ГАЗИНФОРМ СЕРВИС

Программный комплекс по защите системно-технической инфраструктуры «Efros Defence Operations»

Руководство пользователя
Часть 3
Контроль устройств

Приложение А
Настройка возможностей контроля целостности функционального модуля «Efros ICC»

Санкт-Петербург, 2024

Аннотация

Данный документ является приложением документа «Руководство пользователя. Часть 3. Контроль устройств» и входит в комплект пользовательской документации для работы с программным комплексом по защите системно-технической инфраструктуры «Efros Defence Operations» (далее – ПК «Efros DO» или комплекс).

Полный комплект пользовательской документации приведен в документе «Описание применения».

Данное приложение содержит описание рекомендуемой последовательности работы для настройки возможностей контроля целостности функционального модуля «Efros Integrity Check Compliance» («Efros ICC»).

Модуль «Efros ICC» реализует следующие возможности контроля целостности:

- контроль изменения конфигураций операционной системы (ОС), прикладного программного обеспечения (ППО), виртуализации, контейнеров и средств оркестрации;
- контроль целостности файлов ОС, ППО, виртуализации, контейнеров и средств оркестрации;
- проверки соответствия безопасности ОС, ППО, виртуализации, контейнеров и средств оркестрации.

Для работы с возможностями контроля целостности необходимо убедиться в установке лицензии модуля «Efros ICC».

Знаки, расположенные на полях руководства, указывают на примечания.

Степени важности примечаний:

Важная информация
Указания, требующие особого внимания.

Дополнительная информация
Информация, позволяющая упростить работу с ПК «Efros DO».

Представленные в документе снимки экрана могут отличаться для различных версий поставляемого комплекса и предназначены для демонстрации работы комплекса.

Содержание

1 Общие сведения

1.1 Предварительная настройка

Общие вопросы администрирования комплекса рассмотрены в первой части руководства пользователя (см. документ «Руководство пользователя. Часть 1. Настройка и администрирование»).

Для работы с модулем «Efros ICC» необходимо произвести следующие подготовительные действия:

1) Загрузить внешние модули для работы с устройствами.
2) Проверить установку внешних модулей, перейдя в раздел «Настройки», подраздел «Модули». Убедиться в том, что необходимые модули включены – переключатель «Состояние» активен « ».

Перечень типов устройств, поддерживаемый функциональным модулем «Efros ICC», приведен в документе «Описание применения».

3) Добавить объект защиты (устройство) с возможностью «Контроль устройств» в разделе «Объекты сети» или «Контроль устройств».
4) Установить для устройства тип контроля «INTEGRITY CHECK COMPLIANCE».

Применение типа контроля «INTEGRITY CHECK COMPLIANCE» предусмотрено для:

- ОС и ППО;
- систем управления базами данных (СУБД);
- виртуализации;
- контейнеров и средств оркестрации.

Допустимо создание вложенных устройств. Например, создать ППО внутри группы созданной ОС.

При наличии в комплексе настроенной иерархии и, если пользователю назначены права доступа к различным серверам иерархии, то перед выполнением действий по контролю целостности пользователю необходимо выбрать в главном меню сервер, к которому подключено контролируемое оборудование (подробнее см. документ «Руководство пользователя. Часть 1. Настройка и администрирование»).

1.2 Схема работы ПК «Efros DO»

Схема работы ПК «Efros DO» в рамках контроля целостности (рис. 1):

1) На устройстве с включенным типом контроля «INTEGRITY CHECK COMPLIANCE» изменили конфигурацию.
2) Комплекс запускает проверку изменений и выявление нарушений конфигурации. Изменения фиксируются в отчете.
3) Комплекс отправляет письмо или Syslog сообщение ответственным лицам.
4) Пользователь, получив письмо или уведомление при работе в комплексе, открывает уведомление и изучает изменения, приведенные в отчете.
5) Пользователь принимает изменения или отклоняет, выясняя причину изменений с последующей их отменой.

Рисунок 1 – Схема работы ПК «Efros DO» в рамках контроля целостности

1.3 Рекомендуемая последовательность действий для настройки возможностей контроля целостности

Рекомендуемая последовательность действий для настройки возможностей контроля целостности устройств приведена в таблице 1.

Таблица 1 – Последовательность действий для настройки возможностей контроля целостности устройств

№ п/п	Действие	Раздел веб-интерфейса комплекса	Описано в разделе документа
1	Ознакомиться с предустановленными отчетами устройств	«Контроль устройств» → «Устройства» → вкладка «Отчеты»	2.1 и 3.1
2	Назначить тип использования для отчетов конфигурации устройств («Архив версий», «Запрещено», «Контроль изменений», «Только последний», «Наследовать» из профиля отчетов)		2.2
3	Назначить тип использования для проверок безопасности устройств («Запрещено», «Разрешено», «Наследовать» из профиля отчетов)		3.2
4	Создать необходимые пользовательские отчеты конфигурации устройств	«Контроль устройств» → «Профили отчетов» → вкладка «Конфигурации»	2.4, 2.5, 2.6 и 2.7
5	Создать необходимые пользовательские проверки безопасности устройств	«Контроль устройств» → «Проверка безопасности»	3.4
6	Настроить расписание опроса устройств	«Администрирование» → «Планировщик» → вкладка «По расписанию»	4.1
7	Настроить оповещения об изменениях	«Администрирование» → «Планировщик» → вкладка «По событию»	4.2

1.4 Описание подраздела «Устройства»

Отчеты по изменениям конфигурации и проверкам безопасности устройств приведены в разделе «Контроль устройств», подраздел «Устройства», вкладка «Отчеты» (рис. 2).

