ALD Pro

ИНСТРУКЦИИ

НАСЛЕДОВАНИЕ И СУММИРОВАНИЕ ПАРАМЕТРОВ ГРУППОВЫХ ПОЛИТИК

Версия 2.4.1

Содержание

Аннотация

Настоящий документ объясняет порядок наследования и суммирования параметров групповых политик в ALD Pro в сравнении с Microsoft Active Directory (MS AD).

Термины и определения

Термин	Альтернатива	Определение
Групповая политика	ГП	Разделы параметров, с помощью которых можно выполнить централизованную настройку ОС и окружения пользователя. Например, «безопасность», «оборудование», «сеть», «система».
Объект групповой политики	ГПО, (group policy object, gpo), Объект ГПО	Именованный набор параметров с конкретными значениями, которые могут быть назначены на структурные подразделения. В ALD Pro соответствуют записям в DN`cn=gpolicy,cn=gp,cn=domain_suffix`
Параметр групповой политики		Именованный набор атрибутов, которые позволяют сконфигурировать определенную функцию операционной системы или окружения пользователя. Например, параметр «Переменная окружения» объединяет такие атрибуты как «Имя переменной» и «Значение переменной».
Атрибут параметра групповой политики		Именованное значение, которое позволяет управлять конкретной настройкой операционной системы или окружения пользователя. Например, атрибуту «Имя переменной» можно присвоить значение «var1»
Связанный объект ГП	Связанный ГПО, Назначенный ГПО, gpo link	Объект групповой политики, назначенный на конкретное подразделение. В ALD Pro соответствуют записям в DN`cn=gprules,cn=gp,dc=domain_suffix`
Наследуемые ГПО		Объекты групповых политик, назначенные на родительские подразделения, параметры которых по умолчанию наследуются дочерними подразделениями. В ALD Pro соответствуют записям в DN`cn=gprules,cn=gp,dc=domain_suffix`
Простой параметр		Параметр групповой политики, имеющий один список атрибутов.
Составной параметр	Списочный параметр	Параметр групповой политики, атрибуты которого представлены массивом списков.
Подразделение	Organizational unit, ou	Структурные подразделения организации, предназначенные для группировки объектов, чтобы на них можно было назначать ГПО. В**ALD Pro** соответствуют записям в DN `cn=orgunits,cn=accounts,dc=domain_suffix`
Приоритет		Целое число, определяющее порядок применения параметров ГПО, если на одно подразделение назначено несколько объектов. Если у объекта приоритет равен единице, то его параметры будут применяться в самую последнюю очередь и смогут переопределить все ранее установленные значения в соответствии с правилами суммирования. В ALD Pro соответствует атрибут`rbtaprioritypolicy` в `gprules`
Флаг «Отключить наследование»	block inheritance	Устанавливается для подразделения и позволяет отключить наследование параметров, определенных в объектах групповых политик, назначенных на родительские (вышестоящие) подразделения.
Флаг «Наследовать принудительно»	enforced	Устанавливается для связанного объекта ГП (gpo link) и позволяет сделать наследование параметров соответствующего объекта обязательным на все дочерние подразделения, даже если где-то наследование отключено. В**ALD Pro** еще нет этого параметра, должен стать атрибутом записей в DN `cn=gprules,cn=gp,dc=domain_suffix`
Флаг «Связь включена»	Link Enebled	Устанавливается для связанного объекта**ГП** (gpo link) и позволяет отключить применение параметров соответствующего объекта, не удаляя назначение ГПО на структурное подразделение.
Флаг «Состояние объекта групповой политики»	GPO Status	Устанавливается для ГПО и позволяет отключить применение параметров этого объекта, не удаляя настроек. Переключатель имеет следующие состояния: а) Все параметры (enabled) - применяются все параметры ГПО при его назначении на структурное подразделение, б) Параметра пользователей, в) Параметры компьютеров

Предварительные настройки

3.1. Создание дополнительных параметров групповых политик

Если для работы с функционалом групповых политик будут созданы дополнительные параметры групповых политик, необходимо воспользоваться инструкцией add_parameter_GP.

3.2. Создание объекта групповой политики

Для создания объектов групповой политики необходимо перейти в подраздел group_policies_2 (раздел group_policies_1)

Наследование

В домене **ALD Pro** назначить объект групповой политики (далее - ГПО) возможно только на подразделения. ГПО, назначенный на подразделение, называется связанным объектом групповой политики. Назначение ГПО на подразделение возможно 2 способами:

- Групповые политики → Групповые политики → {Имя ГПО} → Подразделения;
- Более удобный способ: Пользователи и компьютеры → Организационная структура → {Имя подразделения} → Групповые политики.

При назначении ГПО на структурное подразделение, его параметры по умолчанию наследуются пользователями/компьютерами всех нижестоящих подразделений. На рис. 1 показано, что на Целевой компьютер распространяется действие как объектов групповой политики ГПО-7 и ГПО-8, назначенных на OU3 напрямую, так и объектов ГПО-1 … ГПО-6, назначенных на вышестоящие подразделения. Приоритет ГПО - это выставленный пользователем приоритет ГПО в рамках выбранного подразделения. Порядок применения - порядок в котором параметры ГПО будут суммироваться.

