиск по имени. Для этого в соответствующем поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем

углу.

Для закрытия карточки и возврата к списку команд нажать на кнопку закрытия.

10.3.2.4. Удаление команды sudo

Команду sudo или одновременно несколько команд sudo можно удалить. Для этого необходимо выделить команду sudo в списке и нажать кнопку **[Удалить]**.

Также удалить команду sudo можно из ее карточки: открыть карточку нажатием на команду в списке, затем на карточке на вкладке **Основное** нажать кнопку **[Удалить команду]**. После подтверждения удаления будет выполнен переход к списку команд sudo.

Если команда входит в состав правила sudo, то появится соответствующее сообщение об ошибке и команда не будет удалена.

10.3.3. Группы команд Sudo

На вкладке осуществляется управление группами команд, выполняемых с sudo.

10.3.3.1. Список групп команд

На вкладке приведен список групп команд, выполняемых с sudo.

В списке доступен поиск по имени или описанию группы. Для этого в поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Внизу списка указано количество записей в списке.

10.3.3.2. Добавление группы команд

Для добавления группы команд sudo нажать кнопку **[Новая группа]**, будет выполнен переход на карточку новой группы.

На карточке на вкладке **Основное** заполнить обязательное поле **Имя группы**.

Важно: В имени группы можно использовать a - z, A - Z, 0 - 9, - _

Вкладка **Команды** станет доступна после сохранения группы команды (см. *Редактирование группы команд*).

Для сохранения группы команд sudo нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку групп команд sudo нажать на кнопку закрытия.

10.3.3.3. Редактирование группы команд

Редактирование группы команд sudo осуществляется на ее карточке. Для перехода на карточку необходимо нажать на группу команд sudo в списке.

На карточке информация о группе команд sudo размещается на вкладках:

- **Основное;**
- **Команды.**

Для закрытия карточки группы команд sudo и возврата к списку нажать на кнопку закрытия.

Основное

На вкладке указано имя группы команд и ее описание. Описание группы команд можно изменить.

Для применения внесенных изменений нажать на кнопку сохранения в правом верхнем углу.

Команды

На вкладке задаются команды, которые будут входить в состав данной группы.

Для добавления команд sudo в состав данной группы необходимо в списке **Все команды** отметить требуемые записи и перенести их в список **Выбранные команды** нажатием кнопки [**<-**].

Для исключения команд из состава данной группы необходимо в списке **Выбранные команды** отметить требуемые записи и перенести их в список **Все команды** нажатием кнопки **[->]**.

Список команд sudo задается на вкладке *Команды Sudo* (подраздел *Политики повышения привилегий*).

Во всех списках доступен поиск по имени. Для этого в соответствующем поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку групп команд sudo нажать на кнопку закрытия.

10.3.3.4. Удаление группы команд

Группу команд sudo или одновременно несколько групп команд sudo можно удалить. Для этого необходимо выделить группу команд sudo в списке и нажать кнопку **[Удалить]**.

Также удалить группу команд sudo можно из ее карточки: открыть карточку нажатием на группу команд sudo в списке, затем на карточке на вкладке **Основное** нажать кнопку **[Удалить группу]**. После подтверждения удаления будет выполнен переход к списку групп команд sudo.

10.4. Политики паролей

В подразделе осуществляется управление политиками паролей: создание, настройка и удаление политик.

10.4.1. Список политик паролей

В подразделе приведен список политик паролей с указанием наименования группы пользователей, для которой применяется политика паролей, и приоритета применения политики.

В списке доступен поиск по наименованию группы пользователей. Для этого в поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Внизу списка указано количество записей в списке.

10.4.2. Создание политики паролей

Для создания новой политики паролей нажать кнопку **[Новая политика паролей]**, будет выполнен переход на карточку новой политики.

На карточке из выпадающего списка **Наименование группы пользователей** выбрать группу пользователей, для которой будет применяться политика паролей, а в поле **Приоритет** задать приоритет применения данной политики. Приоритет политики паролей должен быть уникальным числом.

После сохранения политики паролей станут доступны для заполнения дополнительные атрибуты (см. [Редактирование политики паролей](#)).

Для сохранения политики паролей нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку политик паролей нажать на кнопку закрытия.

10.4.3. Редактирование политики паролей

Редактирование политики паролей осуществляется на ее карточке. Для перехода на карточку необходимо нажать на наименование группы пользователей в списке.

На карточке политики паролей для редактирования доступны поля:

- **Приоритет** — приоритет применения политики;
- **Максимальный срок действия (в днях)** — максимальный срок действия пароля пользователя;
- **Минимальный срок действия (в часах)** — минимальный срок действия пароля пользователя;
- **Размер журнала (количество паролей)** — количество сохраняемых предыдущих паролей;
- **Классы символов** — требование по сложности пароля, указывающее сколько разных классов символов должно быть использовано в пароле, доступны значения от

0 до 5;

- **Минимальная длина** — минимальное количество символов в пароле;
- **Максимальное количество ошибок** — количество неудачных попыток ввода пароля, по достижении которого учетная запись блокируется;
- **Интервал сброса ошибок (в секундах)** — интервал времени, по прошествии которого счетчик количества неудачных попыток ввода пароля сбрасывается в 0;
- **Длительность блокировки (в секундах)** — интервал времени, по прошествии которого заблокированная учетная запись будет разблокирована.

Классы символов включают в себя:

- цифры,
- буквы нижнего регистра,
- буквы верхнего регистра,
- символы UTF-8,
- остальные символы.

По умолчанию нет требований по сложности пароля, значение классов символов равно 0. Значения от 1 до 5 означают, сколько классов символов должно быть использовано в пароле.

Важно: При использовании одного и того же символа более двух раз подряд сложность пароля будет занижена на один балл.

Для применения внесенных изменений нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки политики паролей и возврата к списку нажать на кнопку закрытия.

10.4.4. Удаление политики паролей

Политику паролей или одновременно несколько политик паролей, применяемых к группе пользователей, можно удалить. Для этого необходимо отметить соответствующее наименование группы пользователей в списке и нажать кнопку **[Удалить]**.

Также удалить политику паролей можно из ее карточки: открыть карточку нажатием на

наименование группы пользователей в списке, затем на карточке нажать кнопку **[Удалить политику паролей]**. После подтверждения удаления будет выполнен переход к списку.

Установка и обновление ПО

В разделе осуществляется управление группами и репозиториями программного обеспечения (ПО), а также журналом заданий.

11.1. Политики ПО

В подразделе выполняется настройка политик установки и обновления программного обеспечения (ПО).

11.1.1. Список политик ПО

В подразделе приведен список политик ПО с указанием имени политики, версии, даты изменения и автора изменения.

В списке доступен поиск, для этого в поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

В левом нижнем углу указано количество записей, а в правом нижнем углу кнопки переключения страниц.

11.1.2. Создание политики ПО

Для создания новой политики ПО необходимо нажать на кнопку **[Новая политика ПО]**. Будет выполнен переход на карточку новой политики.

На карточке на вкладке **Основное** задать имя политики ПО. Также можно указать описание политики.

Остальные вкладки станут доступны после сохранения политики (см. [Настройка политики ПО](#)).

Для сохранения новой политики ПО необходимо нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку политик ПО нажать на кнопку закрытия.

11.1.3. Настройка политики ПО

Настройка политики ПО выполняется на ее карточке. Для открытия карточки необходимо в списке политик ПО нажать на соответствующую политику ПО.

Важно: При внесении изменений в настройку политики ПО, ее версия меняется автоматически.

На карточке политики ПО представлены следующие вкладки:

- **Основное;**
- **Конфигурация политики;**
- **Каталог ПО;**
- **Подразделения.**

Для закрытия карточки и возврата к списку политик ПО нажать на кнопку закрытия.

11.1.3.1. Основное

На вкладке **Основное** приведена основная информация о политике ПО: имя политики (например, *Установка Chromium*), ее описание, даты создания и изменения, версия политики и автор последнего изменения. Поле **Описание** доступно для редактирования.

Для сохранения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

11.1.3.2. Конфигурация политики

На вкладке **Конфигурация политики** приведен список ПО, которое входит состав данной политики ПО.

В списке доступен поиск, для этого в поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

При нажатии на ПО в списке будет выполнен переход на вкладку *Каталог ПО* к форме настройки данного ПО.

Для удаления ПО из состава данной политики необходимо в списке отметить требуемое наименование ПО и нажать кнопку **[Удалить]**.

Важно: При удалении ПО из состава политики стандартным поведением ПО на устройстве будет удаление, независимо от того, каким образом было установлено ПО - через политики ПО или вручную. У ОС нет возможности определять способ установки ПО и удалять через состав политики ПО только то ПО, что было установлено через политику.

Чтобы отметить все записи — отметить пункт **Наименование ПО**.

В левом нижнем углу указано количество записей, а в правом нижнем углу кнопки переключения страниц.

11.1.3.3. Каталог ПО

На вкладке **Каталог ПО** настраивается ПО, которое будет входить в состав данной политики ПО.

ПО сгруппировано по разделам. Формирование разделов ПО и добавление ПО в разделы осуществляется в подразделе *Каталог ПО* (раздел *Установка и обновление ПО*).

Для поиска раздела ПО или ПО начать вводить в поле поиска название, результат поиска будет выводиться по мере ввода.

Для раскрытия раздела ПО нажать на соответствующий раздел.

При выборе ПО будет отображена форма **Настройка параметра**, в которой указываются значения параметров данного ПО. Параметры ПО задаются на карточке ПО в подразделе *Каталог ПО* (раздел *Установка и обновление ПО*). Например, для ПО Chromium указан параметр **Стартовая страница** со значением по умолчанию <https://yandex.ru>. Значения параметров, заданные по умолчанию, могут быть изменены для данной политики ПО.

Для добавления ПО в состав данной политики ПО необходимо нажать кнопку **[Применить]** в правом нижнем углу формы.

Если параметр составной, то для него доступна возможность продублировать все поля

параметров. Для этого необходимо нажать кнопку **[+]** справа от названия формы

Настройка параметра.

Для сохранения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

11.1.3.4. Подразделения

На вкладке настраивается список подразделений, к которым будет применена данная политика ПО.

Список подразделений

На вкладке приведен список подразделений, к которым применяется данная политика ПО, с указанием приоритета политики ПО.

В списке доступен поиск по названию подразделения. Для этого в поле поиска ввести значение поиска от трех символов, результат поиска будет выводиться по мере ввода.

В левом нижнем углу указано количество записей, а в правом нижнем углу кнопки переключения страниц.

Назначение политики ПО на подразделение

Для назначения на подразделение политики ПО с заданными параметрами нажать кнопку **[Добавить подразделение]**, будет выполнен переход на карточку выбора нового подразделения.

На карточке необходимо выбрать подразделение, на которое будет назначена данная политика ПО, а также приоритет применения политики. Поле **Расположение подразделения в организационной структуре** заполняется автоматически при выборе подразделения.

На одно подразделение может быть назначено несколько политик ПО, но с разным приоритетом — приоритет должен быть уникальным числовым значением.

Если на выбранное подразделение уже назначены другие политики ПО, то они и их приоритет будут отображены в блоке **Назначенные ПО на подразделение**.

Для применения изменений нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку подразделений нажать на кнопку закрытия.

Назначение политики ПО на компьютеры и группы компьютеров

Для назначения политики ПО с заданными параметрами на компьютер, либо на группу компьютеров нажать кнопку **[Добавить подразделение]**, после чего будет выполнен переход на карточку выбора нового подразделения.

На карточке в выпадающем списке **Название подразделения** необходимо выбрать корневой каталог подразделения домена, после чего ниже отобразится форма выбора компьютеров и групп компьютеров, на которые необходимо установить ПО. Поле **Расположение подразделения в организационной структуре** заполняется автоматически при выборе подразделения.

Для выбора компьютеров, на которые необходимо установить ПО, в блоке **Установить на компьютеры** в списке **Все компьютеры** отметить требуемые записи и перенести их в список **Выбранные компьютеры** нажатием кнопки **[<-]**.