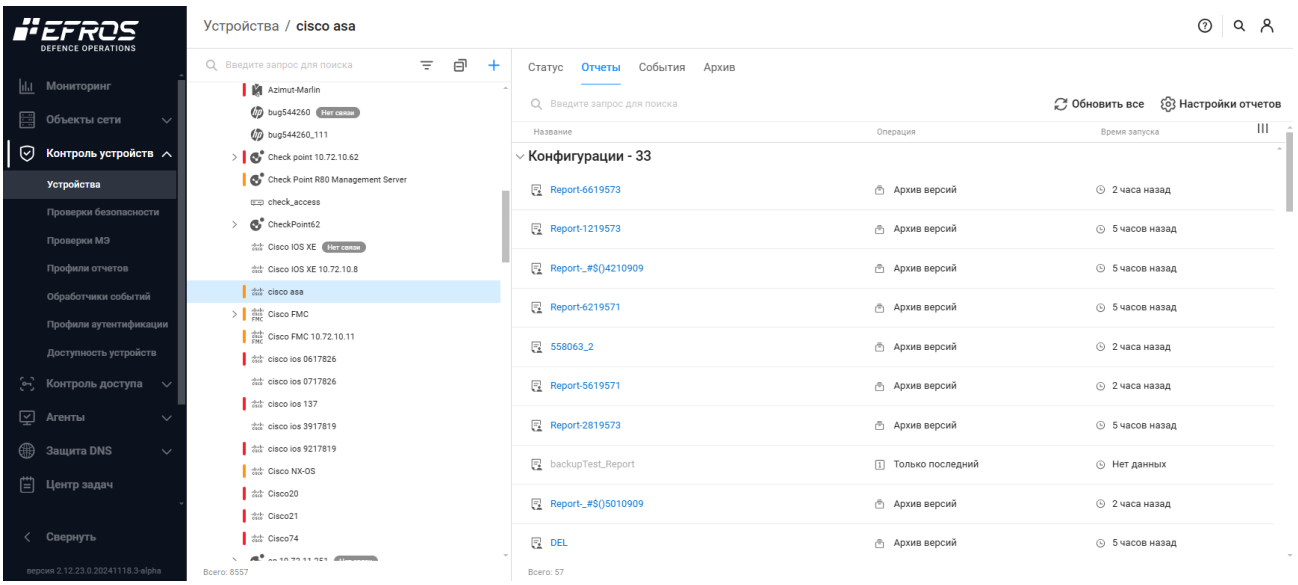


Рисунок 2 – Подраздел «Устройства»

Вкладка «Отчеты» содержит список отчетов конфигурации и проверок безопасности устройства, выбранного в дереве устройств, в соответствии с назначенным устройству профилем отчетов (подробнее про профили отчетов см. подраздел 1.5).

Отчеты могут быть как предустановленные – добавленные автоматически при подключении к комплексу внешних модулей для работы с контролируемыми устройствами, так и пользовательские – созданные пользователями на основе предустановленных.

Загрузка отчетов с устройства выполняется по нажатию кнопки «Обновить» ( ) в строке отчета либо по расписанию (подробнее о настройке расписания см. подраздел 4.1).

При нажатии кнопки «Обновить все» (Обновить все) выполняется запрос на загрузку всех отчетов с устройства, для их обработки потребуется определенное время.

Отчеты затеняются при ошибке загрузке данных с устройства. На вкладке «Статус» устройства можно посмотреть результат выполнения последней операции. Новые пользовательские отчеты также затеняются, пока не будет произведен опрос устройства по этому отчету.

1.4.1. Описание индикации элементов дерева

Описание индикации элементов дерева устройств:

Слева от иконки вендора устройства расположена полоса, цвет которой отображает наличие или отсутствие уведомлений у устройства:

- желтый – обнаружено событие;
- красный – обнаружена ошибка;
- прозрачный – уведомления отсутствуют.

Справа от названия устройства может отображаться сообщение:

- «Нет связи» – отсутствует связь с устройством;
- «Ошибка подключения» – последняя операция с устройством закончилась ошибкой аутентификации;
- «Сервисный режим» – устройство переведено в сервисный режим.

Слева от иконки группы устройств, в которую входит хотя бы одно устройство, расположена полоса, цвет которой отображает текущее состояние группы:

- желтый – обнаружено событие на устройстве, входящем в группу;
- красный – обнаружена ошибка на устройстве, входящем в группу;
- прозрачный – уведомления отсутствуют.

1.4.2. Отчеты типа «Конфигурации»

Список отчетов типа «Конфигурации» приведен на вкладке «Отчеты». Для каждой записи списка отображаются следующие пиктограммы отчетов типа «Конфигурации»:

- текстовый «»;
- структурированный «»;
- пользовательский отчет « »;
- отчет типа «Фильтр» « », созданный на основе другого отчета путем фильтрации данных;
- отчет «Правила межсетевых экранов» «»;
- правила NAT « ».

При загрузке отчета контроль целостности загружаемой версии отчета и ее сравнение с эталоном выполняется только для тех отчетов, для которых установлен вариант использования «Контроль изменений» (подробнее см. подраздел 2.2). Первый загруженный с устройства отчет становится эталонным. Если при следующей загрузке версии отчета обнаружено ее отличие от эталона, то на вкладках «Отчеты» и «Статус» устройства появится сообщение о нарушении целостности данного отчета, пользователю придет соответствующее оповещение. Пользователь имеет возможность принять текущую версию за эталон.

1.4.3. Отчеты типа «Проверки»

Список отчетов типа «Проверки» приведен на вкладке «Отчеты». Для каждой записи списка отображаются следующие пиктограммы отчетов типа «Проверки»:

- пользовательская проверка «»;
- стандартная проверка «»;
- зонный анализ «»
- проверка на уязвимости «»;
- оптимизация правил «».

Для проверок в столбце «Операции» приведены следующие данные:

- для отчетов по оптимизации правил – количество теневых и избыточных правил, а также при их наличии – неиспользуемых и нулевых правил;
- для отчетов по уязвимости устройств – количество уязвимостей, найденных при выполнении проверки, по уровню критичности, с учетом скрытых уязвимостей (аналогично блоку «Защищенность» (см. подпункт 1.4.4);
- для отчетов по проверкам безопасности – процент выполнения проверок в графическом виде и количество пройденных проверок из их общего числа;
- для других отчетов по проверкам – результат выполнения проверки – пройдена или не пройдена.

Для отчетов проверок МЭ (отчет оптимизации правил, отчеты зонного анализа и отчет стандартов МЭ) слева от значения состояния может отображаться признак их неактуальности в виде пиктограммы «» (появляется при изменении настроек отчетов проверок МЭ до обновления отчета). При наведении курсора на пиктограмму отображается всплывающая подсказка «Настройки проверки изменились, для получения актуальных данных обновите отчет». При открытии такого отчета на просмотр отображается сообщение с тем же текстом и кнопкой «Обновить». После обновления отчета пиктограмма исчезает.

1.4.4. Вкладка «Статус»

Блок «Защищенность» на вкладке «Статус» отображает результаты выполнения проверок на выбранном устройстве (рис. 3).

Результат выполнения проверок на защищенность представлен в виде количества положительно выполненных правил, содержащихся в проверке устройства.

Для группы устройств блок «Защищенность» не отображается.

Блок «Уведомления» на вкладке «Статус» отображает уведомления о произошедших событиях контроля устройства и об ошибках выполнения заданий, заданных на устройстве (рис. 4).