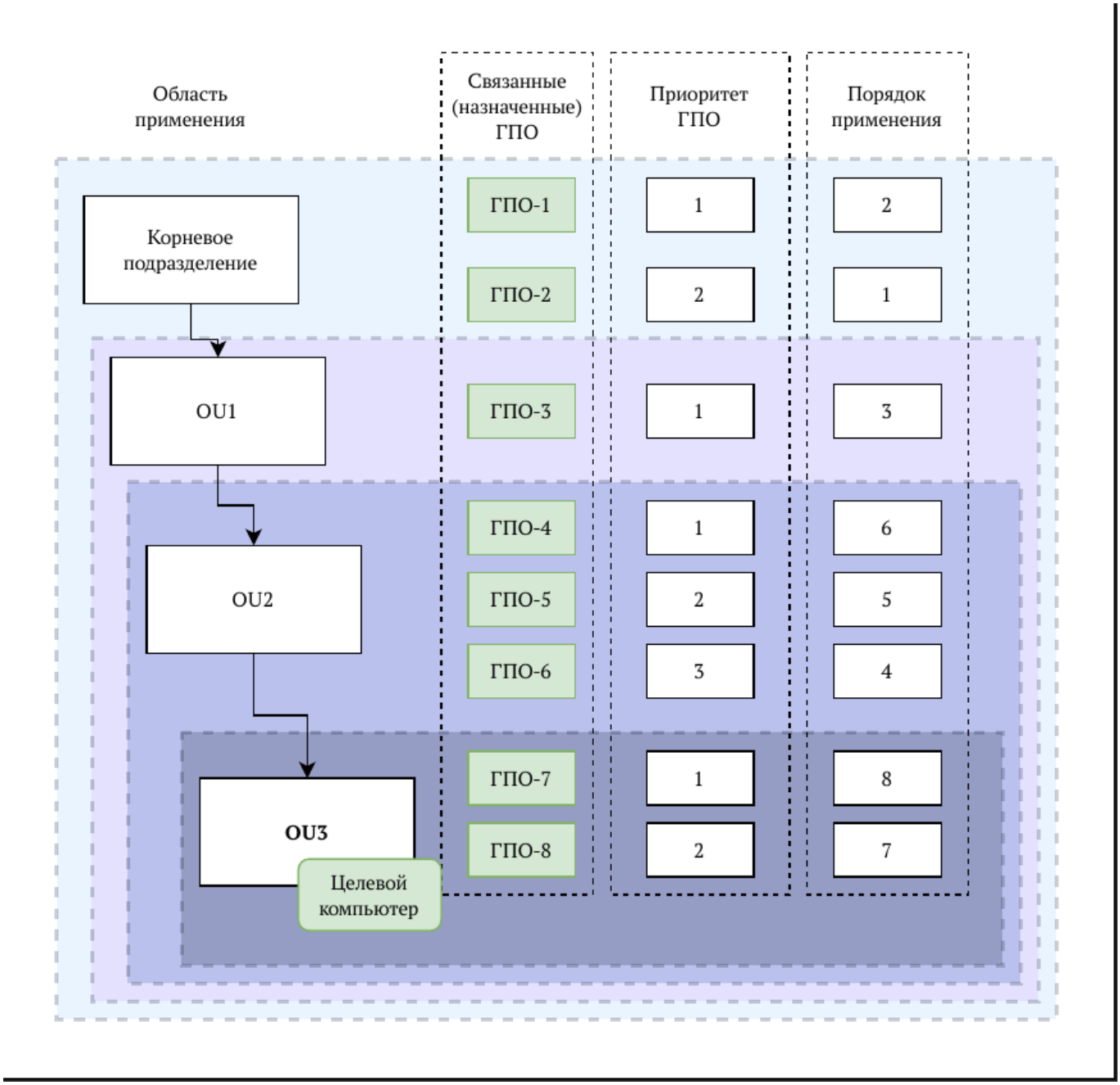

Рис. 1. Порядок наследования суммирования групповых политик

4.1. Флаг «Отключить наследование»

С 2.4.0 в домене **ALD Pro** для структурного подразделения можно установить флаг **Включить наследование** (аналог `Block Inheritance` (отключить наследование) в MS AD), что позволит включать и отключить наследование параметров, определенных в объектах групповых политик, назначенных на родительские (вышестоящие) подразделения, см. рисунок 2.

По умолчанию наследование включено для всех подразделений. Функция удобна для отладки или если в рамках организационной структуры есть объекты, на которые нужно назначить принципиально иные настройки. Например, в рамках московского офиса может быть open space или компьютерный класс, для которых проще задать настройки заново, чем переопределять общие настройки, заданные для офиса в целом.