Для исключения компьютеров из списка выбранных необходимо в списке **Выбранные компьютеры** отметить требуемые записи и перенести их в список **Все компьютеры** нажатием кнопки **[->]**.

Выбор группы компьютеров выполняется в блоке **Установить на группу компьютеров** аналогично выбору отдельных компьютеров.

Важно: При установке ПО на компьютеры/группу компьютеров возможно возникновение ошибки, связанной с распространением source-листов на целевых рабочих станциях. Для устранения данной проблемы необходимо через выполнение задания автоматизации передать на рабочие станции необходимые конфигурации, а именно:

- На портале управления перейти на карточку **Задания автоматизации** (раздел [Управление доменом](#) — подраздел [Каталог заданий автоматизации](#)). На карточке, в таблице **Каталог дополнительных заданий** выбрать корневой каталог **Дополнительные настройки** и нажать появившуюся кнопку **[+ Новое задание]**;
- В открывшемся окне, на вкладке **Основное**, в поле **Название задания** ввести наименование задания, например *gero*, в поле **Уникальный идентификатор** ввести

значение идентификатора, например *repo*, после чего нажать кнопку сохранения;

- После успешного создания задания вкладка **Конфигурация скрипта** станет активной, нужно перейти на эту вкладку и нажать кнопку **[Редактировать файл]**;
- В поле **Редактировать скрипт вручную** добавить следующие данные:

```
repo:
  cmd.run:
    - name: |
        echo -e "deb http://repo.alldpro.ru/repos/astra/1 1.7_x86-64 main
↵contrib non-free" | sudo tee /etc/apt/sources.list.d/repo_alldpro.list
        apt update
    - failhard: True
```

где `http://repo.alldpro.ru/repos/astra/1 1.7_x86-64 main contrib non-free`
- путь до репозитория.

Затем в поле **Комментарий** указать любой комментарий и нажать кнопку сохранения;

- После успешного добавления задания перейти на вкладку **Каталог заданий автоматизации** (раздел [Автоматизация](#) — подраздел [Задания автоматизации](#)). На вкладке выбрать корневой каталог **Дополнительные настройки**. В открывшемся дереве найти созданное задание, например *repo* и нажать появившуюся кнопку **[Запустить задание]**;
- В открывшемся окне выбрать компьютер, группу компьютеров или подразделение, которому необходимо добавить задание и нажать кнопку сохранения;
- После успешного окончания работы задания на вкладке **Журнал заданий** (раздел [Автоматизация](#) — подраздел [Задания автоматизации](#)) в таблице, в строке с этим заданием, в столбце статус будет значение **Успешно**;
- Выполнить операцию по установке ПО на компьютеры, либо группы компьютеров.

Изменение приоритета назначенной политики ПО

Изменение приоритета назначенной на подразделение политики ПО осуществляется на карточке подразделения. Для открытия карточки необходимо на вкладке **Подразделения** нажать на соответствующее подразделение.

Для изменения приоритета применения политики ПО в поле **Приоритет политики ПО** задать новое значение.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку подразделений нажать на кнопку закрытия.

Отмена назначения политики ПО на подразделение

Отмена назначения на подразделение политики ПО выполняется путем удаления подразделение из списка.

Для удаления подразделения или одновременно нескольких подразделений из списка необходимо отметить требуемые подразделения и нажать кнопку **[Удалить]**.

Чтобы отметить все записи — отметить пункт **Наименование подразделения**.

Также удалить подразделение можно из карточки подразделения: в списке подразделений нажать на соответствующее подразделение, затем на карточке нажать кнопку **[Удалить подразделение]**. После подтверждения удаления будет выполнен переход к списку подразделений.

11.1.4. Применение политики ПО

11.1.4.1. Установка ПО

Установка ПО согласно политики осуществляется по PULL-модели, т.е. после сохранения параметров политики ПО запускается один из следующих сценариев:

- если компьютер, к которому применяется политика, выключен (находится не в сети), то он получит список ПО, которое должно быть установлено/обновлено, сразу после включения (появления в сети);
- если компьютер, к которому применяется политика, в сети, он получает список ПО, которое должно быть установлено/обновлено, каждые 30 минут.

На компьютере ПО будет установлено автоматически после успешного применения данной политики ПО.

Для корректного применения назначенных политик ПО на доменном компьютере, информация о репозитории должна содержаться в Source list компьютера.

11.1.5. Дополнительные настройки установки ПО

11.1.5.1. Обновление ПО

Обновление версии ПО, участвующего в политиках, осуществляется на вкладке **Пакеты** подраздела *Каталог ПО* (раздел *Установка и обновление ПО*).

Обновление ПО осуществляется путем замены пакета ПО на более актуальную версию пакета ПО, доступную в репозитории ПО. При этом обновление соответствующей политики ПО не требуется.

11.1.6. Удаление политики ПО

Удаления политики ПО выполняется из ее карточки: открыть карточку, нажав в списке политик ПО на соответствующую политику, затем на карточке на вкладке **Основное** нажать кнопку **[Удалить политику]**. После подтверждения удаления будет выполнен переход к списку политик ПО.

11.2. Каталог ПО

В подразделе выполняются функции управления программным обеспечением (ПО): добавление и удаление пакетов ПО, настройка шаблонов конфигурации и параметров ПО, создание структуры хранения пакетов ПО (добавление разделов хранения ПО).

11.2.1. Каталог программного обеспечения

На странице подраздела отображается **Каталог программного обеспечения**. В каталоге представлено ПО, добавленное в ALD Pro. ПО может быть сгруппировано по разделам. Для раскрытия раздела ПО необходимо нажать на соответствующий раздел в структуре каталога.

В каталоге доступен поиск ПО или раздела ПО, для этого начать вводить в поле поиска название, результат поиска будет выводиться по мере ввода.

При выборе в каталоге раздела ПО будет отображена форма **Объекты**, в которой приводится список входящих в состав выбранного раздела объектов (ПО и других

разделов). В списке доступен поиск по названию и типу объекта, для этого вверху формы в поле поиска ввести значение. Внизу формы отображено количество объектов, входящих в выбранный раздел.

При выборе в каталоге программного обеспечения будет отображена форма **Пакеты**, в которой приводится список входящих в выбранное ПО пакетов. В списке доступен поиск по названию и версии пакета, для этого вверху формы в поле поиска ввести значение. Внизу формы отображено количество пакетов, входящих в выбранное программное обеспечение.

11.2.2. Создание раздела ПО

Для создания раздела ПО необходимо нажать кнопку **[Раздел ПО]**. Будет открыта карточка создания нового раздела.

Раздел ПО можно создать внутри другого раздела. Внутри ПО невозможно создать раздел ПО.

На карточке раздела ПО на вкладке **Основное** необходимо заполнить обязательные поля **Наименование раздела** (например, *Браузеры*) и **Родительский раздел каталога ПО**. По умолчанию в качестве родительского раздела указан раздел, из которого была открыта карточка создания нового раздела. Также на карточке можно заполнить поле **Описание**.

Вкладка **Программное обеспечение** станет доступна для редактирования после сохранения раздела ПО (см. [Редактирование раздела ПО](#)).

Для сохранения раздела ПО нажать на кнопку сохранения. Будет выполнен переход к каталогу программного обеспечения.

Для закрытия карточки создания раздела ПО и возврата к каталогу программного обеспечения нажать на кнопку закрытия.

11.2.3. Редактирование раздела ПО

Редактирование раздела ПО осуществляется на его карточке. Для перехода на карточку необходимо в каталоге выбрать требуемый раздел ПО и нажать кнопку **[Редактировать]**. Будет открыта карточка редактирования раздела ПО.

Карточка раздела ПО состоит из вкладок:

- **Основное;**
- **Программное обеспечение.**

Для закрытия карточки раздела ПО и возврата к каталогу программного обеспечения нажать на кнопку закрытия.

11.2.3.1. Основное

На вкладке приведена основная информация о разделе ПО: наименование, имя родительского раздела и описание. Для редактирования доступны все поля.

Для сохранения изменений нажать на кнопку сохранения. Будет выполнен переход к каталогу программного обеспечения.

11.2.3.2. Программное обеспечение

На вкладке выполняется добавление и исключение ПО из данного раздела.

Для добавления ПО в данный раздел необходимо в списке **Все программное обеспечение** отметить ПО (например, *Chromium*) и перенести его в список **Выбранное программное обеспечение** нажатием кнопки [**<-**]. В списке **Все программное обеспечение** приведено ПО, которое не было добавлено ни в один раздел ПО.

Для исключения ПО из раздела необходимо в списке **Выбранное программное обеспечение** отметить требуемое ПО и перенести его в список **Все программное обеспечение** нажатием кнопки [**->**].

Во всех списках доступен поиск по наименованию. Для этого в соответствующем поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

11.2.4. Добавление ПО в каталог программного обеспечения

Новое ПО может быть добавлено в корень каталога ПО или в раздел ПО. Внутри ПО невозможно создать дочернее ПО.

Для добавления ПО необходимо нажать кнопку **[Программное обеспечение]**. Будет открыта карточка нового ПО.

На карточке на вкладке **Основное** необходимо заполнить обязательные поля **Наименование ПО** и **Родительский раздел каталога ПО**. По умолчанию в качестве родительского раздела будет указан раздел ПО, из которого была открыта карточка добавления нового ПО. Также можно заполнить поле **Описание**.

Остальные вкладки станут доступны после добавления ПО (см. [Редактирование ПО](#)).

Для добавления нового ПО нажать на кнопку сохранения. Будет выполнен переход к каталогу программного обеспечения.

Для закрытия карточки добавления ПО и возврата к каталогу программного обеспечения нажать на кнопку закрытия.

11.2.5. Редактирование ПО

Редактирование ПО осуществляется на его карточке. Для перехода на карточку необходимо в каталоге ПО выбрать требуемое ПО и нажать кнопку **[Редактировать]**.

Карточка ПО состоит из вкладок:

- **Основное;**
- **Пакеты;**
- **Шаблоны конфигурации;**
- **Параметры.**

Для закрытия карточки и возврата к каталогу программного обеспечения нажать на кнопку закрытия.

11.2.5.1. Основное

На вкладке приведена основная информация о ПО: наименование ПО, родительский раздел каталога ПО и описание. Для редактирования доступны родительский раздел ПО и описание ПО.

Для сохранения изменений нажать на кнопку сохранения. Будет выполнен переход к каталогу программного обеспечения.

Для закрытия карточки ПО и возврата к каталогу программного обеспечения нажать на кнопку закрытия.

11.2.5.2. Пакеты

На вкладке осуществляется управление пакетами данного ПО.

Список пакетов

На вкладке приведен список пакетов, входящих в состав ПО, с указанием имени и версии пакета.

В списке доступен поиск по имени и версии. Для этого в соответствующем поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Внизу списка указано количество записей в списке.

Добавление пакета в состав ПО

Для добавления пакета в состав ПО необходимо на вкладке **Пакеты** нажать кнопку **[Пакет]**. Будет открыта карточка добавления пакета ПО.

На карточке добавления пакета ввести наименование пакета (например, *chromium*) и сохранить его, нажав кнопку сохранения в правом верхнем углу. Для добавления доступны пакеты из состава репозитория, настроенных в подразделе [Репозитории ПО](#) (раздел [Установка и обновление ПО](#)).

Удаление пакета из состава ПО

Пакет или одновременно несколько пакетов можно удалить из состава данного ПО. Для этого необходимо отметить пакет в списке и нажать кнопку **[Удалить]**.

11.2.5.3. Шаблоны конфигурации

На вкладке осуществляется настройка шаблонов конфигурации ПО.

Список шаблонов конфигурации

На вкладке приведен список шаблонов конфигурации для данного ПО.

В списке доступен поиск по названию и пути размещения. Для этого в поле поиска ввести значение.

Внизу списка указано количество записей в списке.

Добавление шаблона конфигурации

Для добавления шаблона конфигурации необходимо на вкладке **Шаблоны конфигурации** нажать кнопку **[Шаблон]**. Будет открыта карточка добавления шаблона.