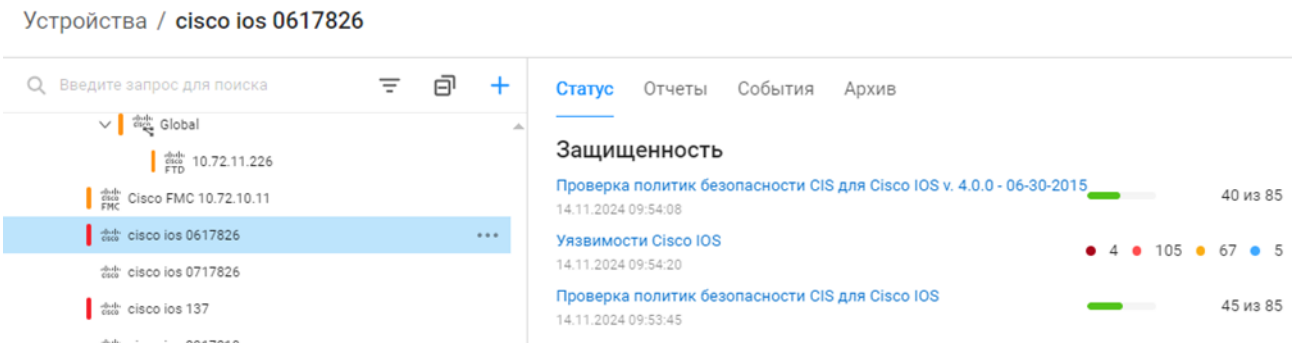


Рисунок 3 – Блок «Защищенность»

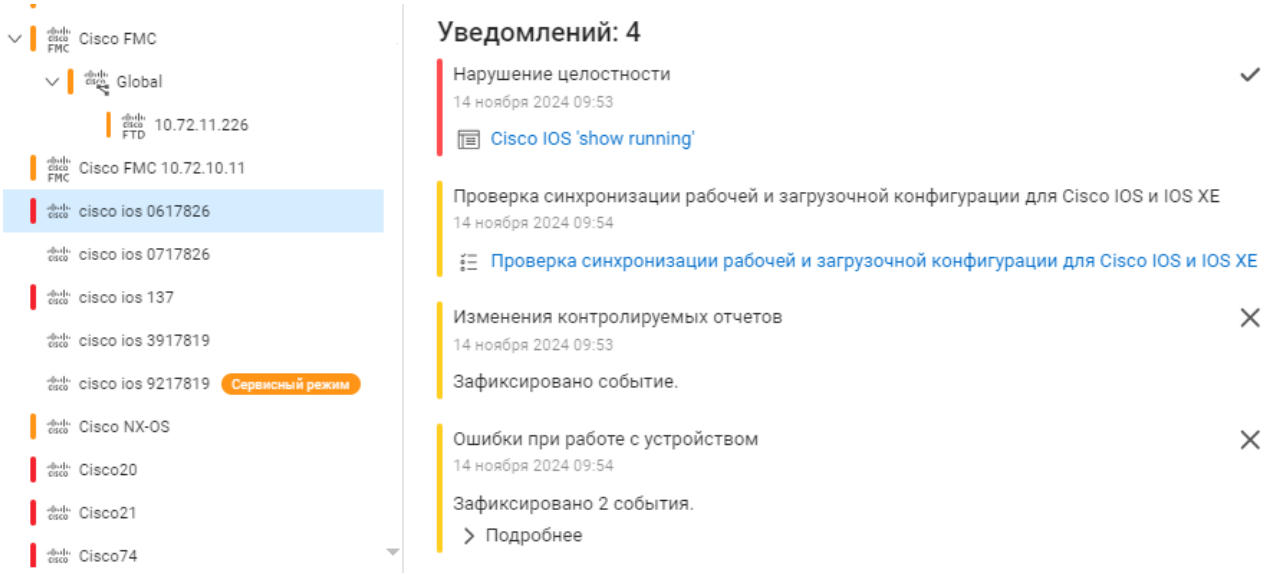


Рисунок 4 – Блок «Уведомления»

Быстрые действия с уведомлениями:

- «Удалить уведомление» (✕) для удаления выбранного уведомления;
- «Принять новую версию за эталон» (✓) для принятия новой версии загруженного отчета за эталон;
- «Переход к просмотру нарушений» – переход в окно сравнения текущего отчёта с эталоном с возможностью принятия текущего отчета за эталон;
- «Переход к отчету» – переход в окно просмотра отчета.

Блок «Информация об устройстве» на вкладке «Статус» содержит следующую информацию (рис. 5):

- текущий статус устройства:
  - недоступен (серый круг рядом с IP-адресом устройства);
  - активен (зеленый круг рядом с IP-адресом устройства).
- профиль отчетов, используемый для устройства в комплексе;
- модель устройства;

— версия установленного на устройстве ПО;
— серийный номер (при наличии);
— расписания, если они настроены для устройства;
— последняя операция, производимая с устройством.

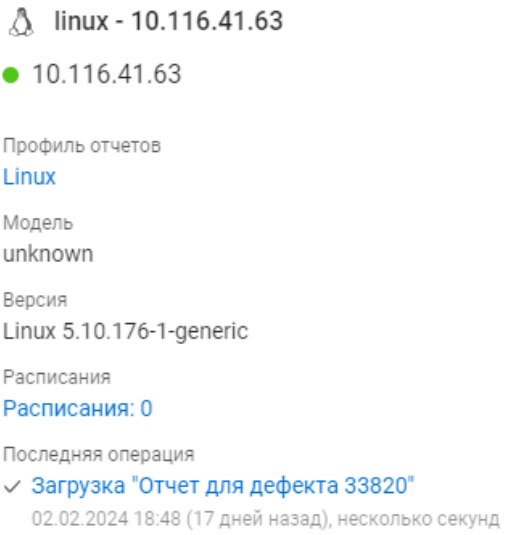


Рисунок 5 – Блок «Информация об устройстве»

Поле «Профиль отчетов» является ссылкой на подраздел «Профили отчетов» (см. подраздел 1.5).

Поле «Расписания» является ссылкой, при переходе по которой открывается вкладка «Расписания» выбранного устройства с возможностью редактирования списка используемых расписаний (см. подраздел 4.1).

Поле «Последняя операция» содержит информацию о результатах выполнения последней операции с устройством с указанием даты, времени и длительности выполнения операции, а также ссылку для открытия окна с отчетом о выполнении операции.

Блок «Операции» на вкладке «Статус» содержит перечень основных операций, которые доступны для выполнения на выбранном устройстве (рис. 6). Перечень операций отличается в зависимости от типа устройства:

— «Загрузить все отчеты» – позволяет начать загрузку всех отчетов с устройства;
— «SSH-терминал» – ссылка для соединения с устройством по протоколу SSH;
— «Подключиться по HTTPS» – ссылка для соединения с устройством по протоколу HTTPS;
— «Выполнить команды» – позволяет задать команды напрямую;
— «Восстановить конфигурацию» – позволяет восстановить любую конфигурацию, существовавшую на устройстве;
— «Проверить соединение» – позволяет получить информацию о доступности устройства;

— «Скопировать running в startup» – позволяет скопировать рабочую конфигурацию в эталон;
— «Проверка подключения по SNMP» – позволяет выполнить проверку подключения к устройству по выбранному профилю SNMP;
— «Синхронизация устройств» – позволяет обновить список вложенных устройств по выбранному родительскому устройству.

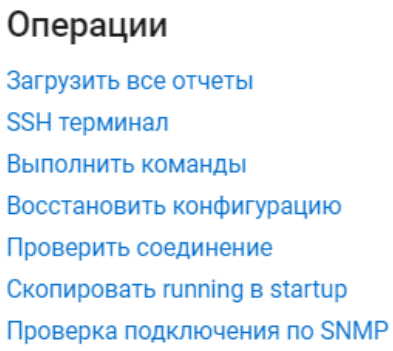


Рисунок 6 – Блок «Операции»

1.5 Описание подраздела «Профили отчетов»

Профили отчетов конфигурации и проверки безопасности устройств приведены в разделе «Контроль устройств», подраздел «Профили отчетов» (рис. 7).