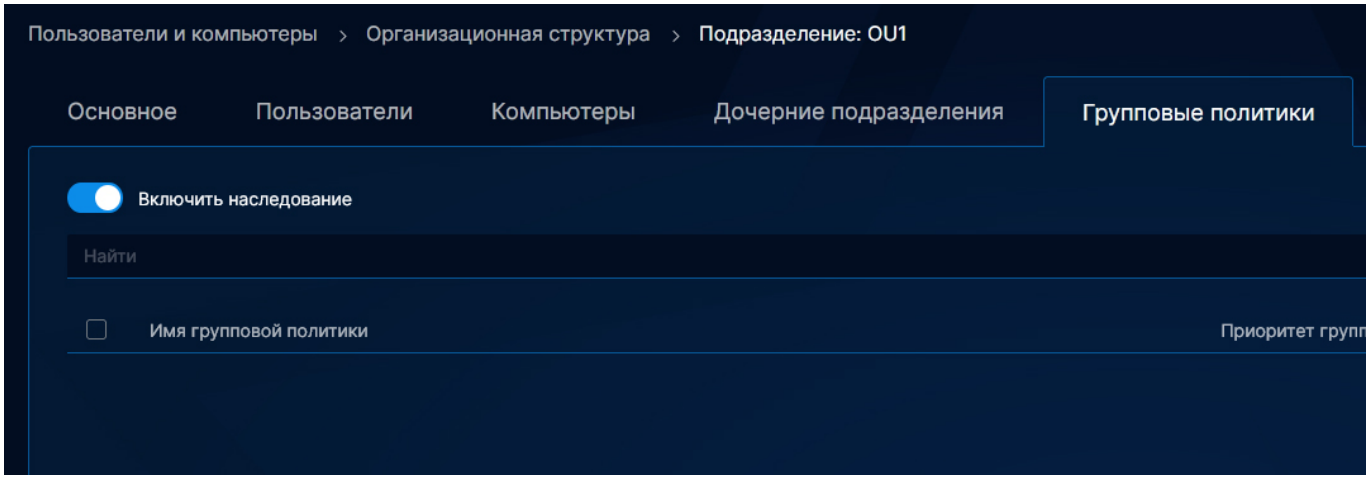

Рис. 2. Включение наследования ГПО для структурного подразделения в интерфейсе ALD Pro

Если отключить наследование для OU1, то объекты групповой политики ГПО-1 и ГПО-2, назначенные на Корневое подразделение, перестанут распространять свое действие на Целевой компьютер. Применяться будут только объекты ГПО-3 … ГПО-8, см. рисунок 3.

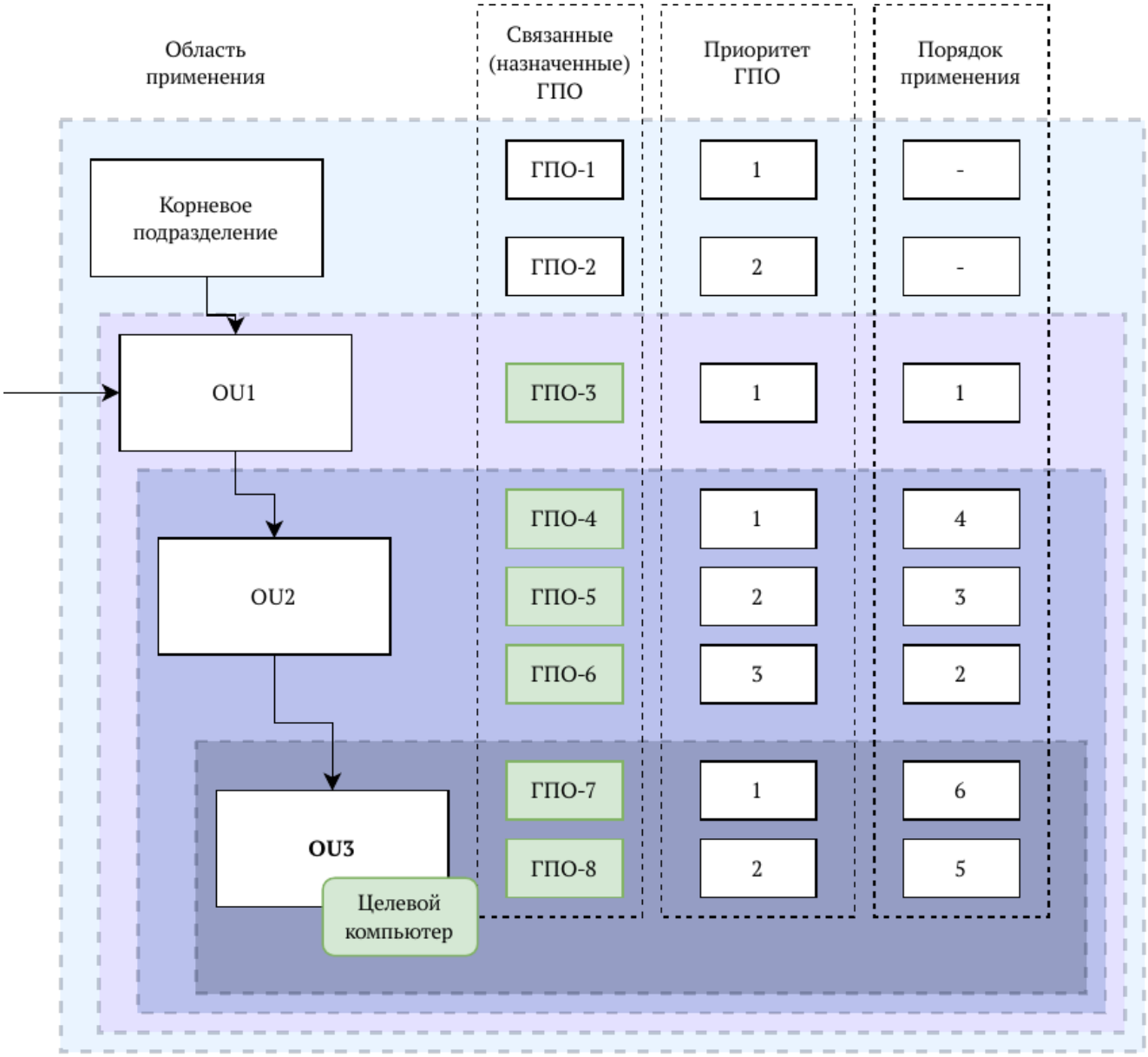

Рис. 3. Иллюстрация работы блокировки наследования ГПО для структурного подразделения

4.2. Флаг «Наследование принудительно»

С **ALD Pro** версии 2.4.0 для связанного ГПО, можно установить флаг **Наследовать принудительно** (аналог флага `Enforced` (Наследовать принудительно) в MS AD), что позволит сделать наследование параметров соответствующего объекта групповой политики обязательным для всех дочерних подразделений, даже если где-то наследование отключено, см. рисунок 4.