На карточке на вкладке **Основное** указать наименование шаблона (например, *chromiumtemplate*) и путь размещения (например, */etc/chromium/policies/managed/chrome.json*).

Вкладка **Редактирование шаблона** будет доступна после сохранения нового шаблона (см. [Редактирование шаблона конфигурации](#)).

Для сохранения нажать кнопку сохранения в правом верхнем углу.

Для закрытия карточки нажать на кнопку закрытия.

Редактирование шаблона конфигурации

Редактирование шаблона конфигурации осуществляется на его карточке. Для перехода на карточку необходимо в списке шаблонов выбрать требуемый шаблон.

Карточка шаблона состоит из вкладок:

- **Основное;**
- **Редактирование шаблона.**

Для закрытия карточки и возврата к каталогу программного обеспечения нажать на кнопку закрытия.

Основное

На вкладке приведено наименование шаблона и путь его размещения. Для редактирования доступен путь размещения.

Для сохранения изменений нажать на кнопку сохранения.

Редактирование шаблона

На вкладке указывается текст скрипта шаблона конфигурации с возможностью его редактирования.

Пример 1

```
{%- set StartPage = parameters.get('firefox_StartPage', none) -%}
{% set Homepage = parameters.get('firefox_Homepage', none) -%}
{
  "policies":{
    "ImportEnterpriseRoots": true,
    "Certificates": {
      "Install": ["/etc/ipa/ca.crt"]
    },
{% if Authentication %}
    {%- set Authentication = Authentication.replace(" ", "") -%}
    {%- set TempAuthentication = Authentication.split(",") -%}
    {%- set TempAuthenticationLen = TempAuthentication |length -%}
    "Authentication":{
      "SPNEGO": [
        {% for i in range(TempAuthenticationLen) %}
          "{{ TempAuthentication[i] }}" {% if TempAuthenticationLen - 1 != i %}
↪, {% endif %}
        {% endfor %}
      ],
      "Delegated": [
        {% for i in range(TempAuthenticationLen) %}
          "{{ TempAuthentication[i] }}" {% if TempAuthenticationLen - 1 != i %}
↪, {% endif %}
        {% endfor %}
      ]
    }
  }
{% endif %} {% if Authentication and (Homepage or StartPage) %}, {%
```

(продолжение на следующей странице)

```

↪endif %}
    {%- if Homepage or StartPage -%}
    "Homepage":{
        {%- if StartPage -%}"URL": "{{ StartPage }}",{% endif %}
        "Locked":true,
        "StartPage": {%- if Homepage == 'true' -%}"previous-session"{% else
↪%}"homepage"{% endif %}
        }{% endif %}
    }
}

```

Пример 2

```

{%- set HomepageLocation = parameters.get('chromium_HomepageLocation', none) -
↪%}
{%- set RestoreOnStartupURLs = parameters.get('chromium_HomepageLocation',
↪none) -%}
{%- set RestoreOnStartup = parameters.get('chromium_RestoreOnStartup', none) -
↪%}
{
    {%- if HomepageLocation -%}{{'\n'}}"HomepageLocation": "{{
↪HomepageLocation }}",{{'\n'}}{% endif -%}
    "RestoreOnStartup": {%- if RestoreOnStartup == 'true' -%}1{%- if
↪HomepageLocation -%},{%- endif -%}{{'\n'}}{% else %}4{%- if
↪HomepageLocation -%},{%- endif -%}{{'\n'}}{% endif -%}
    {%- if HomepageLocation -%}
    "RestoreOnStartupURLs":[
        "{{ RestoreOnStartupURLs }}"
    ]
    {%- endif -%}
}

```

Для редактирования скрипта необходимо внести изменения в текст скрипта и нажать на кнопку сохранения в правом верхнем углу.

Для отмены внесенных, но еще не сохраненных изменений, нажать на кнопку **[Отменить]**.

Удаление шаблона конфигурации

Шаблон конфигурации или одновременно несколько шаблонов можно удалить. Для этого необходимо отметить шаблон конфигурации в списке и нажать кнопку **[Удалить]**.

Также удалить шаблон конфигурации можно из карточки: в списке шаблонов нажать на соответствующий шаблон для открытия карточки, затем на карточке на вкладке **Основное** нажать кнопку **[Удалить шаблон]**. После подтверждения удаления будет выполнен переход к списку шаблонов.

11.2.5.4. Параметры

На вкладке осуществляется управление параметрами данного ПО.

Параметры ПО используются при создании шаблонов конфигурации (см. [Редактирование шаблона](#)). Значения параметров ПО могут быть заданы при настройке политики ПО на вкладке **Каталог ПО** в подразделе [Политики ПО](#) (раздел [Установка и обновление ПО](#)).

Список параметров

На вкладке приведен список параметров с указанием имени параметра, значения параметра по умолчанию и его описания.

В списке доступен поиск, для этого в поле поиска ввести значение.

Внизу списка указано количество записей в списке, а в правом нижнем углу кнопки переключения страниц.

Добавление параметра

Для добавления параметра необходимо на вкладке **Параметры** нажать кнопку **[Параметр]**. Будет открыта карточка добавления параметра.

На карточке указать заполнить поля:

- **Имя параметра** — имя для использования в тексте шаблона конфигурации (например, *chromium_HomepageLocation*);

Важно: В имени параметра можно использовать a-z, 0-9, -_

- **Отображаемое имя параметра** — имя для отображения в списке параметров и в формах настройки параметра (например, *Стартовая страница*);

Важно: В отображаемом имени параметра можно использовать a-z, A-Z, a-я, A-Я, ёЁ, 0-9, -_. и пробел между словами

- **Значение параметра** — значение параметра, применяемое по умолчанию (например, <https://yandex.ru>).

Также можно указать описание параметра.

Для сохранения нажать кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку параметров нажать на кнопку закрытия.

Редактирование параметра

Редактирование параметра осуществляется на его карточке. Для перехода на карточку необходимо в списке параметров нажать на требуемый параметр.

Для редактирования доступны поля **Отображаемое имя параметра**, **Значение параметра** и **Описание**.

Для применения изменений нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку параметров нажать на кнопку закрытия.

Удаление параметра

Параметр или одновременно несколько параметров можно удалить. Для этого необходимо отметить параметр в списке и нажать кнопку **[Удалить]**.

Также удалить параметр можно из карточки: в списке параметров нажать на соответствующий параметр для открытия карточки, затем на карточке нажать кнопку **[Удалить параметр]**. После подтверждения удаления будет выполнен переход к списку

параметров.

11.2.6. Удаление программного обеспечения или раздела

Для удаления программного обеспечения или раздела ПО необходимо в каталоге программного обеспечения выбрать требуемый объект и нажать кнопку **[Редактировать]**. Затем в открывшейся карточке нажать кнопку **[Удалить ПО]** или **[Удалить раздел]**, соответственно. После подтверждения удаления будет выполнен переход к каталогу программного обеспечения.

11.3. Репозитории ПО

В подразделе выполняются функции управления репозиториями ПО и серверами репозитория.

11.3.1. Репозитории ПО

На вкладке осуществляется управление репозиториями ПО: создание, редактирование и удаление репозитория.

11.3.1.1. Список репозитория ПО

Вкладка содержит список репозитория ПО с указанием имени репозитория, типа репозитория и его описания.

В списке доступен поиск по имени репозитория. Для этого в поле поиска ввести значение. Внизу списка указано количество записей в списке.

11.3.1.2. Создание репозитория ПО

Для создания репозитория ПО нажать кнопку **[Новый репозиторий]**, будет выполнен переход на карточку нового репозитория.

На карточке на вкладке **Основное** заполнить обязательные поля **Имя репозитория** и **Относительный путь публикации репозитория**. В поле **Относительный путь публикации репозитория** указывается каталог на компьютере, куда будет сохранен репозиторий (например, `/astra17/bin`).

Также можно указать описание репозитория. Поле **Тип репозитория** будет заполнено автоматически без возможности изменения.

Вкладка **Версии** станет доступна для редактирования после сохранения репозитория (см. [Редактирование репозитория ПО](#)).

Для сохранения репозитория нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку репозитория нажать на кнопку закрытия.

11.3.1.3. Редактирование репозитория ПО

Редактирование репозитория осуществляется на его карточке. Для перехода на карточку необходимо нажать на репозиторий в списке.

На карточке информация о репозитории размещается на вкладках:

- **Основное;**
- **Версии.**

Для закрытия карточки репозитория и возврата к списку нажать на кнопку закрытия.

Основное

На вкладке указана основная информация о репозитории: его имя, тип, описание, относительный и абсолютный путь публикации репозитория. Поля **Тип репозитория** и **Абсолютный путь до репозитория** недоступны для редактирования. Остальные поля возможно изменить.

Для применения внесенных изменений нажать на кнопку сохранения в правом верхнем углу.

Версия

Список версий репозитория

На вкладке в табличном виде приведен список версий репозитория с указанием номера версии, состояния версии, даты создания и типа источника.

В списке доступен поиск. Для этого в поле поиска ввести значение. Также в списке доступна фильтрация по значениям столбцов **Состояние**, **Дата создания** и **Тип источника**, для этого необходимо нажать на значок фильтра рядом с названием столбца и отметить требуемые значения для фильтрации.

В левом нижнем углу указано количество записей в списке, а в правом нижнем углу кнопки переключения страниц.

Пользователям с допуском к абсолютному пути публикации репозитория доступна для просмотра опубликованная версия репозитория.

Создание версии репозитория

Для создания новой версии репозитория нажать кнопку **[Новая версия]**, будет выполнен переход на карточку создания новой версии.

На карточке на вкладке **Основное** необходимо выбрать тип источника версии репозитория: **Пакеты** или **ISO-образ**.

Тип источника “ISO-образ”

При выборе типа источника **ISO-образ** необходимо загрузить версию репозитория в виде файла с расширением *.iso. Для этого нажать кнопку **[Выбрать ISO-образ]** и в окне навигации выбрать нужный файл.

При необходимости можно изменить выбранный файл, нажав кнопку **[Изменить ISO-образ]** и выбрав другой iso-файл.

Для загрузки образа нажать на кнопку сохранения в правом верхнем углу.

После загрузки ISO-образа версия репозитория опубликуется автоматически, а на вкладке **Основное** отобразятся автоматически заполненные поля:

- **Описание** (например, *Apt repository for project ALDPro*);
- **Источник** (например, *ALDPro*);
- **Метка** (например, *ALDPro*);
- **Номер версии** (например, *1*);
- **Ветка дистрибутива** (например, *stable*);
- **Кодовое имя дистрибутива** (например, *aldpro*);
- **Архитектура дистрибутива** (например, *amd64*);
- **Компоненты дистрибутива** (например, *salt*).

Также автоматически заполнятся остальные вкладки (см. [Текущее содержимое](#) и [История изменений](#)).

Для закрытия карточки версии репозитория и перехода к списку версий нажать на кнопку закрытия.

Тип источника “Пакеты”

При выборе типа источника **Пакеты** необходимо заполнить следующие обязательные поля:

- **Источник** (например, *ALDPro*);
- **Метка** (например, *ALDPro*);
- **Номер версии** (например, *1*);
- **Кодовое имя дистрибутива** (например, *aldpro*);
- **Архитектура дистрибутива** (например, *amd64*).

Также можно заполнить поля **Описание** и **Ветка дистрибутива**.

Поле **Компоненты дистрибутива** заполняется автоматически и недоступно для редактирования.

После сохранения версии станут доступны для редактирования остальные вкладки (см. [Редактирование версии репозитория](#)).

Для сохранения версии репозитория нажать на кнопку сохранения в правом верхнем углу.

После формирования текущего содержимого репозитория (см. [Текущее содержимое](#)) для настройки пользователей, которые смогут подключаться к версии репозитория, ее

необходимо опубликовать (см. [Публикация версии репозитория](#)).

Для закрытия карточки и возврата к списку версий нажать на кнопку закрытия.

Редактирование версии репозитория

Для редактирования доступна только версия репозитория с состоянием **Редактирование**.