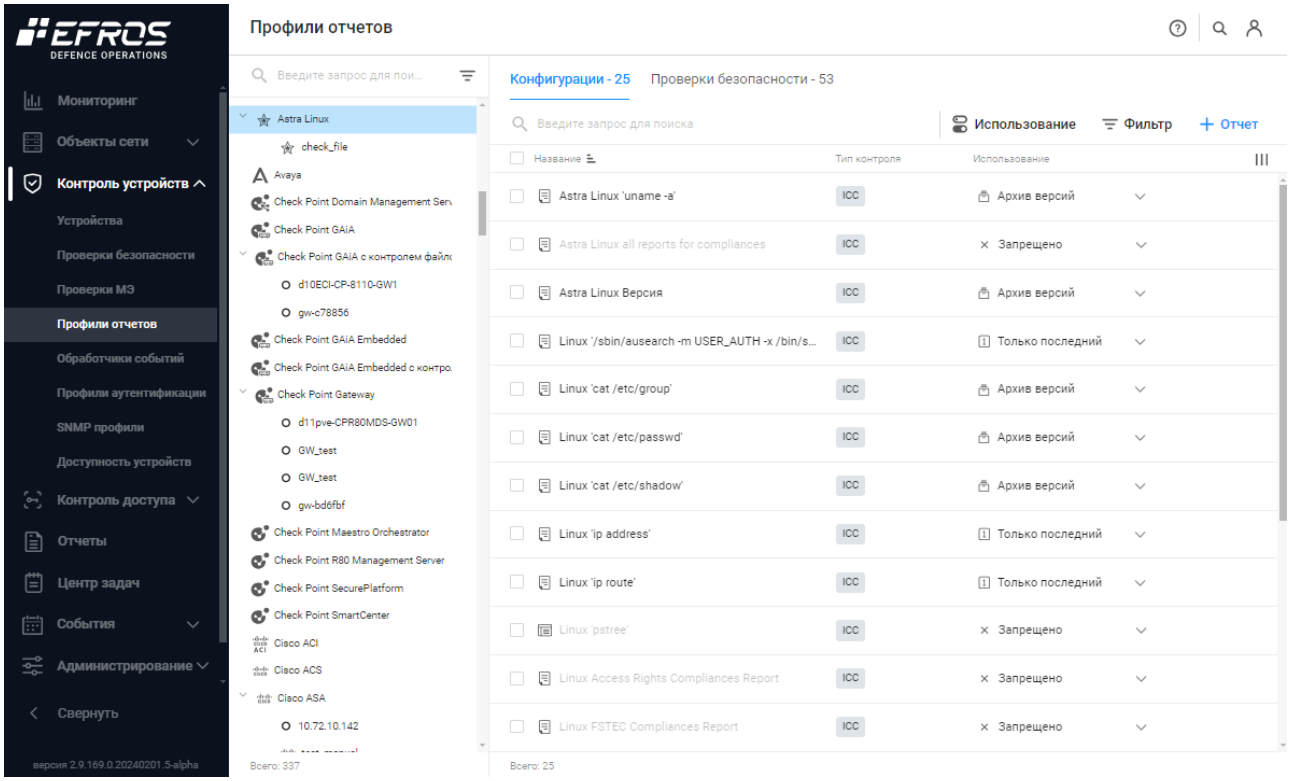


Рисунок 7 – Подраздел «Профили отчетов»

Список профилей отчетов конфигурации и проверок безопасности формируется динамически при подключении к комплексу внешних модулей для работы с контролируемыми устройствами (в разделе «Настройки»). Пользователи с соответствующими правами имеют возможность добавления пользовательских профилей отчетов на основе предустановленных, а также добавлять в профили отчетов новые пользовательские отчеты на основе существующих отчетов.

Профили отчетов предназначены для внесения изменений в части использования отчетов конфигурации и проверок безопасности.

Кнопка «Использование» (Использование) предназначена для перехода в окно просмотра и настройки использования профилей отчетов для устройств (рис. 8).

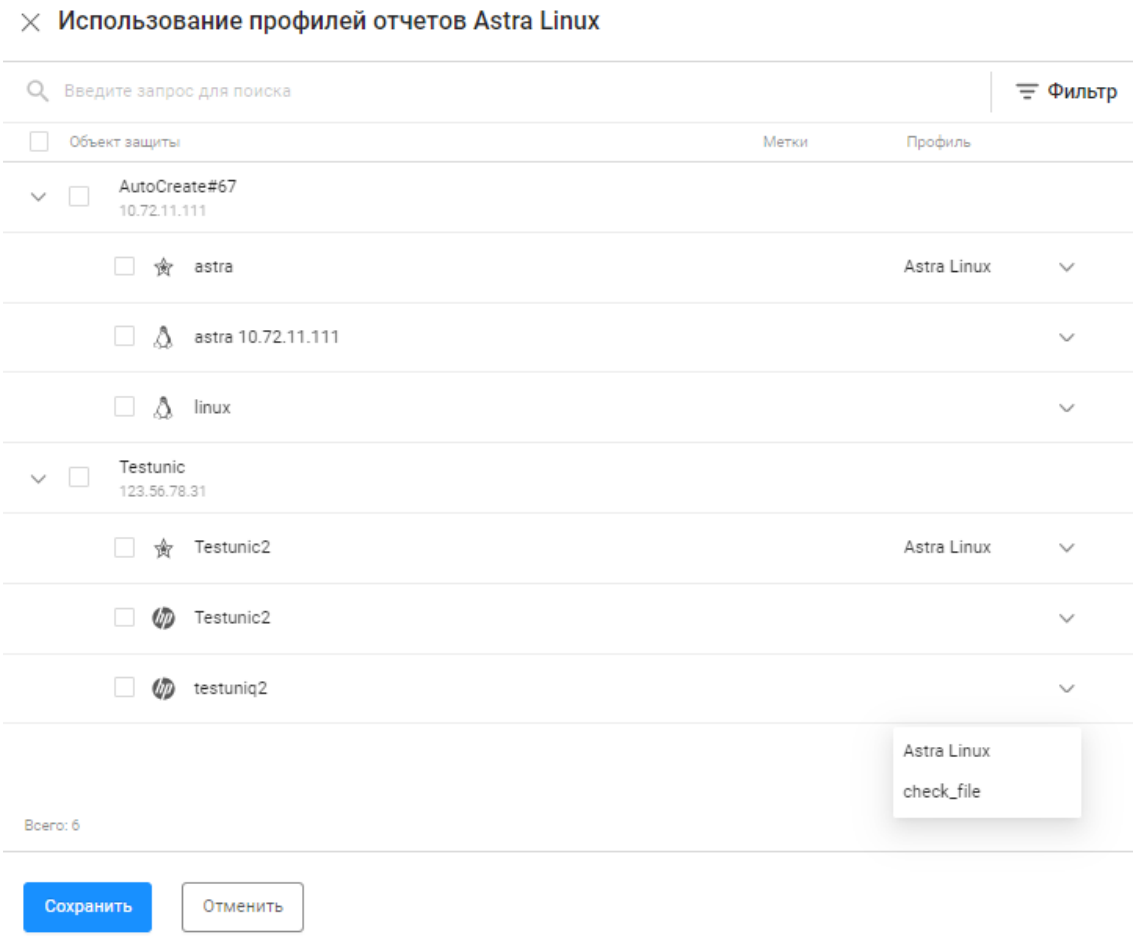


Рисунок 8 – Окно настройки использования профилей отчетов

1.5.1. Описание элементов дерева

Дерево со списком профилей отчетов сгруппировано по типам устройств.