По умолчанию флаг выключен для всех ГПО. Более того, связанные ГПО, отмеченные флагом **Наследовать принудительно**, применяются после обычных ГПО, поэтому переопределяют их значения. То есть алгоритм суммирования имеет два вложенных цикла, сначала суммирует параметры обычных ГПО, потом сверху накладывает суммирование `Enforced` ГПО. Функция удобна, например, для настройки параметров безопасности, действие которых должно распространяться на все структурные подразделения, вне зависимости от того, используется ли отключение наследования или нет.

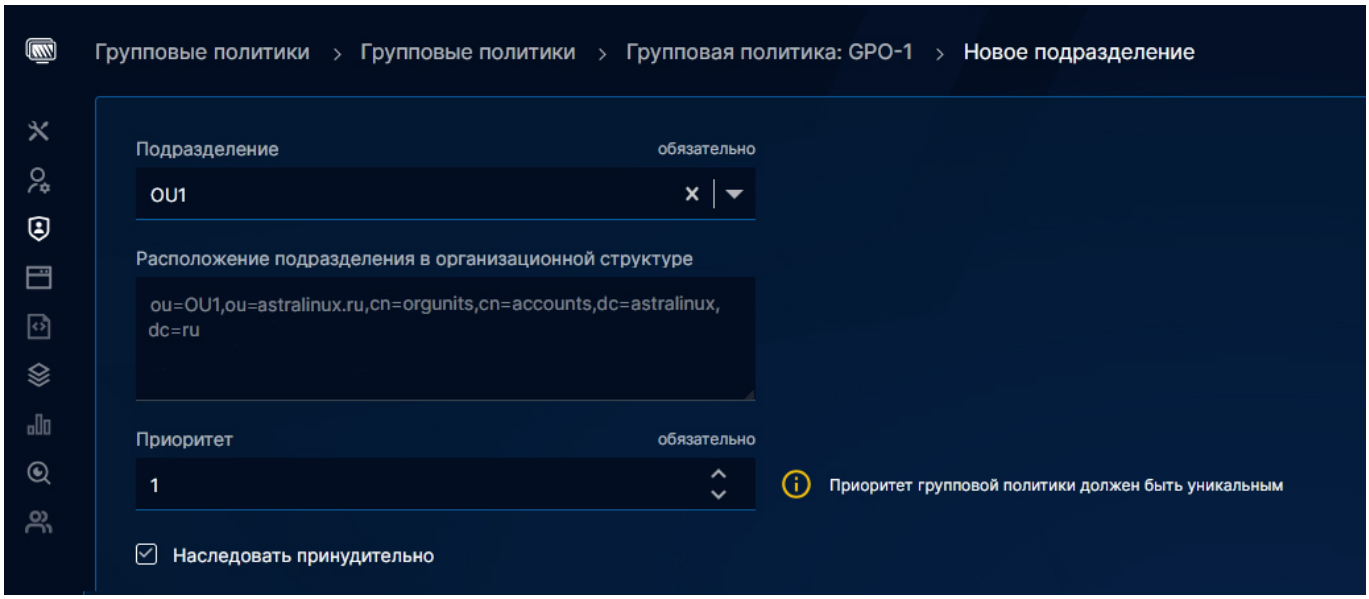

Рис. 4. Включение принудительного наследования параметров для связанного ГПО в интерфейсе ALD Pro

Если для ГПО-1 включить флаг принудительного наследования, то параметры этого объекта будут применяться к Целевому компьютеру, не смотря на то, что для OU1 установлен флаг на запрет наследования. В итоге будут применяться объекты ГПО-1, ГПО-3 … ГПО-8, см. рисунок 5.