Редактирование версии репозитория осуществляется на ее карточке. Для перехода на карточку необходимо в списке версий нажать на версию репозитория.

На карточке информация о версии репозитории размещается на вкладках:

- **Основное;**
- **Текущее содержимое;**
- **История изменений.**

Для закрытия карточки версии репозитория и возврата к списку нажать на кнопку закрытия.

Основное

На вкладке указана основная информация о версии репозитории:

- **Тип источника;**
- **Описание;**
- **Источник;**
- **Метка;**
- **Номер версии;**
- **Ветка дистрибутива;**
- **Кодовое имя дистрибутива;**
- **Архитектура дистрибутива;**
- **Компоненты дистрибутива.**

Поля **Тип источника** и **Компоненты дистрибутива** недоступны для редактирования. Остальные поля возможно изменить.

Для применения внесенных изменений нажать на кнопку сохранения в правом верхнем

углу.

История изменений

На вкладке отображаются изменения, внесенные в данную версию репозитория, с указанием наименования пакета и действия над ним (добавлен или удален).

В списке доступен поиск. Для этого в поле поиска ввести значение.

Внизу списка слева указано количество записей в списке, а справа располагаются кнопки переключения страниц.

Текущее содержимое

На вкладке отображаются пакеты, входящие в состав данной версии репозитория, с указанием наименования пакета, версии пакета и контрольных сумм md5.

В списке доступен поиск. Для этого в поле поиска ввести значение.

Внизу списка слева указано количество записей в списке, а справа располагаются кнопки переключения страниц.

Если версия репозитория имеет состояние **Редактирование**, то текущее содержимое может быть изменено:

- для добавления в версию репозитория пакета нажать кнопку **[Загрузить пакет]**. В открывшемся окне навигации выбрать файл на и нажать **[Открыть]**;
- для удаления из версии репозитория пакета или одновременно нескольких пакетов необходимо отметить пакет в списке и нажать кнопку **[Удалить]**.

Публикация версии репозитория

Для публикации версии репозитория с выбранными пакетами для открытого допуска необходимо открыть карточку версии и на вкладке **Текущее содержимое** нажать кнопку **[Опубликовать]**.

После публикации версия репозитория изменит состояние на **Опубликована** и станет недоступна для редактирования.

Удаление версии репозитория

Для удаления версии репозитория открыть ее карточку, нажав на версию в списке, затем на карточке на вкладке **Основное** нажать кнопку **[Удалить версию]**. После подтверждения удаления будет выполнен переход к списку версий.

11.3.1.4. Удаление репозитория

Для удаления репозитория открыть его карточку, нажав на репозиторий в списке, затем на карточке нажать кнопку **[Удалить репозиторий]**. После подтверждения удаления будет выполнен переход к списку репозитория.

11.3.2. Серверы репозитория ПО

На вкладке осуществляется управление серверами репозитория ПО: развертывание, редактирование и удаление серверов репозитория ПО. Сервер репозитория ПО это отдельная подсистема ALD Pro, устанавливается на выбранный компьютер домена и далее принимает команды портала управления.

11.3.2.1. Список серверов репозитория ПО

Вкладка содержит в табличном виде список развернутых серверов репозитория ПО с указанием имени сервера, его IP-адреса, функций сервера и имени сайта.

В списке доступен поиск. Для этого в поле поиска ввести значение. Также доступна фильтрация по функциям сервера, для этого нажать на значок фильтра рядом с названием столбца **Роль** и выбрать требуемое значение для фильтрации.

Внизу списка указано количество записей в списке.

11.3.2.2. Развертывание сервера репозитория ПО

Для развертывания сервера необходимо на вкладке нажать кнопку **[Развернуть сервер репозитория ПО]**. Будет открыта вкладка нового сервера репозитория ПО.

На карточке из выпадающего списка **Имя компьютера** выбрать компьютер из состава

домена, который будет выполнять функцию сервера репозитория. В поле **Имя сайта** выбрать сайт для сервера репозитория.

Для сохранения сервера нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку серверов нажать на кнопку закрытия.

11.3.2.3. Управление сервером репозитория ПО

Управление сервером осуществляется на его карточке. Для перехода на карточку необходимо нажать левой кнопкой мыши на сервер в списке.

На карточке отображена основная информация о сервере репозитория ПО. Для редактирования доступны поля функций сервера и сайт сервера.

Для применения внесенных изменений нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку серверов нажать на кнопку закрытия.

11.3.2.4. Удаление сервера репозитория ПО

Для удаления сервера открыть его карточку, нажав на сервер в списке, затем на карточке нажать кнопку **[Удалить сервер репозитория]**. После подтверждения удаления будет выполнен переход к списку серверов.

11.4. Политики обновления ALD Pro

В подразделе выполняется настройка политик обновления ALD Pro на компьютеры и группы компьютеров.

11.4.1. Список политик обновления ALD Pro

В подразделе приведен список политик обновления ALD Pro с указанием имени политики, версии и статуса.

В списке доступен поиск, для этого в поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

В левом нижнем углу указано количество записей, а в правом нижнем углу кнопки переключения страниц.

11.4.1.1. Версионность

Каждая политика обновления ALD Pro имеет версию, которая автоматически изменяется, если наступило одно из следующих событий:

1. Внесены любые изменения в политику обновления ALD Pro. В этом случае дата изменений - это дата, когда пользователь внес изменения. А автор - это ФИО пользователя, внесшего изменения.
2. Произошло обновление системы. В этом случае дата изменений - это дата обновления системы. А автор изменений - **Системное обновление**.

11.4.2. Создание политики обновления ALD Pro

Для создания новой политики обновления ALD Pro необходимо нажать на кнопку [+ Новая политика обновления]. Будет выполнен переход на карточку новой политики.

На карточке на вкладке Основное задать имя политики обновления ALD Pro. Также можно указать описание политики. Указать статус политики: включена или выключена.

Остальные вкладки станут доступны после сохранения политики (см. [Настройка политики обновления ALD Pro](#)).

Для сохранения новой политики обновления необходимо нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку политик обновления ALD Pro нажать на кнопку закрытия.

11.4.3. Настройка политики обновления ALD Pro

Настройка политики обновления ALD Pro выполняется на ее карточке. Для открытия карточки необходимо в списке политик обновления нажать на соответствующую политику обновления.

На карточке политики обновления представлены следующие вкладки:

- Основное;
- Source list;
- Компьютеры.

Для закрытия карточки и возврата к списку политик обновления ALD Pro нажать на кнопку закрытия.

11.4.3.1. Основное

На вкладке Основное приведена основная информация о политике обновления: имя политики, ее описание и статус.

Ниже отображаются свойства политики обновления: дата создания, дата изменения, версия и автор изменений.

Поле Описание доступно для редактирования. Также можно изменить статус политики обновления, включив или выключив ее.

Для сохранения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

11.4.3.2. Source list

На вкладке **Source list** осуществляется формирование source list.

На вкладке указывается список репозиториев пакетов для APT.

Добавить или изменить source list можно двумя способами:

- добавить текст из файла на компьютере;
- вручную ввести или изменить текст source list на вкладке.

Для добавления текста source list из файла необходимо нажать кнопку **[Загрузить из файла]**, в окне навигации выбрать на компьютере необходимый файл в формате .list или .txt и нажать **[Открыть]**.

Содержимое файла отобразится в форме **Конфигурация Source list**, при этом предыдущее содержимое source list будет заменено. При необходимости добавленный текст можно отредактировать.

Для добавления или редактирования source list вручную необходимо нажать кнопку **[Редактировать]**, после чего форма **Конфигурация Source list** станет доступна для редактирования.

Для сохранения source list необходимо ввести комментарий и нажать кнопку сохранения. Для отмены внесения изменений в файл конфигурации нажать кнопку **[Отменить]**.

11.4.3.3. Компьютеры

На вкладке **Установить на компьютеры** в списке **Выбранные компьютеры** приведен список компьютеров, на которые будет установлена данная политика. В списке **Все компьютеры** приведен список всех компьютеров домена.

Во всех списках доступен поиск по имени компьютера. Для этого в соответствующем поле поиска ввести значение от трех символов, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для назначения политики на компьютер необходимо в списке **Все компьютеры** отметить компьютеры и перенести их в список **Выбранные компьютеры** нажатием кнопки **[<-]**.

Для отмены политики на компьютер необходимо в списке **Выбранные компьютеры** отметить требуемые компьютеры и перенести их в список **Все компьютеры** нажатием кнопки **[->]**.

На вкладке **Установить на группы компьютеров** в списке **Выбранные группы** приведен список групп, на компьютеры которых будет установлена данная политика. В списке **Все группы** приведен список всех групп домена.

Во всех списках доступен поиск по имени группы. Для этого в соответствующем поле поиска ввести значение от трех символов, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для назначения политики на группу компьютеров необходимо в списке **Все группы** отметить группы и перенести их в список **Выбранные группы** нажатием кнопки [**<-**].

Для отмены политики на группу компьютеров необходимо в списке **Выбранные группы** отметить требуемые группы и перенести их в список **Все группы** нажатием кнопки [**->**].

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

11.4.4. Просмотр назначенных политик на компьютерах и группах компьютеров

Для просмотра политик, назначенных на компьютер, необходимо выбрать компьютер в разделе “Пользователи и компьютеры - Компьютеры”.

Для просмотра политик, назначенных на группу компьютеров, необходимо выбрать группу компьютеров в разделе “Пользователи и компьютеры - Группы компьютеров” и перейти в раздел “Политики обновления”.

11.4.5. Удаление политики обновления ALD Pro

Удаления политики обновления выполняется из ее карточки: открыть карточку, нажав в списке политик обновления на соответствующую политику, затем на карточке на вкладке Основное нажать кнопку [Удалить]. После подтверждения удаления будет выполнен переход к списку политик обновления ALD Pro.

Важно: Удаление политики обновления ALD Pro может занимать до часа после включения компьютера и применения политики.

Роли и службы сайта

В разделе осуществляется управление доменными службами.

12.1. Служба разрешения имен

В подраздел осуществляется управление прямыми и обратными зонами DNS, а также перенаправлением DNS-запросов.

12.1.1. Зоны DNS

На вкладке осуществляется управление зонами DNS.

12.1.1.1. Список зон DNS

На вкладке приведен в табличном виде список зон DNS с указанием имени зоны и ее состояния.

В списке доступен поиск по названию зоны. Для этого в верхнем левом углу вкладки в поле поиска ввести значение. Также возможна фильтрация зон по состоянию, для этого нажать на значок фильтра рядом с названием столбца **Состояние** и выбрать требуемое значение для фильтрации.

Для просмотра информации о зоне DNS нажать на соответствующую зону в списке. Будет открыта карточка зоны DNS.

В левом нижнем углу указано количество зон DNS, а в правом нижнем углу кнопки переключения страниц.

12.1.1.2. Включение и выключение зоны DNS

Управлять состоянием зоны DNS можно непосредственно на вкладке. Для этого необходимо в списке отметить зону DNS или одновременно несколько зон DNS и нажать кнопку **[Включить]** или **[Выключить]** для включения или выключения зоны, соответственно.

Также управлять состоянием зоны можно из ее карточки. Для открытия карточки нажать на зону в списке. В открывшейся карточке на вкладке **Параметры зоны** в пункте **Состояние зоны DNS** отметить **Включено** или **Выключено** для включения или выключения зоны, соответственно.

12.1.1.3. Создание зоны DNS

Для создания новой зоны DNS необходимо нажать на кнопку **[Новая зона]**, будет выполнен переход на карточку новой зоны.

На карточке заполнить обязательное поле **Имя зоны** и выбрать значение для пункта **Тип зоны**. При создании зоны DNS обратного типа, поле **Имя зоны** заполняется в формате:

Пример 1

2001:db8::/64

Пример 2

192.0.2.0/24

Дальнейшая настройка зоны осуществляется после ее сохранения (см. [Управление зоной DNS](#)).

Для сохранения новой зоны нажать на кнопку сохранения в правом верхнем углу. Будет выполнен переход к списку зон DNS.