Название типа устройства в дереве является предустановленным профилем отчетов. Вложенными являются пользовательские профили отчетов.

При наведении курсора на требуемый тип устройства появится кнопка «Создать профиль отчетов» ( ).

При наведении курсора на созданный пользовательский профиль отчета появится кнопка «Контекстное меню» ( ), которая позволяет выполнить следующие действия:

- «Изменить»;
- «Создать копию»;
- «Удалить».

Значком «○» в дереве автоматически отмечаются пользовательские профили отчетов в следующих случаях:

- изменены настройки отчетов устройства («Контроль устройств» → «Устройства» → вкладка «Отчеты») в сравнении с существующими пользовательскими профилями отчетов. Когда настройки станут одинаковыми, значок «○» исчезнет.
- пользовательский профиль отчета устройства создан автоматически, так как были изменены настройки устройства. При удалении профиля все параметры будут сброшены на значения «Наследовать».

Такой профиль доступен только для удаления, не доступен для настройки использования отчетов и добавления нового отчета.

1.5.2. Отчеты типа «Конфигурации»

На вкладке «Конфигурации» для отчетов применены следующие иконки:

- «» – текстовая форма отчета;
- «» – структурированная форма отчета;
- «» – пользовательский отчет;
- «» – отчет типа «Фильтр», созданный на основе другого отчета путем фильтрации данных;
- «» – отчет по правилам NAT;
- «» – отчет по правилам межсетевых экранов.

В столбце «Использование» можно изменить значение использования для каждого отчета, нажатием кнопки раскрывающегося списка ( ) (подробнее об использовании отчетов см. подраздел 2.2).

1.5.3. Отчеты типа «Проверки безопасности»

На вкладке «Проверки безопасности» для отчетов применены следующие иконки:

- «» – стандартная проверка;
- «» – проверка по МЭ;
- «» – проверка типа «Оптимизация правил»;
- «» – проверка на уязвимости.

На вкладке «Проверки безопасности» для отчетов в столбце «Использование» можно изменить значение использования для каждого отчета, нажатием кнопки раскрывающегося списка ( ) (рис. 9).

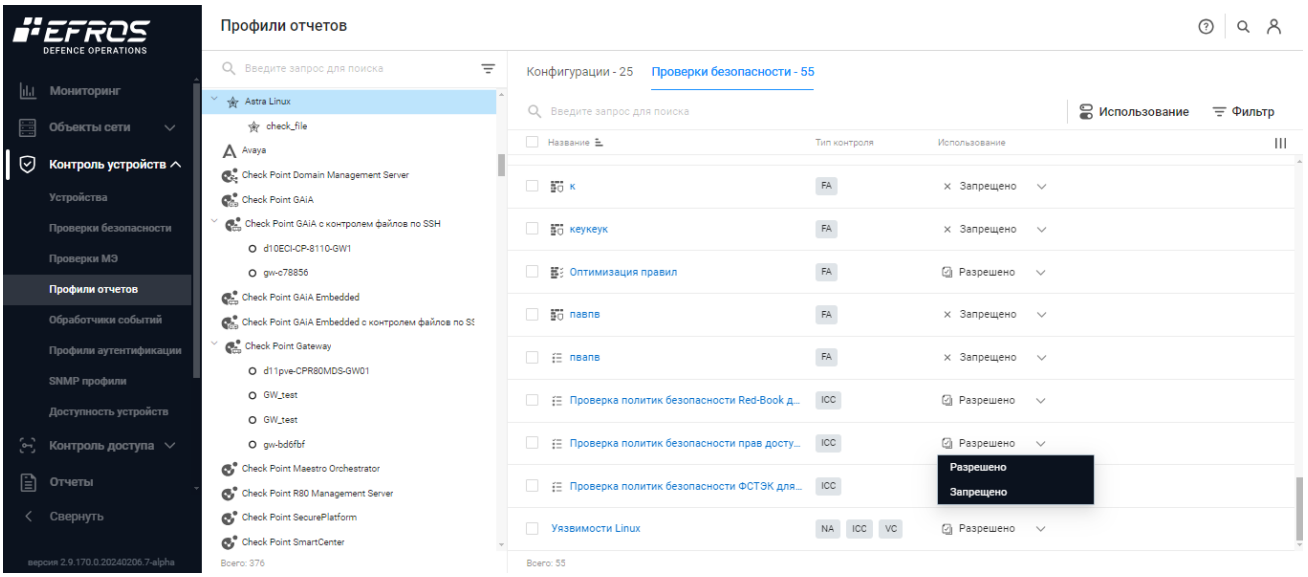


Рисунок 9 – Изменение использования отчетов

2 Возможности контроля изменений конфигураций

Ниже приведена рекомендуемая последовательность работы для реализации возможности контроля изменений конфигурации на примере ОС. Для виртуализации и ППО процесс аналогичный.

2.1 Просмотр отчета конфигурации устройства

Для просмотра отчета конфигурации устройства необходимо выполнить следующие действия:

1) Перейти в раздел «Контроль устройств», подраздел «Устройства», в дереве устройств выбрать требуемое устройство, затем перейти на вкладку «Отчеты».
2) В строке требуемого отчета нажать кнопку «Обновить» ( ) для запуска процесса опроса устройства, после чего отчет будет обновлен.