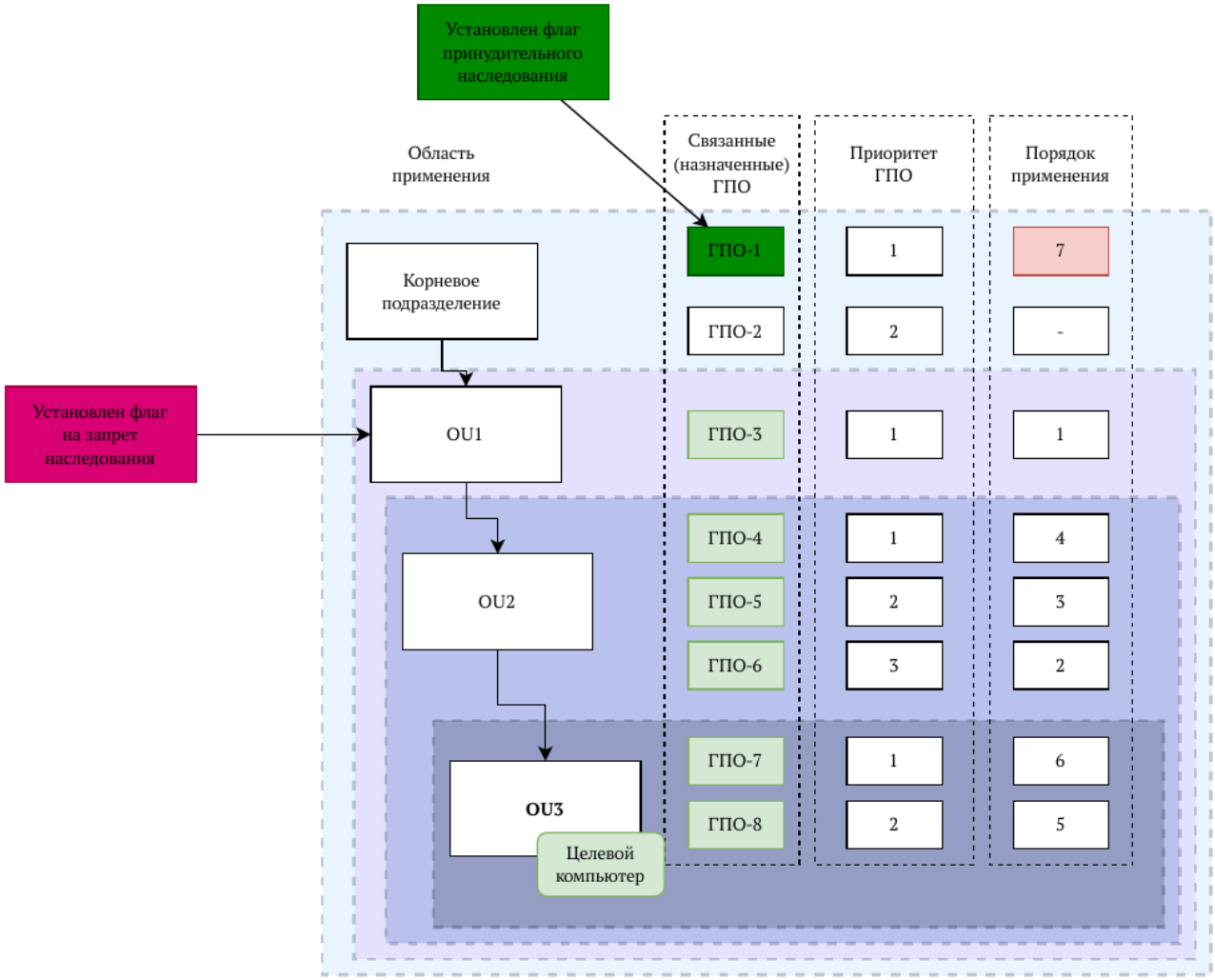

Рис. 5. Иллюстрация работы флага принудительного наследования для ГПО

Суммирование

5.1. Порядок суммирования

Если пользователь или компьютер попадает в область действия нескольких объектов групповых политик, их параметры суммируются следующим образом:

1. Если на одно и тоже структурное подразделение назначено несколько объектов групповых политик, то порядок применения параметров устанавливается с помощью приоритета. Приоритет представляет из себя целое число, если приоритет равен единице, то параметры этого ГПО будут применяться в самую последнюю очередь и смогут переопределить ранее установленные значения в случае конфликтов. На рисунке 6 показано, что на подразделение OU3 назначено два объекта GPO-7 и GPO-8 и первым из них применяется GPO-8, т.к. у него приоритет 2, а вторым GPO-7, поэтому параметры GPO-7 будут перетирать параметры GPO-8 в случае конфликтов.

2. Если ГПО назначены на разные подразделения, то порядок их применения определяется иерархией подразделений. Чем ближе ГПО по иерархии к целевому пользователю/компьютеру, тем позже будут применяться параметры этого объекта, поэтому параметры этого ГПО смогут переопределить ранее установленные значения в случае конфликтов. На рисунке 6 показано, что GPO-1 и GPO-2, назначенные на корневое подразделение, применяются в самом начале, а GPO-7 и GPO-8, которые назначены на OU3, в котором компьютер находится непосредственно, выполняются в последнюю очередь.

Конфликтом считается если на целевого пользователя/компьютер назначено несколько одинаковых параметров групповых политик, которые наследуются от разных ГПО.