Для закрытия карточки и возврата к списку зон DNS нажать на кнопку закрытия.

12.1.1.4. Управление зоной DNS

Управление зоной DNS выполняется на ее карточке. Для открытия карточки необходимо в списке нажать на соответствующую зону DNS.

На карточке управление зоной DNS осуществляется на вкладках:

- **Записи ресурсов DNS;**
- **Параметры зоны.**

Записи ресурсов DNS

Список записей ресурсов DNS

На вкладке приведен список записей ресурсов, содержащихся в зоне, с указанием имени записи, типа записи и значения записи.

В списке доступен поиск по имени записи и по ее данным. Для этого в верхнем левом углу вкладки в поле поиска ввести значение. Также доступна фильтрация по типу записи, для этого нажать на значок фильтра рядом с названием столбца **Тип записи** и выбрать требуемое значение для фильтрации.

Для просмотра информации о записи ресурса нажать на соответствующую запись в списке. Будет открыта карточка записи ресурса DNS.

В левом нижнем углу указано количество записей ресурсов DNS, а в правом нижнем углу кнопки переключения страниц.

Добавление записи ресурса DNS

Для добавления новой записи ресурса DNS необходимо на вкладке **Записи ресурсов DNS** нажать на кнопку **[Новая DNS запись]**, будет выполнен переход на карточку новой записи.

На карточке заполнить обязательные поля:

- **Имя записи** — отображаемое имя записи, выбирается исходя из типа записи;
- **Тип записи** — определяет тип ресурсной записи. В зависимости от выбранного типа потребуются заполнить дополнительные поля.

В зависимости от выбранного типа записи отображаются следующие поля:

- тип **A** (в качестве имени записи должно быть указано имя компьютера):
 - поле **IP-адрес** — IP-адрес компьютера в формате IPv4;

- тип **AAAA** (в качестве имени записи должно быть указано имя компьютера):
 - поле **IP-адрес** — IP-адрес компьютера в формате IPv6;
- тип **A6**:
 - поле **Данные записи**;
- тип **AFSDB**:
 - поле **Подтип** (является необязательным);
 - поле **Имя узла** — имя компьютера, на котором размещена база данных AFS;
- тип **CERT**:
 - **Тип сертификата** — тип сертификата;
 - **Тег ключа** — числовое значение для выбора записи сертификата;
 - **Алгоритм** — алгоритм создания подписи;
 - **Сертификат или список отзыва сертификатов (CRL)**;
- тип **CNAME**:
 - **Имя узла**;
- тип **DNAME**:
 - **Цель**;
- тип **DS**:
 - **Тег ключа**;
 - **Алгоритм**;
 - **Тип дайджеста**;
 - **Дайджест**;
- тип **DLV**:
 - **Тег ключа**;
 - **Алгоритм**;
 - **Тип дайджеста**;
 - **Дайджест**;
- тип **KX**:
 - **Приоритет**;

- Обменник;
- тип LOC:
 - Градусы широты;
 - Минуты широты (является необязательным);
 - Секунды широты (является необязательным);
 - переключатель **Направление широты**;
 - Градусы долготы;
 - Минуты долготы (является необязательным);
 - Секунды долготы (является необязательным);
 - переключатель **Направление долготы**;
 - Высота над уровнем моря;
 - Размер (является необязательным);
 - Горизонтальная точность (является необязательным);
 - Вертикальная точность (является необязательным);
- тип MX:
 - Приоритет;
 - Обменник;
- тип NAPTR:
 - Порядок;
 - Приоритет;
 - Флаги;
 - Служба;
 - Регулярное выражение;
 - Замена;
- тип NS:
 - Имя узла;
- тип PTR:
 - Имя узла;
- тип SRV:

- **Приоритет (порядок);**
- **Вес;**
- **Порт;**
- **Цель;**
- **тип SSHFP:**
 - **Алгоритм;**
 - **Тип отпечатка;**
 - **Отпечаток;**
- **тип TLSA:**
 - **Использование сертификата;**
 - **Селектор;**
 - **Тип соответствия;**
 - **Данные сопоставления сертификата;**
- **тип TXT:**
 - **Текстовые данные;**
- **тип URI:**
 - **Приоритет (порядок);**
 - **Вес;**
 - **Универсальный код ресурса (URI).**

При выборе типа записи необходимо учитывать существующие ограничения (см. [Ограничения на типы записей](#)).

Для сохранения записи ресурса DNS нажать на кнопку сохранения в правом верхнем углу. Будет выполнен переход к списку записей ресурсов.

Для закрытия карточки и возврата к списку записей ресурсов нажать на кнопку закрытия.

Редактирование записи ресурса DNS

Для редактирования записи ресурса DNS нажать на соответствующую запись в списке. Будет открыта карточка записи ресурса DNS.

На карточке записи не доступны для редактирования имя и тип записи. Изменить возможно поля, соответствующие выбранному типу записи (см. [Добавление записи ресурса DNS](#)).

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку записей ресурсов нажать на кнопку закрытия.

Удаление записи ресурса DNS

Для удаления записи ресурса DNS или одновременно нескольких записей ресурсов DNS необходимо в списке записей отметить запись и нажать кнопку **[Удалить]**.

Чтоб отметить все записи — отметить пункт **Имя записи**. Для снятия отметки нажать на кнопку закрытия в правом верхнем углу.

Также удалить запись ресурса DNS можно из ее карточки: открыть карточку нажатием на запись ресурса в списке, затем на карточке нажать кнопку **[Удалить данные записи]**. После подтверждения удаления будет выполнен переход к списку записей ресурсов DNS.

Параметры зоны

На вкладке приведены параметры выбранной зоны.

Значения параметров заполняются автоматически при создании зоны, при необходимости значения можно изменить:

- Полномочный сервер имен;
- Адрес электронной почты администратора;
- Номер SOA;
- Обновление SOA;
- Повторный запрос SOA;
- Окончание действия SOA;
- Минимальный срок жизни SOA;
- Срок жизни по умолчанию;
- Срок жизни;
- Динамическое обновление;

- Разрешить запрос;
- Разрешить перенос;
- Глобальные перенаправители;
- Политика перенаправления;
- Состояние зоны DNS.

Для параметров **Разрешить запрос**, **Разрешить перенос** и **Глобальные перенаправители** возможно добавить несколько значений. Для добавления значения необходимо в соответствующем параметре нажать кнопку **[Добавить]** и в появившемся поле ввести значение. Для удаления значения — нажать кнопку **[Удалить]** рядом с соответствующим полем.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку зон DNS нажать на кнопку закрытия.

12.1.1.5. Удаление зоны DNS

Удаление зоны DNS осуществляется из ее карточки: открыть карточку, нажав в списке зон DNS на зону, затем на карточке на вкладке **Параметры зоны** нажать кнопку **[Удалить зону]**. После подтверждения удаления будет выполнен переход к списку зон DNS.

12.1.1.6. Ограничения на типы записей

Тип записи	Правила создания нового типа записи
A6	Запись NS нельзя использовать вместе с записью A6, если только они не расположены в корневой записи зоны
AFSDB	Запись NS нельзя использовать вместе с записью AFSDB, если только они не расположены в корневой записи зоны
DNAME	Запись NS нельзя использовать вместе с записью DNAME, если только они не расположены в корневой записи зоны. Для одного имени можно использовать только одну запись DNAME
DS	Запись DS должна использоваться вместе с записью NS. Запись DS не должна находиться в начале зоны
DLV	Запись NS нельзя использовать вместе с записью DLV, если только они не расположены в корневой записи зоны
KX	Запись NS нельзя использовать вместе с записью KX, если только они не расположены в корневой записи зоны
LOC	Запись NS нельзя использовать вместе с записью LOC, если только они не расположены в корневой записи зоны
NAPTR	Запись NS нельзя использовать вместе с записью NAPTR, если только они не расположены в корневой записи зоны
PTR	Запись NS нельзя использовать вместе с записью PTR, если только они не расположены в корневой записи зоны
SRV	Запись NS нельзя использовать вместе с записью SRV, если только они не расположены в корневой записи зоны
SSHFP	Запись NS нельзя использовать вместе с записью SSHFP, если только они не расположены в корневой записи зоны
TLSA	Запись NS нельзя использовать вместе с записью TLSA, если только они не расположены в корневой записи зоны
TXT	Запись NS нельзя использовать вместе с записью TXT, если только они не расположены в корневой записи зоны
URI	Запись NS нельзя использовать вместе с записью URI, если только они не расположены в корневой записи зоны

12.1.2. Перенаправление запросов

На вкладке Перенаправление запросов осуществляется управление перенаправлением запросов.

12.1.2.1. Список перенаправлений

На вкладке приведен в табличном виде список зон, для которых настроено перенаправление, с указанием состояния зоны DNS, глобальных перенаправителей и политики перенаправления.

В списке доступен поиск по зоне и перенаправителю. Для этого в верхнем левом углу вкладки в поле поиска ввести значение. Также доступна фильтрация по состоянию зоны и политике перенаправления, для этого нажать на значок фильтра рядом с названием соответствующего столбца и выбрать значение для фильтрации.

Для просмотра информации о перенаправлении нажать на соответствующую зону в списке, будет открыта ее карточка.

В левом нижнем углу указано количество записей, а в правом нижнем углу кнопки переключения страниц.

12.1.2.2. Включение и выключение зоны

Управлять состоянием зоны можно непосредственно на вкладке **Перенаправление запросов**. Для этого необходимо в списке отметить зону или одновременно несколько зон и нажать кнопку **[Включить]** или **[Выключить]** для включения или выключения зоны, соответственно.

Также управление состоянием зоны возможно из карточки зоны: открыть карточку нажатием на зону в списке, затем на карточке установить переключатель **[Состояние зоны DNS]** в соответствующее положение. Для применения изменений нажать на кнопку сохранения в правом верхнем углу, после подтверждения сохранения будет выполнен переход к списку зон.

Для закрытия карточки и возврата к списку зон нажать на кнопку закрытия.

12.1.2.4. Редактирование зоны

Редактирование зоны осуществляется на ее карточке. Для открытия карточки необходимо в списке зон нажать на соответствующую зону.

На карточке доступны для редактирования поля **Глобальные перенаправители**, **Тип зоны** и **Политика перенаправления** (см. [Добавление зоны](#)).

Также на карточке осуществляется управление состоянием зоны (см. [Включение и выключение зоны](#)).

Для применения изменений нажать на кнопку сохранения в правом верхнем углу. Будет выполнен переход к списку зон.

Для закрытия карточки и возврата к списку зон нажать на кнопку закрытия.

12.1.2.5. Удаление зоны

Удаление зоны осуществляется из ее карточки: открыть карточку, нажав на зону в списке, затем на карточке нажать кнопку **[Удалить зону]**. После подтверждения удаления будет выполнен переход к списку зон.

12.1.3. Глобальная конфигурация DNS

На вкладке осуществляется управление глобальными перенаправителями запросов.

После настройки в ALD Pro первого контроллер домена он является единственным DNS-сервером, в связи с этим необходимо добавить глобальный перенаправитель запросов на внешний DNS-сервер (публичный или сторонний внутренний).

Также на вкладке отображается информация о том, какие DNS-серверы IPA равернуты в ALD Pro.

Для добавления глобального перенаправителя необходимо указать его IP-адрес в поле **Глобальные перенаправители**. При необходимости можно добавить несколько глобальных перенаправителей: для добавления каждого последующего перенаправителя

нажать кнопку **[Добавить]** и в отобразившемся поле ввести IP-адрес.

Для удаления глобального перенаправителя нажать кнопку **[Удалить]** рядом с соответствующим IP-адресом.

Для настройки политики перенаправления требуется выбрать необходимое значение для пункта **Политика перенаправления**.

Также можно отметить пункт **Разрешить PTR-синхронизацию**.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

12.2. Служба динамической настройки узла

В подразделе выполняется управление серверами службы динамической настройки узла (DHCP). DHCP-сервера развертываются с помощью команд с портала управления на выбранных компьютерах в домене ALD Pro.