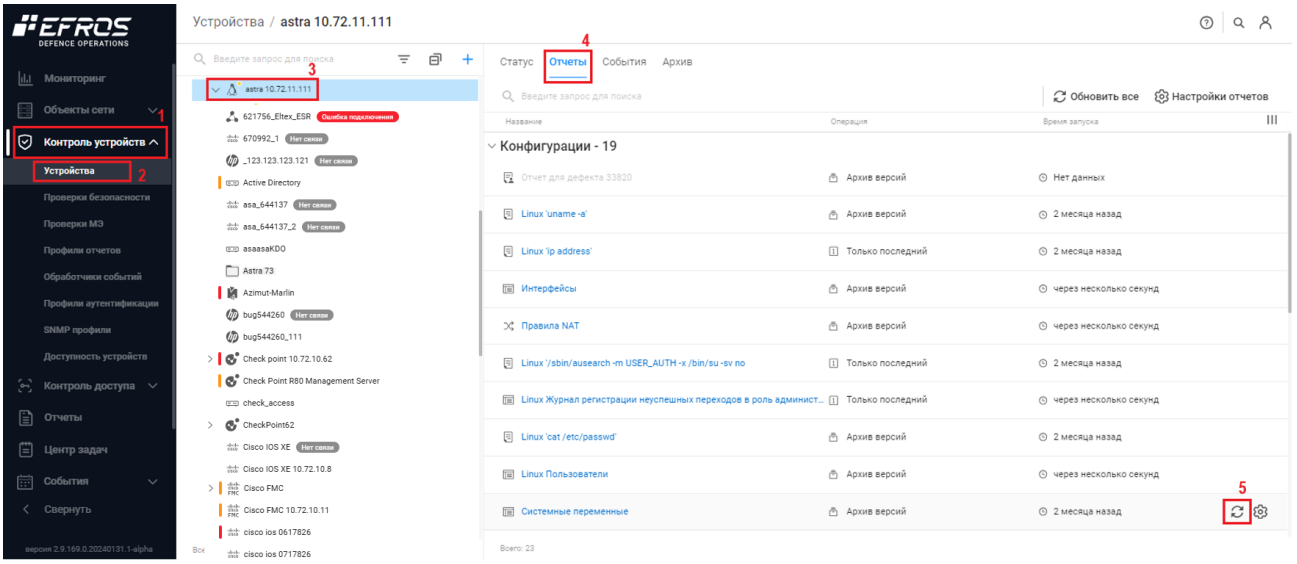


Рисунок 10 – Обновление отчета

3) В списке отчетов конфигурации нажать на название требуемого отчета. Откроется форма просмотра отчета. На рис. 11 – 12 приведены страницы с текстовой и структурированной формами отчетов.

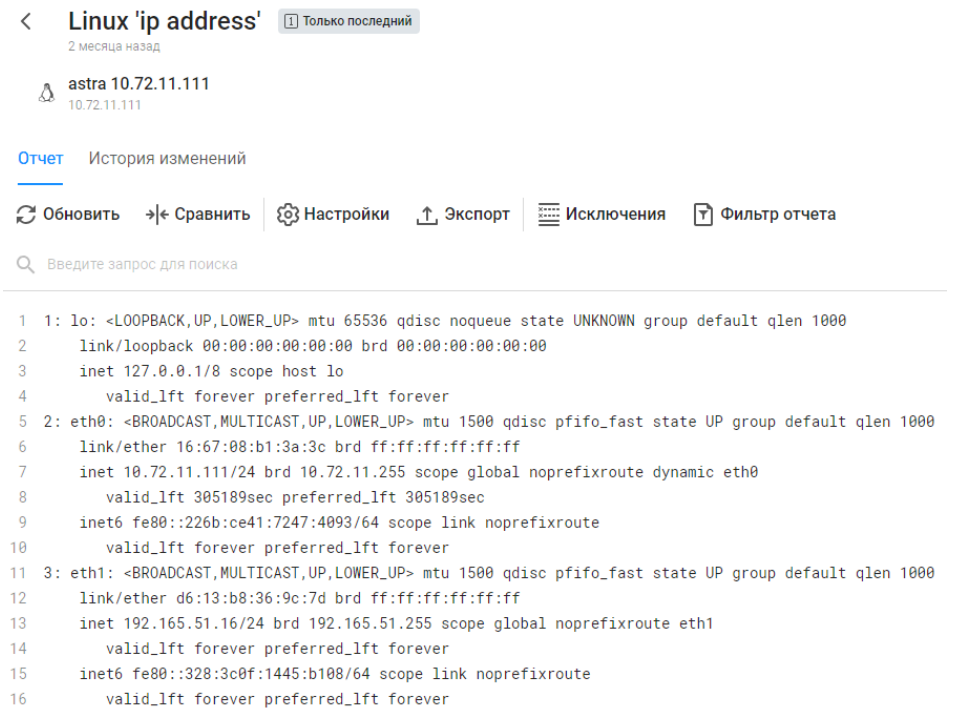


Рисунок 11 – Страница текстовой формы отчета

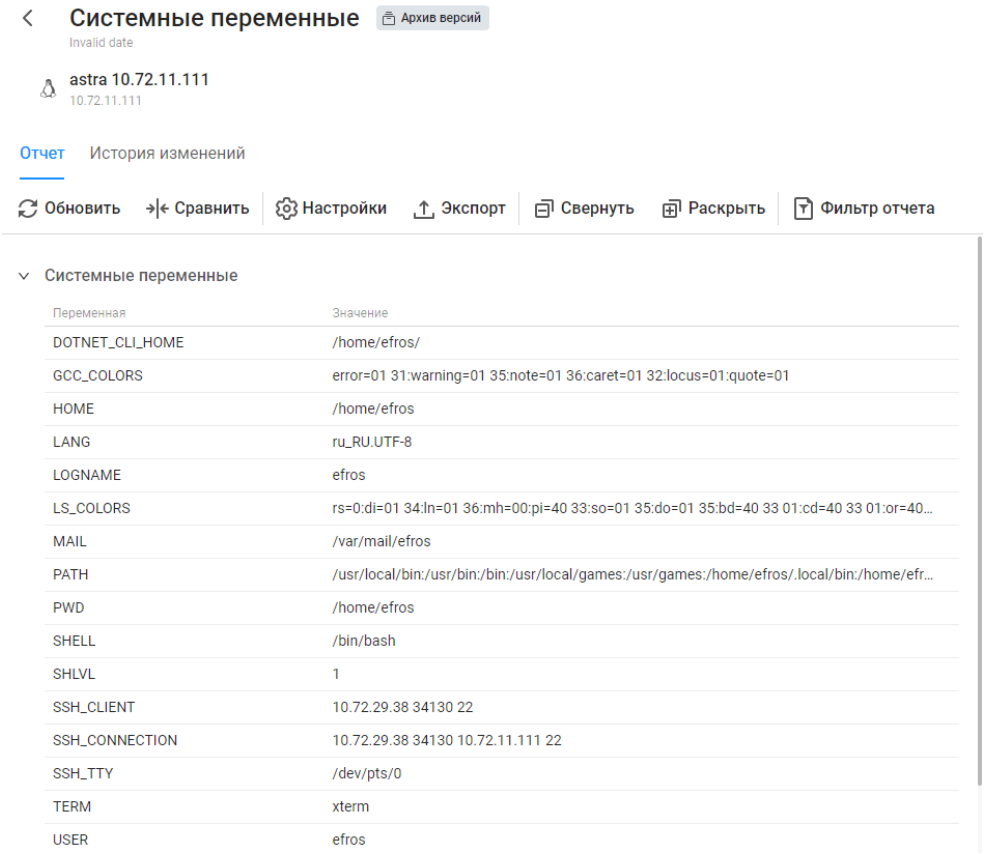


Рисунок 12 – Страница структурированной формы отчета

Описание основных функций формы просмотра различных отчетов:

- кнопка «Обновить» (Обновить) позволяет обновить версию отчета, запустив процесс опроса устройства;
- кнопка «Сравнить» (Сравнить) позволяет сравнить текущий отчет с ранее загруженными версиями отчетов;
- кнопка «Настройки» (Настройки) позволяет настроить использование отчета (см. подраздел 2.2);
- кнопка «Экспорт» (Экспорт) позволяет выгрузить отчет;
- кнопка «Исключения» (Исключения) позволяет указать строки, которые будут исключены из анализа контроля целостности. Правила применяются к отчету на всех объектах защиты;
- кнопка «Фильтр отчета» (Фильтр отчета) используется для настройки параметров поиска, фильтрации в отчетах по заданным параметрам. После доступна возможность создать новый отчет и (или) возможность выгрузить отчет на основе фильтрации.