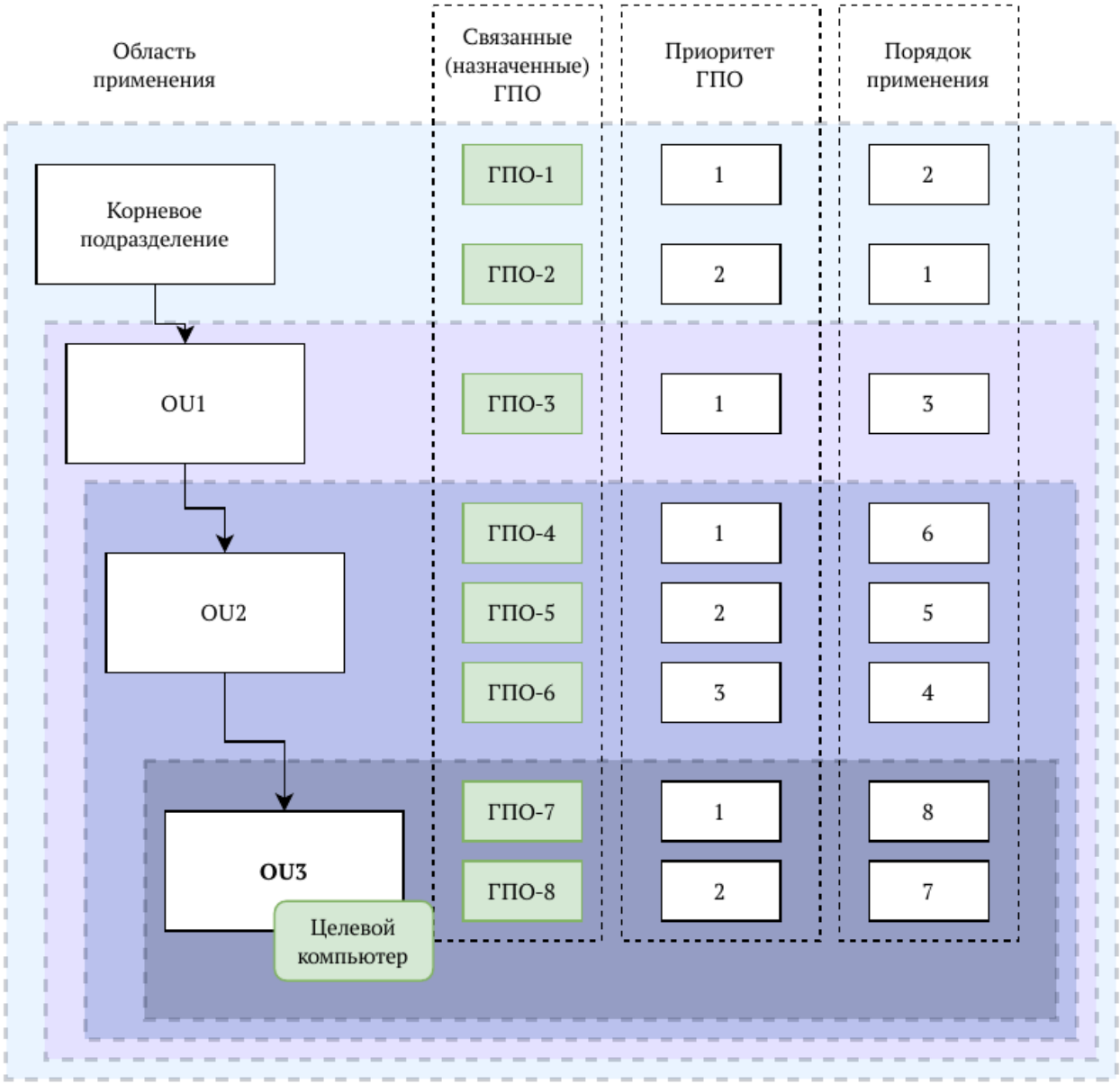

Рис. 6. Порядок суммирования ГПО

5.2. Механика разрешения конфликтов для простых параметров

Простой параметр имеет один список атрибутов, и если такой параметр определен в нескольких ГПО, остается один список значений атрибутов согласно правилам суммирования и наследования. В этом случае берется список атрибутов целиком, и, если какие-то из атрибутов не определены, то будет взято его «пустое» значение.

5.3. Механика разрешения конфликтов для составных (списочных) параметров

В домене ALD Pro есть составные (списочные) параметры для которых можно задавать таблицу однотипных таблицу атрибутов, например, ярлыки, принтеры и т.п. Если такой параметр определен в нескольких объектах ГПО, то после суммирования получатся результирующий массив строк в том же порядке, в котором параметры должны применяться на целевом хосте. Бизнес-логика разрешения конфликтов для составных параметров может различаться. Есть 3 типа разрешения конфликтов для составных параметров:

Тип разрешения конфликта	Описание работы
С уникальными атрибутами	Составные параметры, у которых возможны конфликты. Для разрешения конфликтов для каждого параметра определен уникальный атрибут. В рамках одного ГПО нельзя создать массив списка атрибутов с одинаковыми значениями уникального параметра. Результат суммирования будет состоять из массива списка атрибутов с неповторяющимися значениями уникальных атрибутов в случайном порядке.
Без уникальных атрибутов	Составные параметры, массивы списка атрибутов, которых суммируются без конфликтов.
Комбинация уникальных атрибутов	Составные параметры, у которых массивы списка атрибутов считаются уникальными при комбинации атрибутов. С точки зрения работы механизма Групповых политик, эти составные атрибуты суммируются аналогично типу «Без уникальных атрибутов».Конфликты в этом случае разрешаются на стороне операционной системы.

5.3.1. Поведение составных параметров компьютеров

В таблице ниже приведено описание работы каждого составного параметра компьютеров, в зависимости от его типа.