12.2.1. Список серверов

В подразделе на вкладке **Перечень серверов** приводится список DHCP-серверов с указанием имени сервера, имени сайта и IP-адреса.

В списке доступен поиск по имени сервера, имени сайта или IP-адресу сервера. Для этого в верхнем левом углу вкладки в поле поиска ввести значение.

В левом нижнем углу указано количество серверов, а в правом нижнем углу кнопки переключения страниц.

12.2.2. Добавление DHCP-сервера

Для добавления нового DHCP-сервера необходимо нажать на кнопку **[Новый сервер]**, будет выполнен переход на карточку нового сервера.

На карточке на вкладке **Основное** заполнить обязательные поля:

- **Имя компьютера** — имя компьютера, добавленного в ALD Pro, который будет выполнять функции DHCP-сервера;
- **Имя сайта** — выбрать из списка сайт, добавленный на вкладке *Сайты и службы* подраздела *Сайты и службы* (раздел *Управление доменом*).

Вкладка **Конфигурация скрипта** будет доступна после сохранения сервера (см. *Настройка конфигурации DHCP-сервера*).

Для сохранения сервера нажать на кнопку сохранения в правом верхнем углу. Будет выполнен переход к списку серверов.

Для закрытия карточки и возврата к списку серверов нажать на кнопку закрытия.

12.2.3. Настройка конфигурации DHCP-сервера

Настройка конфигурации DHCP-сервера выполняется на его карточке. Для открытия карточки необходимо в списке серверов нажать на соответствующий сервер.

На карточке настройка сервера осуществляется на вкладках:

- **Основное;**
- **Конфигурация скрипта;**
- **Настройка сетевых интерфейсов.**

Для закрытия карточки и возврата к списку серверов нажать на кнопку закрытия.

12.2.3.1. Основное

На вкладке **Основное** приведена основная информация о сервере. Для редактирования доступно поле **Имя сайта**.

Для сохранения изменений нажать на кнопку сохранения в правом верхнем углу. Будет выполнен переход к списку серверов.

12.2.3.2. Конфигурация скрипта

На вкладке **Конфигурация скрипта** осуществляется настройка файла конфигурации DHCP-сервера.

Пример 1: Конфигурация сервера DHCP с DDNS

```
ddns-updates on;
update-conflict-detection false;
allow booting;
do-forward-updates on;
update-optimization on;
allow declines;
ddns-update-style interim;
include "/etc/dhcp/rndc.key";
ddns-domainname "";
update-static-leases off;

option domain-name "aldpro.ru";
option domain-search "aldpro.ru";

option domain-name-servers 192.168.10.10;
option dhcp-server-identifier 192.168.10.15;

#Следующая строка нужна только если используется Samba с WINS

#option netbios-name-servers 10.0.2.102;

default-lease-time 129600;
max-lease-time 1296000;
authoritative;

#server-name "dc3.aldpro.ru";

#server-identifier 192.168.10.13;

#Эта подсеть должна соответствовать подсети вашей локальной сети, обращенной
↳к устройству Ethernet.
Subnet 192.168.10.0 netmask 255.255.255.0 {
    option broadcast-address 192.168.10.255;
    option subnet-mask 255.255.255.0;
    option routers 192.168.10.1;
    pool {
        range 192.168.10.220 192.168.10.230;
        allow known-clients;
        allow unknown-clients;
```

(продолжение на следующей странице)


```

    max-lease-time 86400;
    default-lease-time 43200;
}
zone alldpro.ru. {
    primary 192.168.10.10;
    key "rndc-key";
}
}

```

Пример 2: Конфигурация сервера DHCP для установки ОС по сети

```

#Все параметры расписаны тут https://github.com/42wim/isc-dhcp/blob/master/
↪server/dhcpd.conf.example
#Все опции DHCP тут https://www.iana.org/assignments/bootp-dhcp-parameters/
↪bootp-dhcp-parameters.xhtml

#Сетевой интерфейс
INTERFACES="eth1";
allow booting;
allow bootp;
option classless-routes-lin code 121 = array of unsigned integer 8;
#Подсеть и маска подсети
#Адрес сервера установки ОС
next-server 192.168.17.5;
#Путь до загрузчика
if substring (option vendor-class-identifier, 15, 5) = "00000" {
    filename "lpxelinux.0";
} elsif substring (option vendor-class-identifier, 15, 5) = "00007" {
    filename "bootx64.efi";
} else {
    filename "pxelinux.0";
}
subnet 192.168.17.0 netmask 255.255.255.0 {
#Пул адресов, из которого будут выдаваться адреса, где 192.168.17.10 -
↪первый адрес, 192.168.17.100 - последний адрес
range 192.168.17.10 192.168.17.100;
#DNS сервер. В результате 10.10.0.1 запишется в /etc/resolv.conf на клиенте
option domain-name-servers 10.10.0.1;
#DNS сервер. В результате domain alld.pro запишется в /etc/resolv.conf на

```

(продолжение на следующей странице)

```

↪клиенте
option domain-name "ald.pro";
#Шлюз по-умолчанию
option routers 192.168.17.1;
#Статический маршрут (Опционально)
option classless-routes-lin 24, 192,168,17, 0, 192,168,17,1;
#Широковещательный адрес
option broadcast-address 192.168.17.255;
#Время аренды по-умолчанию
default-lease-time 6000;
#Максимальное время аренды
max-lease-time 72000;

}

#Статические адреса

#Задаем адрес tftp сервера + настраиваем его статику
host os {
    hardware ethernet 1E:0F:E6:05:7C:01;
    fixed-address 192.168.17.5;
}

```

На вкладке указывается актуальный текст файла конфигурации.

Добавить или изменить файл конфигурации можно двумя способами:

- добавить текст из файла на компьютере;
- вручную ввести или изменить текст файла конфигурации на вкладке.

Для добавления текста конфигурации из файла необходимо нажать кнопку **[Загрузить из файла]**, в окне навигации выбрать на компьютере необходимый файл в формате *.conf* или *.txt* и нажать **[Открыть]**.

Содержимое файла отобразится в форме **Редактировать скрипт вручную**, при этом предыдущее содержимое файла конфигурации будет заменено. При необходимости добавленный текст можно отредактировать.

Для сохранения файла конфигурации необходимо ввести комментарий и нажать кнопку сохранения. Для отмены внесения изменений в файл конфигурации нажать кнопку

[Отменить].

Для добавления или редактирования файла конфигурации вручную необходимо нажать кнопку **[Редактировать файл]**, после чего форма **Редактировать скрипт вручную** станет доступна для редактирования.

Для сохранения файла конфигурации необходимо ввести комментарий и нажать кнопку сохранения. Для отмены внесения изменений в файл конфигурации нажать кнопку **[Отменить].**

Для просмотра истории изменений файла конфигурации необходимо нажать на кнопку **[История изменений]**. Откроется карточка с отображением списка изменений с указанием даты изменения, автора изменения и комментария. В списке доступен поиск, для этого в верхнем левом углу вкладки в поле поиска ввести значение. В левом нижнем углу указано количество записей, а в правом нижнем углу кнопки переключения страниц.

12.2.3.3. Настройка сетевых интерфейсов

На вкладке **Настройка сетевых интерфейсов** осуществляется настройка перечня протоколов и сетевых интерфейсов, с которыми будет работать сервис DHCP.

При необходимости указать несколько сетевых интерфейсов, их можно перечислить через пробел.

Пример настроек (для протокола IPv4 используется интерфейс eth0, работа по протоколу IPv6 запрещена):

Пример

```
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
#DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpd6.conf

# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPDv4_PID=/var/run/dhcpd.pid
#DHCPDv6_PID=/var/run/dhcpd6.pid

# Additional options to start dhcpd with.
```

(продолжение на следующей странице)

```
#      Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpcd) serve DHCP requests?
#      Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="eth1" # Наименование сетевого интерфейса v4, с которого будут
↳ раздаваться IP адреса
INTERFACESv6="" # Наименование сетевого интерфейса v6, с которого будут
↳ раздаваться IP адреса
```

На вкладке указывается актуальный текст файла конфигурации.

Добавить или изменить файл конфигурации можно двумя способами:

- добавить текст из файла на компьютере;
- вручную ввести или изменить текст файла конфигурации на вкладке.

Для добавления текста конфигурации из файла необходимо нажать кнопку **[Загрузить из файла]**, в окне навигации выбрать на компьютере необходимый файл в формате *.txt и нажать **[Открыть]**.

Содержимое файла отобразится в форме **Редактировать скрипт вручную**, при этом предыдущее содержимое файла конфигурации будет заменено. При необходимости добавленный текст можно отредактировать.

Для сохранения файла конфигурации необходимо ввести комментарий и нажать кнопку сохранения. Для отмены внесения изменений в файл конфигурации нажать кнопку **[Отменить]**.

Для добавления или редактирования файла конфигурации вручную необходимо нажать кнопку **[Редактировать файл]**, после чего форма **Редактировать скрипт вручную** станет доступна для редактирования.

Для сохранения файла конфигурации необходимо ввести комментарий и нажать кнопку сохранения. Для отмены внесения изменений в файл конфигурации нажать кнопку **[Отменить]**.

Для просмотра истории изменений файла конфигурации необходимо нажать на кнопку **[История изменений]**. Откроется карточка с отображением списка изменений с указанием даты изменения, автора изменения и комментария. В списке доступен поиск, для этого в верхнем левом углу вкладки в поле поиска ввести значение. В левом нижнем углу указано

количество записей, а в правом нижнем углу кнопки переключения страниц.

12.2.4. Удаление DHCP-сервера

Удаление сервера осуществляется из его карточки: открыть карточку, нажав в списке серверов на соответствующий сервер, затем на вкладке **Основное** нажать кнопку **[Удалить сервер]**. После подтверждения удаления будет выполнен переход к списку серверов.

12.3. Служба синхронизации времени

В подразделе осуществляется добавление и удаление серверов синхронизации времени (NTP-серверов)

12.3.1. Внешний пул NTP-серверов

На вкладке настраиваются внешние сервера синхронизации времени. Внешний NTP-сервер не относится к компьютерам данного домена и доступен из внешней сети (в т.ч. интернет).

12.3.1.1. Список NTP-серверов

На вкладке приведен список внешних NTP-серверов с указанием доменного имени и типа.

В правой верхней части вкладки отображается информация о состоянии синхронизации: включена или выключена.

В списке доступен поиск по названию. Для этого в верхнем левом углу вкладки в поле поиска ввести значение.

В левом нижнем углу указано количество NTP-серверов, а в правом нижнем углу кнопки переключения страниц.

12.3.1.2. Добавление NTP-сервера

Для добавления нового NTP-сервера необходимо нажать на кнопку **[Новый NTP-сервер]**, будет выполнен переход на карточку добавления NTP-сервера.

На карточке заполнить обязательные поля:

- **NTP-сервер** — доменное имя внешнего NTP-сервера;
- **Тип** — отметить тип добавляемого ресурса (сервер или пул серверов).

Для сохранения нового NTP-сервера нажать на кнопку сохранения в правом верхнем углу. Будет выполнен переход к списку NTP-серверов.

Для закрытия карточки и возврата к списку NTP-серверов нажать на кнопку закрытия.

12.3.1.3. Удаление NTP-сервера

Для удаления NTP-сервера или одновременно нескольких NTP-серверов необходимо в списке NTP-серверов отметить запись и нажать кнопку **[Удалить]**.

Чтоб отметить все записи — отметить пункт **Доменное имя**. Чтобы снять выделение — нажать кнопку закрытия в правом верхнем углу.

12.3.2. Корневые NTP-серверы домена

На вкладке настраиваются внутренние сервера синхронизации времени. Внутренний NTP-сервер это развернутый на компьютерах данного домена ALD Pro.

12.3.2.1. Список корневых NTP-серверов

На вкладке приведен список корневых NTP-серверов домена с указанием имени сервера, IP-адреса и имени сайта.

В списке доступен поиск по имени сервера, IP-адресу сервера и имени сайта. Для этого в верхнем левом углу вкладки в поле поиска ввести значение.