4) Для просмотра изменений необходимо перейти на вкладку «История изменений» (рис. 13).

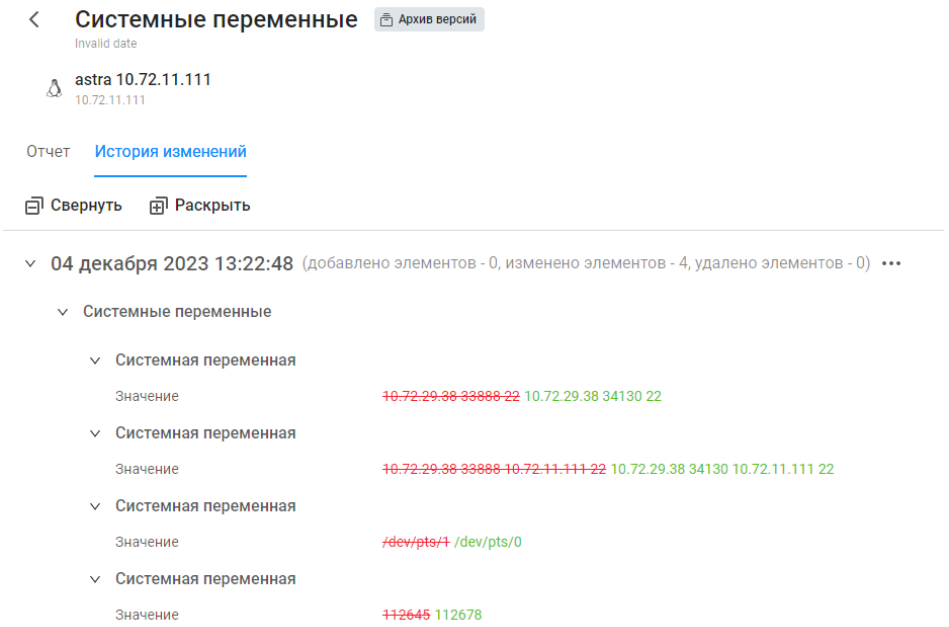


Рисунок 13 – Страница структурированной формы отчета, вкладка «История изменений»

Зеленым выделяются добавленные элементы. Красным выделяются удаленные элементы.

2.2 Настройка отчета конфигурации устройств

Для настройки одного отчета конфигурации для выбранного устройства пользователю необходимо выполнить следующие действия:

1) Перейти в раздел «Контроль устройств», подраздел «Устройства», в дереве устройств выбрать требуемое устройство, затем перейти на вкладку «Отчеты».

2) В строке требуемого отчета нажать кнопку «Настройки» (⚙) (рис. 14).

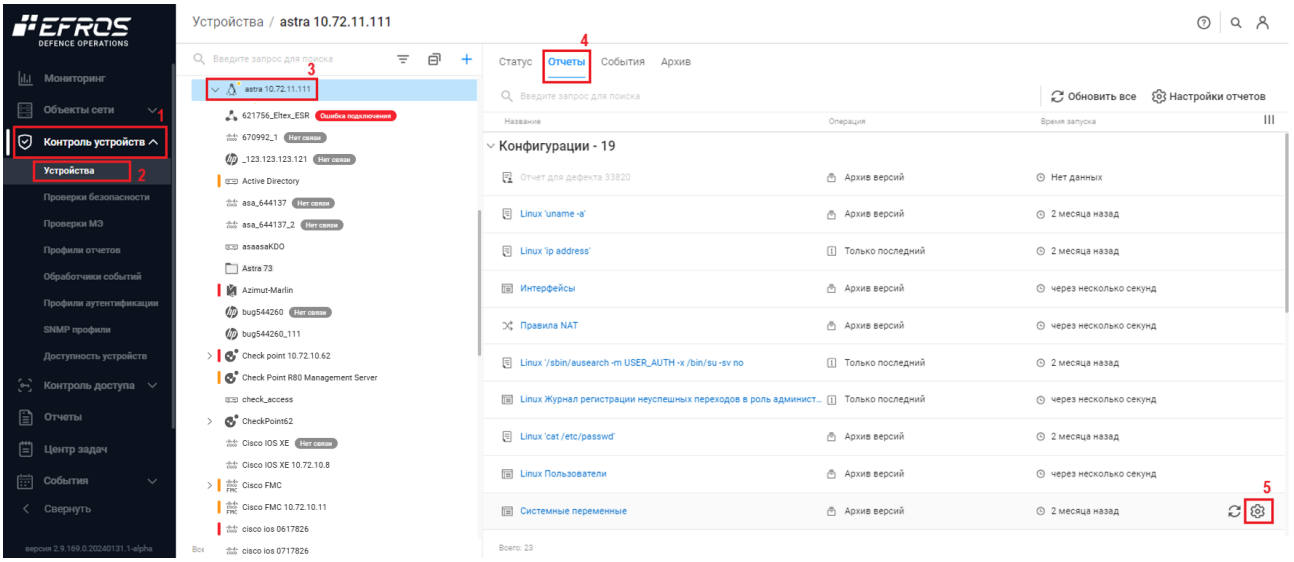


Рисунок 14 – Вкладка «Отчеты»

3) В открывшемся окне из раскрывающегося списка поля «Использование» выбрать необходимое значение (рис. 15).