	Параметр	Уникальный атрибут	Поведение при конфликте в случае суммирования и наследования
	С уникальными атрибутами		Нельзя создать в рамках одного ГПО массивы списка атрибутов одинаковыми значениями уникальных атрибутов.
1	Безопасность → Глобальные настройки киоска → Автозапуск приложения в киоске	Путь до исполняемого файла.*Название в БД:* `rbta_ldap_kiosk_global_parametrs__app__path`	
2	Безопасность → Конфигурация параметра ядра	Имя конфигурационного файла.*Название в БД:*`rbta_ldap_kernel_parametrs__params__name`	
3	Безопасность → Мандатные атрибуты → Категории	Наименование.*Название в БД:* `rbta_ldap_mandate_attrs__categories__name`	
4	Безопасность → Мандатные атрибуты → Уровни конфиденциальности	Наименование.*Название в БД:* `rbta_ldap_mandate_attrs__levels__name`	
5	Безопасность → Мандатный целостности (**МКЦ**) → Исключения конфигурации защиты файловой системы	Путь к объекту.*Название в БД:* `rbta_ldap_integrity_control__fs_protection_exceptions__exception`	
6	Безопасность → Мандатный целостности (**МКЦ**) → Конфигурация защиты файловой системы	Путь к объекту.*Название в БД:* `rbta_ldap_integrity_control__fs_protection_config__path`	
7	Безопасность →**Политика** очистки памяти → Настройка гарантированного удаления файлов на устройстве	Адрес устройста или точка монтирования.*Название в БД:* `rbta_ldap_memory_clearing__drives__path`	
8	Безопасность → Управление квотами → Квота устройства	Адрес устройста или точка монтирования.*Название в БД:* `rbta_ldap_quotas__drives__path`	
9	Система → Вход в систему → Изображение пользователя	Логин пользователя.*Название в БД:*`rbta_ldap_login__user_pics__login`	
10	Система → Дата и время → Параметры сервера или пула сетевого времени	Адрес сервера или пула.*Название в БД:*`rbta_ldap_date_time_h__servers__name`	
11	Система → Приложение для типа файлов	Перечень mime-типов.*Название в БД:*`rbta_ldap_mimeapps_h__local__mimes`	
12	Система → Системная альтернатива	Символическая ссылка.*Название в БД:*`rbta_ldap_system_alternatives__alternatives__name`	
13	Безопасность → Санкции PolicyKit-1 → Привилегированное действие	Название привилегированного действия.*Название в БД:*`rbta_ldap_policykit__actions__explicit_name`	
	Без уникального атрибута		Все массивы атрибутов суммируются и появляются в интерфейсе.
14	Безопасность → Управление квотами → Расписание проверки квот	Нет уникального атрибута	
15	Оборудование → Редактор маркеров → Входная переменная	Нет уникального атрибута	
16	Оборудование → Редактор маркеров → Маркер	Нет уникального атрибута	
17	Система → Переменная окружения	Нет уникального атрибута	
18	Система → Планировщик задач → Планировщик задач пользователя cron	Нет уникального атрибута	
	Третья категория		
19	Безопасность → Управление квотами → Индивидуальная квота	Комбинация «Адрес устройства или точка монтирования» + «Имя группы пользователей или логин пользователя».	При полном совпадении атрибутов «Адрес устройства или точка монтирования» + «Имя группы пользователей или логин пользователя» квота создастся только одна, первая которая была применена.
20	Оборудование → Установить принтер(ы)	Комбинация «Имя принтера» + «Имя сервера печати».	При полном совпадении атрибутов «Имя принтера» + «Имя сервера печати» принтер появится только один.
21	Сеть → Настройка межсетевого экрана → Обычное правило	Комбинация «**Политика**» + «Направление» + «Протокол» + «Порт».	При полном совпадении атрибутов «**Политика**» + «Направление» + «Протокол» + «Порт» новые правила с такими же атрибутами не создаются.
22	Сеть → Настройка межсетевого экрана → Предустановленное правило	Уникальна комбинация «**Политика**» + «Направление» + «Протокол» + «Порт», **ОС** сама разруливает конфликт в случае дублей принтеров.	При полном совпадении атрибутов «Наименование предустановленного приложения» + «**Политика**» + «Направление» новые правила с такими же атрибутами не создаются.
23	Сеть → Настройка межсетевого экрана → Расширенное правило	Комбинация «**Политика**» + «Направление» + «Протокол» + «Порт».	При полном совпадении атрибутов «**Политика**» + «Направление» + «Протокол» + «Порт» новые правила с такими же атрибутами не создаются.
24	Система → Планировщик задач → Переменная пользователя cron	Нет уникального атрибута, графика дает создавать одинаковые переменные пользователя cron.	Все массивы атрибутов суммируются и появляются в интерфейсе. Дальнейшее применение зависит от операционной системы, в основном случае будет использована последняя добавленная переменная.

5.3.2. Поведение составных параметров пользователей

В таблице ниже приведено описание работы каждого составного параметра компьютеров, в зависимости от его типа.

	Параметр	Уникальный атрибут	Поведение при конфликте в случае суммирования и наследования
	1 категория		Нельзя создать в рамках одного ГПО массивы списка атрибутов одинаковыми значениями уникальных атрибутов.
1	Оборудование → Значение для предпросмотра редактора маркеров	Название переменной.*Название в БД:* `rbta_ldap_marker_editor_u__preview_values__name`	
2	Оборудование → Обработка «горячего» подключения	*Имя.Название в БД:*`rbta_ldap_fly_reflex__actions__name`	
3	Рабочий стол → Параметры окон → Настройки программы или класса окон	Название программы или класса окон.*Название в БД:* `rbta_ldap_windows_settings__presets__name`	
4	Система → Приложения для типов файлов → Приложение для типа файлов	Перечень mime-типов.*Название в БД:* `rbta_ldap_mimeapps_u__local__mimes`	
5	Оборудование → Электропитание → Настройки уведомлений о событиях	Наименование уведомления.*Название в БД:* `rbta_ldap_power_management__notifications__event`	Нельзя создать в рамках одного ГПО массивы списка атрибутов одинаковыми значениями уникальных атрибутов.Итоговое количество настроенных уведомлений не более 6, потому что поле «Наименование уведомления» может содержать только одно из 6 значений: pluggedin, unplugged, fullbattery, lowbattery, criticalbattery, lowperipheralbattery
	2 категория		Все массивы атрибутов суммируются и появляются в интерфейсе.
6	Рабочий стол → Меню «Пуск» → Каталог	Нет уникального атрибута	
7	Рабочий стол → Меню «Пуск» → Приложение	Нет уникального атрибута	
8	Рабочий стол → Меню «Пуск» → Ссылка	Нет уникального атрибута	
9	Рабочий стол → Панель быстрого запуска → Каталог	Нет уникального атрибута	
10	Рабочий стол → Панель быстрого запуска → Приложение	Нет уникального атрибута	
11	Рабочий стол → Панель быстрого запуска → Приложение	Нет уникального атрибута	
12	Система → Автозапуск → Приложение	Нет уникального атрибута	
13	Система → Автозапуск → Ссылка	Нет уникального атрибута	
14	Система → Переменные окружения → Переменная окружения	Нет уникального атрибута	

5.3.3. Суммирование дополнительных параметров ГП

Суммирование дополнительных параметров ГП не отличается от коробочных. Для составных дополнительных параметров ГП можно настроить уникальный атрибут.