В левом нижнем углу указано количество NTP-серверов, а в правом нижнем углу кнопки переключения страниц.

12.3.2.2. Добавление корневого NTP-сервера

Для добавления нового корневого NTP-сервера необходимо нажать на кнопку **[Новый NTP-сервер]**, будет выполнен переход на карточку добавления NTP-сервера.

На карточке необходимо в поле **Имя компьютера** выбрать контроллер домена, на котором будет развернут NTP-сервер.

Для добавления нового NTP-сервера нажать на кнопку сохранения в правом верхнем углу. Будет выполнен переход к списку корневых NTP-серверов.

Для закрытия карточки и возврата к списку корневых NTP-серверов нажать на кнопку закрытия.

12.3.2.3. Удаление корневого NTP-сервера

Для удаления корневого NTP-сервера или одновременно нескольких корневых NTP-серверов необходимо в списке корневых NTP-серверов домена отметить требуемый NTP-сервер и нажать кнопку **[Удалить]**.

Чтоб отметить все записи — отметить пункт **Имя компьютера**. Для снятия выделения со всех серверов — нажать кнопку закрытия в правом верхнем углу.

12.4. Служба глобального каталога

В подразделе выполняется управление серверами службы динамической настройки узла (DHCP).

12.4.1. Список серверов

В подразделе на вкладке **Серверы глобального каталога** приводится список серверов с указанием названия сервера и имени сайта.

В списке доступен поиск по названию сервера и имени сайта. Для этого в верхнем левом углу вкладки в поле поиска ввести значение.

В левом нижнем углу указано количество серверов, а в правом нижнем углу кнопки

переключения страниц.

12.4.2. Добавление сервера глобального каталога

Для добавления нового сервера необходимо нажать на кнопку **+ Развернуть сервер глобального каталога**, будет выполнен переход на карточку нового сервера, вкладка **Серверы глобального каталога**.

На карточке необходимо заполнить обязательное поле:

- **Имя компьютера** — имя контроллера домена ALD Pro, который будет выполнять функции сервера глобального каталога, выбирается из выпадающего списка.

Поле **Имя сайта** заполняется автоматически после выбора имени компьютера.

Добавленный сервер глобального каталога недоступен для редактирования.

Для закрытия карточки и возврата к списку серверов нажать на кнопку закрытия.

12.4.3. Удаление сервера глобального каталога

Удаление сервера осуществляется с таблицы серверов на странице **Служба глобального каталога**.

Для удаления сервера необходимо выделить его в таблице серверов и нажать кнопку **Удалить**. После подтверждения удаления сервер будет удален из списка серверов.

12.5. Служба печати

В подразделе осуществляется добавление серверов печати, управление сетевыми принтерами и заданиями на печать. Сервер печати это отдельный компьютер, включенный в домен, на который установлен CUPS-сервер печати. CUPS-сервер получает команды от службы печати и запускает необходимые утилиты на компьютере.

12.5.1. Серверы печати

На вкладке подраздела приведен список серверов печати с указанием названия сервера, IP-адреса и имени сайта.

В списке доступен поиск по названию и IP-адресу сервера, а также по имени сайта. Для этого в верхнем левом углу вкладки в поле поиска ввести значение.

В левом нижнем углу указано количество серверов печати, а в правом нижнем углу кнопки переключения страниц.

12.5.2. Добавление сервера печати

Для добавления нового сервера печати необходимо нажать на кнопку **[Развернуть сервер печати]**, будет выполнен переход на карточку нового сервера печати.

На карточке на вкладке **Основное** заполнить обязательные поля:

- **Имя компьютера** — имя компьютера, добавленного в ALD Pro, который будет выполнять функции сервера печати;
- **Имя сайта** — выбрать из списка сайт, добавленный на вкладке [Сайты и службы](#) подраздела [Сайты и службы](#) (раздел [Управление доменом](#)).

Вкладка **Список принтеров** станет доступна после добавления сервера печати (см. [Настройка сервера печати](#)).

Для добавления нового сервера печати необходимо нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку серверов печати нажать на кнопку закрытия.

12.5.3. Настройка сервера печати

Настройка сервера печати выполняется на его карточке. Для открытия карточки необходимо в списке серверов печати нажать на соответствующий сервер печати.

На карточке настройка сервера печати осуществляется на вкладках:

- **Основное;**

- **Список принтеров.**

Для закрытия карточки и возврата к списку серверов печати нажать на кнопку закрытия.

12.5.3.1. Основное

На вкладке приведено имя компьютера и имя сайта. Имя сайта доступно для редактирования.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

12.5.3.2. Список принтеров

На вкладке осуществляется управление сетевыми принтерами.

На вкладке приведен список принтеров, добавленных к данному серверу печати, с указанием наименования принтера, его расположения, драйвера и описания.

В списке доступен поиск. Для этого в верхнем левом углу вкладки в поле поиска ввести значение.

В левом нижнем углу указано количество принтеров, а в правом нижнем углу кнопки переключения страниц.

Добавление принтера

Для добавления нового принтера необходимо на вкладке **Список принтеров** нажать на кнопку **[Новый принтер]**, будет выполнен переход на карточку нового принтера.

На карточке заполнить обязательные поля:

- **Подключение** — адрес подключения принтера в сети, с указанием протокола (ipr, socket, http(s)) (например, [ipp://192.168.31.154](http://192.168.31.154));
- **Наименование принтера** — отображаемое имя принтера. Указывается на латинице, без пробелов.

Дополнительно можно заполнить поля:

- **Расположение** — местоположение принтера;
- **Драйвер** — загрузить драйвер принтера из файла (файлы с расширением *.ppd). Для загрузки драйвера необходимо в поле **Драйвер** нажать кнопку в виде папки и в открывшемся окне навигации выбрать требуемый файл;
- **Описание** — описание принтера.

Вкладка **Список заданий** станет доступна после добавления принтера (см. [Настройка принтера](#)).

Для добавления принтера необходимо нажать на кнопку сохранения в правом верхнем углу. Будет выполнен переход к списку принтеров.

Для закрытия карточки и возврата к списку принтеров нажать на кнопку закрытия.

Настройка принтера

Настройка принтера выполняется на его карточке. Для открытия карточки необходимо в списке принтеров нажать на соответствующий принтер.

На карточке настройка принтера осуществляется на вкладках:

- **Основное;**
- **Список заданий.**

Для закрытия карточки и возврата к списку принтеров нажать на кнопку закрытия.

Основное

На вкладке приведена основная информация о принтере. Для редактирования доступны поля **Расположение** и **Описание** (см. [Добавление принтера](#)).

Возможно заменить драйвер принтера, для этого в поле **Драйвер** нажать кнопку в виде папки и в открывшемся окне навигации выбрать требуемый файл.

Для сохранения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

Список заданий

На вкладке приведен список заданий, которые были отправлены для печати на данном принтере, с указанием наименования документа, имени пользователя, отправившего задание, размера файла, количества страниц и состояния задания на печать.

В списке доступен поиск. Для этого в верхнем левом углу вкладки в поле поиска ввести значение.

В левом нижнем углу указано количество заданий на печать, а в правом нижнем углу кнопки переключения страниц.

Для отмены задания на печать или одновременно нескольких заданий необходимо в списке заданий отметить требуемое и нажать кнопку **[Снять задание]**.

Чтобы отметить все задания — отметить пункт **Наименование задания**.

Удаление принтера

Для удаления принтера или одновременно нескольких принтеров необходимо в списке принтеров отметить требуемый и нажать кнопку **[Удалить]**.

Чтобы отметить все записи — отметить пункт **Наименование принтера**.

Также удалить принтер можно из его карточки: открыть карточку, нажав в списке принтеров на принтер, затем на карточке на вкладке **Основное** нажать кнопку **[Удалить принтер]**. После подтверждения удаления будет выполнен переход к списку принтеров.

12.5.4. Удаление сервера печати

Удаление сервера печати осуществляется из его карточки: открыть карточку, нажав в списке серверов печати на сервер, затем на карточке на вкладке **Основное** нажать кнопку **[Удалить сервер печати]**. После подтверждения удаления будет выполнен переход к списку серверов печати.

12.6. Общий доступ к файлам

В подразделе осуществляется добавление серверов общего допуска (Samba-сервер), управление общими папками и доступом к ним. Samba-сервер развертывается на компьютере в домене ALD Pro и позволяет создать набор директорий, которые будут доступны для других компьютеров домена.

12.6.1. Серверы общих папок

В подразделе на вкладке **Перечень серверов** приведен список серверов с указанием названия сервера, его IP-адреса и имени сайта.

В списке доступен поиск по названию и IP-адресу сервера и по имени сайта. Для этого в верхнем левом углу вкладки в поле поиска ввести значение.

В левом нижнем углу указано количество серверов, а в правом нижнем углу кнопки переключения страниц.

12.6.2. Добавление сервера общих папок

Для добавления нового сервера необходимо нажать кнопку **[Новый сервер]**, будет выполнен переход на карточку нового сервера.

На карточке на вкладке **Основное** заполнить обязательные поля:

- **Имя компьютера** — имя компьютера, добавленного в ALD Pro, на котором будут размещаться папки общего допуска;
- **Имя сайта** — выбрать из списка сайт, добавленный на вкладке *Сайты и службы* подраздела *Сайты и службы* (раздел *Управление доменом*).

Вкладка **Общие папки** станет доступна после добавления сервера (см. *Настройка сервера общих папок*).

Для добавления нового сервера необходимо нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку серверов нажать на кнопку закрытия.

12.6.3. Настройка сервера общих папок

Настройка сервера выполняется на его карточке. Для открытия карточки необходимо в списке серверов нажать на соответствующий сервер.

На карточке настройка сервера осуществляется на вкладках:

- **Основное;**
- **Общие папки.**

Для закрытия карточки и возврата к списку серверов нажать на кнопку закрытия.

12.6.3.1. Основное

На вкладке слева показана информация о подсистеме:

- название подсистемы,
- имя компьютера, на котором эта подсистема расположена,
- состояние подсистемы (см. system_set)
- дата создания подсистемы,
- дата последнего обновления подсистемы,
- версия установленного на компьютер подсистемы ALD Pro.

Есть возможность выполнить обновление ALD Pro на данном компьютере. Для этого необходимо нажать кнопку **Обновить ALD Pro**.

Есть возможность запустить удаление подсистемы с данного компьютера. Для этого необходимо нажать кнопку **Удалить**.

Внимание: После удаления подсистемы, компьютер останется в домене. Установка новой подсистемы (удаленной или любой другой) возможна только после вывода компьютера из домена и переустановки операционной системы на нем.

Для просмотра всех изменений, произошедших с данным компьютером, необходимо нажать кнопку **Открыть журнал событий**. Откроется окно **Журнал истории изменений**, где отображены имя события и дата его наступления. Кнопка **Обновить** позволяет получить актуальную информацию о событиях на компьютере.

На вкладке справа приведено имя компьютера, его IP-адрес и имя сайта. Имя сайта доступно для редактирования (см. [Добавление сервера общих папок](#)).

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

12.6.3.2. Общие папки

На вкладке осуществляется управление общими папками на данном сервере и допуском к ним.

Список общих папок

На вкладке приведен список общих папок данного сервера.

В списке доступен поиск по названию папки. Для этого в верхнем левом углу вкладки в поле поиска ввести значение.

Для просмотра информации об общей папке необходимо открыть ее карточку, нажав на папку в списке (см. [Информация об общей папке](#)).

В левом нижнем углу указано количество папок, а в правом нижнем углу кнопки переключения страниц.

Создание общей папки

Для создания новой общей папки необходимо нажать на кнопку **[Новая папка]**, будет выполнен переход на карточку новой папки.

На карточке на вкладке **Основное** указать следующие обязательные параметры:

- **Название папки:** задать отображаемое имя папки;
- **Относительный путь к локальной папке:** указать путь до папки, по умолчанию абсолютный путь `/opt/samba_shares` + `<относительный путь>`. Если локальной папки нет, она будет создана.