Просмотр смоделированного отчета о назначенных параметрах ГП

Для каждого компьютера и пользователя можно посмотреть моделирование результатов применения групповых политик (рисунок 7). (см. Пользователи и Компьютеры).

Для компьютера: **Пользователи и компьютеры → Компьютеры → {Имя компьютера} → Групповые политики**. Для пользователя: **Пользователи и компьютеры → Пользователи → {Логин пользователя} → Групповые политики**. Данный список представляет собой моделирование результатов применения групповых политик. Это значит, что не все параметры из данного списка могут быть применены к конкретному пользователю и не все политики могут быть отображены в данном списке. Чтобы групповая политика применилась к пользователю, необходимо соблюдать требования к операционной системе и заполненять значения атрибутов.

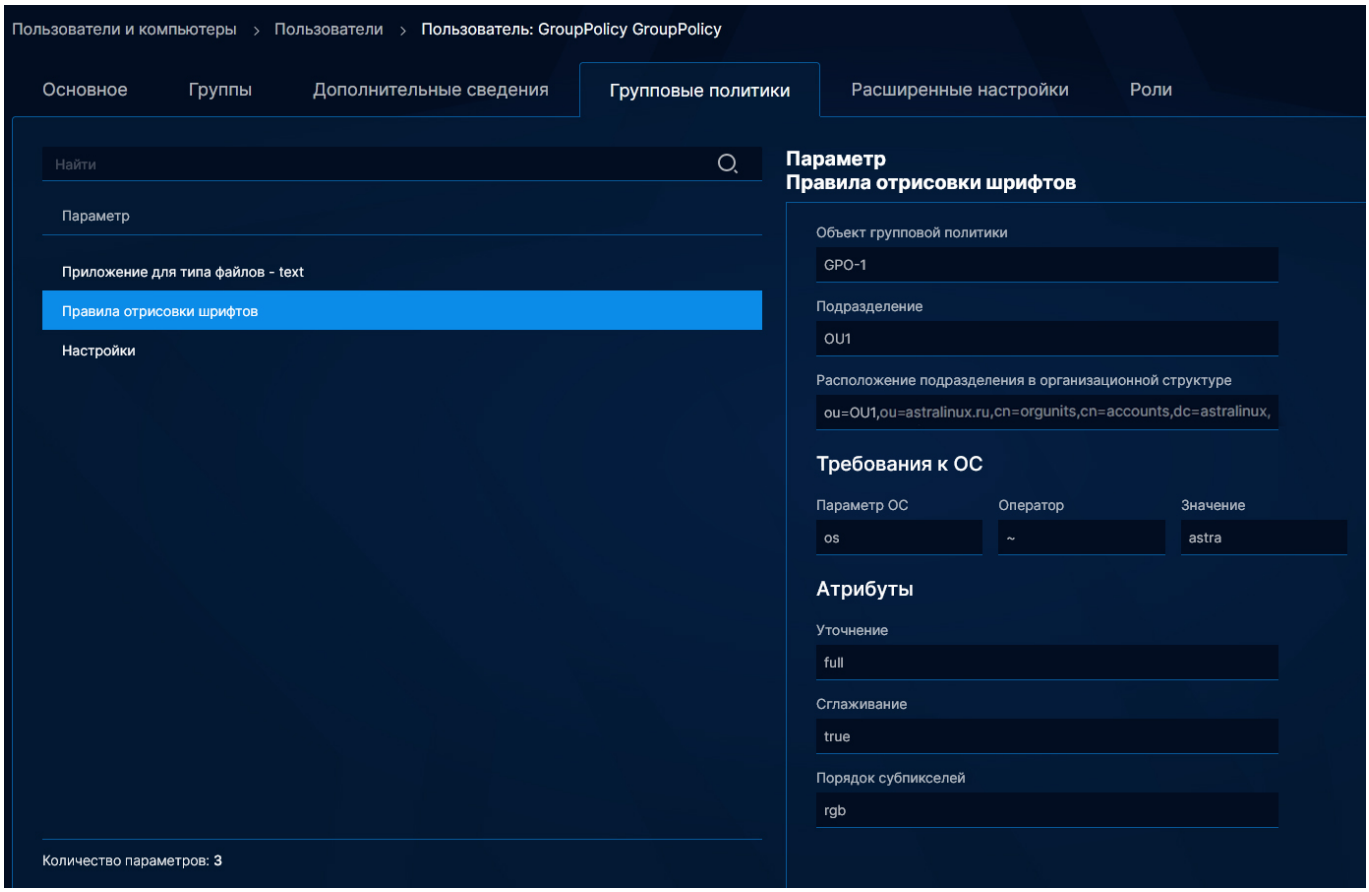

Рис. 7. Моделирование результата применения параметров ГП на пользователя