Так же можно указать:

- **Тип виртуальной файловой системы:** выбирается из выпадающего списка;

- **Browsable:** устанавливает, будет ли общая папка отображаться в списке доступных общих ресурсов в сетевом окружении и в списке просмотра;
- **Access based share enum:** скрывает от пользователя файлы и папки, к которым у него нет доступа;
- **Права доступа для новых файлов:** набор разрешений Unix в восьмеричном коде, устанавливаемых на файл (см. подробнее документацию по Samba);
- **Права доступа для новых папок:** набор разрешений Unix в восьмеричном коде, устанавливаемых на папку (см. подробнее документацию по Samba);
- **Наследование прав доступа:** управление правами доступа к новым файлам и папкам, созданным в общей папке. При установке флажка **Да** значения полей **Права доступа для новых файлов** и **Права доступа для новых папок** игнорируются.

Вкладки **Доступ пользователей** и **Доступ групп** станут доступны для редактирования после создания папки (см. [Управление допуском к общей папке](#)).

Для создания новой общей папки необходимо нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку папок нажать на кнопку закрытия.

Информация об общей папке

Информация об общей папке доступна на ее карточке. Для открытия карточки необходимо в списке общих папок нажать на соответствующую папку.

На вкладке **Основное** приведено название папки. Название можно изменить. Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

Для просмотра размера папки нажать кнопку **[Получить размер папки]**.

Для закрытия карточки и возврата к списку серверов нажать на кнопку закрытия.

Управление допуском к общей папке

Управление допуском к папке выполняется на ее карточке. Для открытия карточки необходимо в списке общих папок нажать на соответствующую папку.

На карточке выбранной папки доступны вкладки:

- **Основное;**
- **Доступ пользователей;**
- **Доступ групп.**

На вкладке **Основное** для изменения доступны все поля:

- **Название папки;**
- **Относительный путь к локальной папке;**
- **Тип виртуальной файловой системы;**
- **Browsable;**
- **Access based share enum;**
- **Права доступа для новых файлов;**
- **Права доступа для новых файлов;**
- **Наследование прав доступа.**

На вкладке **Доступ пользователей** представлен список пользователей, которым предоставлен доступ к папке, с указанием типа предоставляемого права доступа (чтение/полный доступ).

Для изменения настроек доступа к папке необходимо нажать кнопку **[Редактировать доступ]**, после чего откроется карточка управления доступом к папке.

Открывшаяся карточка представляет из себя области со списками пользователей **Выбранные пользователи** и **Все пользователи**, а так же поле с выпадающим списком **Доступ** для выбора типа предоставляемого доступа:

- **Чтение** — доступ на просмотр;
- **Полный доступ** — доступ на просмотр, добавление, изменение и удаление;
- **Изменение и назначение прав** - доступ на просмотр, запись, изменение прав доступа к объектам;
- **Доступ запрещен** - доступа к папке нет.

Для управления доступом к выбранной общей папке из выпадающего списка **Доступ** необходимо выбрать тип предоставляемого доступа к файлам данной общей папки, затем в списке **Все пользователи** отметить нужных пользователей и перенести их в список **Выбранные пользователи** нажатием кнопки **[<-]**.

Для отмены предоставления данного типа доступа пользователям необходимо в

списке **Выбранные пользователи** отметить требуемые записи и перенести их в список **Все пользователи** нажатием кнопки **[->]**.

После внесения изменений необходимо нажать кнопку **[Сохранить]** в правом верхнем углу.

Для быстрого поиска пользователя в верхней части каждого из списков доступно поле поиска пользователей по фамилии или логину, в котором достаточно начать вводить нужные данные о пользователе.

Внизу каждого списка указано количество пользователей в данном списке.

На вкладке **Доступ групп** представлен список групп, которым предоставлен доступ к папке, с указанием типа предоставляемого права доступа (чтение/полный доступ).

Для изменения настроек доступа к папке необходимо нажать кнопку **[Редактировать доступ]**, после чего откроется карточка управления доступом к папке.

Открывшаяся карточка представляет из себя области со списками групп **Выбранные группы** и **Все группы**, а так же поле с выпадающим списком **Доступ** для выбора типа предоставляемого доступа:

- **Чтение** — доступ на просмотр;
- **Полный доступ** — доступ на просмотр, добавление, изменение и удаление;
- **Изменение и назначение прав** - доступ на просмотр, запись, изменение прав доступа к объектам;
- **Доступ запрещен** - доступа к папке нет.

Для управления доступом к выбранной общей папке из выпадающего списка **Доступ** необходимо выбрать тип предоставляемого доступа к файлам данной общей папки, затем в списке **Все группы** отметить нужных пользователей и перенести их в список **Выбранные группы** нажатием кнопки **[<-]**.

Для отмены предоставления данного типа доступа для групп необходимо в списке **Выбранные группы** **отметить требуемые записи и перенести их в список ****Все группы** нажатием кнопки **[->]**.

После внесения изменений необходимо нажать кнопку **[Сохранить]** в правом верхнем углу.

Для быстрого поиска группы в верхней части каждого из списков доступно поле поиска групп по названию, в котором достаточно начать название группы.

Внизу каждого списка указано количество групп в данном списке.

Для закрытия карточки и возврата к списку общих папок необходимо нажать на кнопку закрытия.

Удаление общей папки

Удаление общей папки выполняется на ее карточке. Для открытия карточки необходимо в списке общих папок нажать на соответствующую папку, затем на карточке на вкладке **Основное** нажать кнопку **[Удалить папку]**. После подтверждения удаления будет выполнен переход к списку общих папок.

12.6.4. Удаление сервера общих папок

Удаление сервера общих папок осуществляется из его карточки: открыть карточку, нажав на сервер в списке серверов общих папок, затем на карточке на вкладке **Основное** нажать кнопку **[Удалить сервер]**. После подтверждения удаления будет выполнен переход к списку серверов общих папок.

Личный кабинет

В этом разделе осуществляется управление данными личного кабинета авторизованного пользователя.

Раздел состоит из следующих вкладок:

13.1. Основное

На вкладке **Основное** приведены группы полей ввода данных:

- **Персональные данные;**
- **Учетная запись;**
- **Организационные данные;**
- **Контактная информация;**
- **Расположение;**
- **Сертификаты пользователей;**
- **Открытые ключи SSH.**

Для удобства работы группы полей ввода можно разворачивать/сворачивать нажимая на их название.

13.1.1. Персональные данные

В этой группе представлены следующие поля ввода:

- **Фамилия;**
- **Имя;**
- **Отчество;**
- **Отображаемое имя.**

Так же имеется поле для отображения загруженной фотографии пользователя, по

умолчанию фото отсутствует, о чем свидетельствует надпись в поле (**Фото не загружено**). Для загрузки фотографии пользователя имеется кнопка **[Загрузить фото]**. При нажатии на эту кнопку, появляется окно для указания пути на компьютере, откуда фото будет загружено.

13.1.2. Учетная запись

В этой группе представлены следующие поля ввода:

- Идентификатор пользователя (UID);
- Логин;
- Текущий пароль;
- Новый пароль;
- Подтверждение пароля;
- Окончание действия пароля.

Так же имеются кнопка **Заблокировать УЗ**, которая доступна в режиме администратора.

Важно: При смене паролей необходимо учитывать что минимальный срок действия паролей составляет один час, максимальное количество попыток смены пароля — шесть, а длительность блокировки после израсходования попыток составляет 600 секунд. Это значения могут быть изменены в политиках паролей (раздел [Групповые политики](#) — подраздел [Политики паролей](#)).

13.1.3. Организационные данные

В этой группе представлены следующие поля ввода:

- Подразделение;
- Должность;
- Руководитель сотрудника.

13.1.4. Контактная информация

В этой группе представлены следующие поля ввода:

- **Электронный адрес сотрудника;**
- **Номер рабочего телефона и Добавочный;**
- **Номер мобильного телефона.**

Так же имеется кнопка **Дополнительно...** для перехода на вкладку **Расширенные настройки** и ввода дополнительных данных о пользователе.

13.1.5. Расположение

В этой группе представлены следующие поля ввода:

- **Улица;**
- **Город;**
- **Область, край;**
- **Почтовый индекс;**
- **Страна или регион.**

13.1.6. Сертификаты пользователей

В этой группе отображено поле ввода сертификата в формате **base64** или **PEM**. Для добавления сертификата необходимо в поле **Сертификат в формате base64 или PEM** ввести имеющийся сертификат и нажать кнопку **[Добавить]**.

13.1.7. Открытые ключи SSH

В этой группе отображено поле ввода ключа в формате **SSH**. Для добавления ключа необходимо в поле **Ключ в формате SSH** ввести имеющийся ключ и нажать кнопку **[Добавить]**.

13.2. Группы

На вкладке **Группы** приведены две группы полей с данными:

- **Состоит в группах;**
- **Состоит в группах не прямое наследование**

13.2.1. Состоит в группах

В этом поле отображены два списка с группами:

- **Выбранные группы** — список с групп, в которых состоит пользователь;
- **Все группы** — список групп, доступных вступления.

Для того чтобы добавиться в одну или несколько групп, необходимо в списке **Все группы** отметить требуемые группы и перенести их в **Выбранные группы** нажав кнопку [**<-**], расположенную между этими списками. Чтобы выйти из одной или нескольких групп, необходимо в списке **Выбранные группы** отметить требуемые группы и перенести их в **Все группы** нажав кнопку [**->**], расположенную между этими списками.

Для списка **Все группы** так же доступна возможность добавления в список новых групп с помощью кнопки [**+ Новая группа**].

Для списков групп доступен поиск по названию. Для этого в соответствующем поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Внизу списков указано количество записей в данном списке.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

13.2.2. Состоит в группах не прямое наследование

В этом поле отображены группы имеющие не прямое наследование, в которых состоит владелец личного кабинета.

Для списка групп доступен поиск по названию. Для этого в соответствующем поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Внизу списков указано количество записей в данном списке.

13.3. Дополнительные сведения

На вкладке **Дополнительные сведения** приведены поля ввода данных:

- **Дополнительный номер телефона;**
- **Дата приема на работу;**
- **Дополнительные сведения;**
- поле с указанием пола пользователя ([М] или [Ж]);
- **Табельный номер.**

13.4. Групповые политики

На этой вкладке приведен список групповых политик, которые распространяются на владельца личного кабинета.

13.5. Расширенные настройки

На этой вкладке приведены поля ввода для дополнительных адресов пользователя.

13.6. Назначенные роли

На вкладке **Назначенные роли** приведены и отображены два списка с типами администратора:

- **Выбранные роли** — список типов администратора, присвоенных пользователю;
- **Все роли** — список типов администратора, доступных для присвоения пользователю.

Для того чтобы присвоить одну или несколько ролей, необходимо в списке **Все роли** отметить требуемые типы администратора и перенести их в **Выбранные роли**, нажав кнопку [**<**], расположенную между этими списками. Чтобы исключить пользователя из

обладателя одного или нескольких типов администратора, необходимо в списке **Выбранные роли** отметить требуемые типы администратора и перенести их в **Все роли**, нажав кнопку [->], расположенную между этими списками.

Для списков ролей доступен поиск по названию. Для этого в соответствующем поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Внизу списков указано количество записей в данном списке.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

Пользователям без роли или без привилегии на чтение пользователей (Users - Read) доступен только ЛК с возможностью сброса пароля и изменения полей:

- «Номер мобильного телефона»;
- «Открытые ключи SSH».

Пользователям с привилегией на чтение пользователей (Users - Read) доступен ЛК в разделе «Пользователи и компьютеры» -> Пользователи-> Карточка текущего пользователя; просмотр всех вкладок, кроме «Дополнительные сведения»; изменение полей:

- «пароль»;
- «Номер мобильного телефона»;
- «Открытые ключи SSH»;

Остальные поля и таблицы - только для чтения.

Пользователям с привилегией на редактирование пользователей (Users - Modify) доступны все поля для изменения на вкладках «Основное» и «Расширенные настройки». Для изменения других вкладок требуются соответствующие привилегии «Modify».