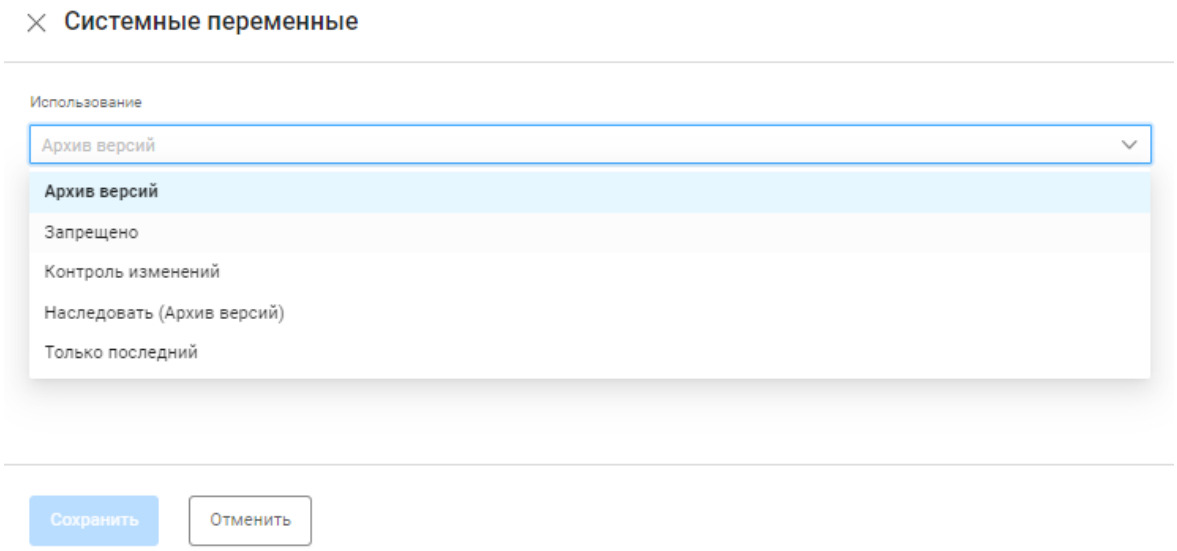


Рисунок 15 – Окно настройки отчета типа «Конфигурации»

В поле «Использование» доступны для выбора следующие режимы использования отчета типа «Конфигурации»:

- «Архив версий» – в базе данных (БД) комплекса будут храниться все измененные версии отчета, загруженные с устройства (см. подраздел 2.3);
- «Запрещено» – загрузка отчета с устройств запрещена вне зависимости от настроек профиля отчетов. Отчет будет скрыт из вкладки «Отчеты» в разделе «Устройства» (отчет останется доступен в разделе «Профили отчетов»);
- «Контроль изменений» – выполнение контроля целостности отчета, загруженного с устройства, вне зависимости от настроек профиля отчетов. Особенности применения данного типа использования:
  - первый загруженный с устройства отчет становится эталоном;
  - при загрузке последней версии отчета, отличной от эталона, на вкладках «Отчеты» и «Статус» устройства появится сообщение о нарушении целостности данного отчета, пользователю придет соответствующее оповещение (подробнее о настройке оповещений см. подраздел 4.2);
  - в БД комплекса будут храниться все измененные версии отчета в виде архива (см. подраздел 2.3);
- «Наследовать» – применить настройки профиля отчетов. В скобках отображается значение, установленное в профиле отчетов (см. подраздел 1.5);
- «Только последний» – в БД комплекса хранится только последняя измененная версия отчета, загруженного с устройства.

Для настройки всех отчетов для выбранного устройства пользователю необходимо выполнить следующие действия:

1) Выбрать в дереве устройств требуемое устройство. Перейти на вкладку «Отчеты» (см. рис. 14).
2) В заголовке вкладки «Отчеты» нажать кнопку «Настройки отчетов» (Настройки отчетов). Откроется окно настройки отчетов выбранного устройства (рис. 16).
3) Выбрать в поле «Профиль отчетов» из раскрывающегося списка требуемый профиль отчета.
4) На вкладке «Конфигурации» в раскрывающемся списке столбца «Использование» выбрать необходимое значение для каждого отчета.
5) Нажать кнопку «Сохранить». Окно настройки отчетов устройства закроется, внесенные изменения будут сохранены.

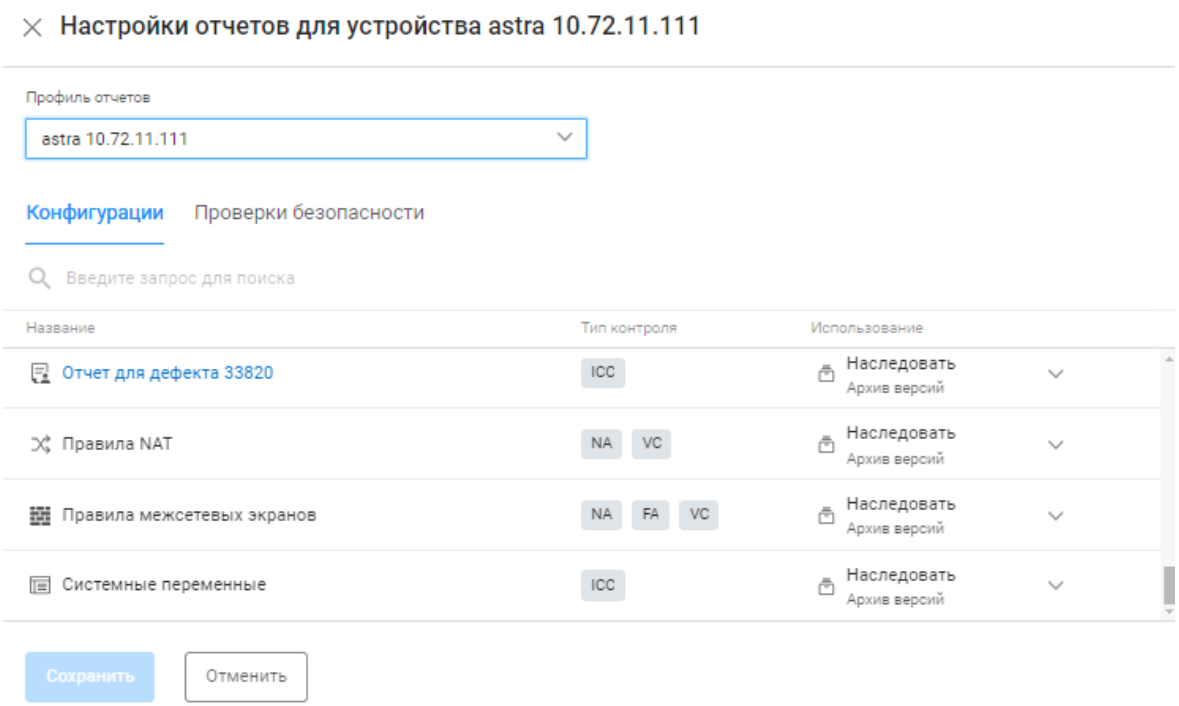


Рисунок 16 – Окно настройки отчетов выбранного устройства

2.3 Архив версий конфигураций устройств

Для просмотра архива версий конфигурации устройства необходимо перейти в раздел «Контроль устройств», подраздел «Устройства», в дереве устройств выбрать требуемое устройство. Перейти на вкладку «Архив» (рис. 17).

Вкладка «Архив» содержит список всех загруженных в БД комплекса версий отчетов устройства/группы устройств, для которых установлен режим использования «Архив версий» или «Контроль изменений».

Списки архивных отчетов группируются по датам проверки устройства. Нажатием на дату проверки можно свернуть текущий список.

При создании эталонного отчета, в столбце «Эталон» в строке отчета отображается пиктограмма «», дата и время создания, а также логин пользователя, создавшего эталон.

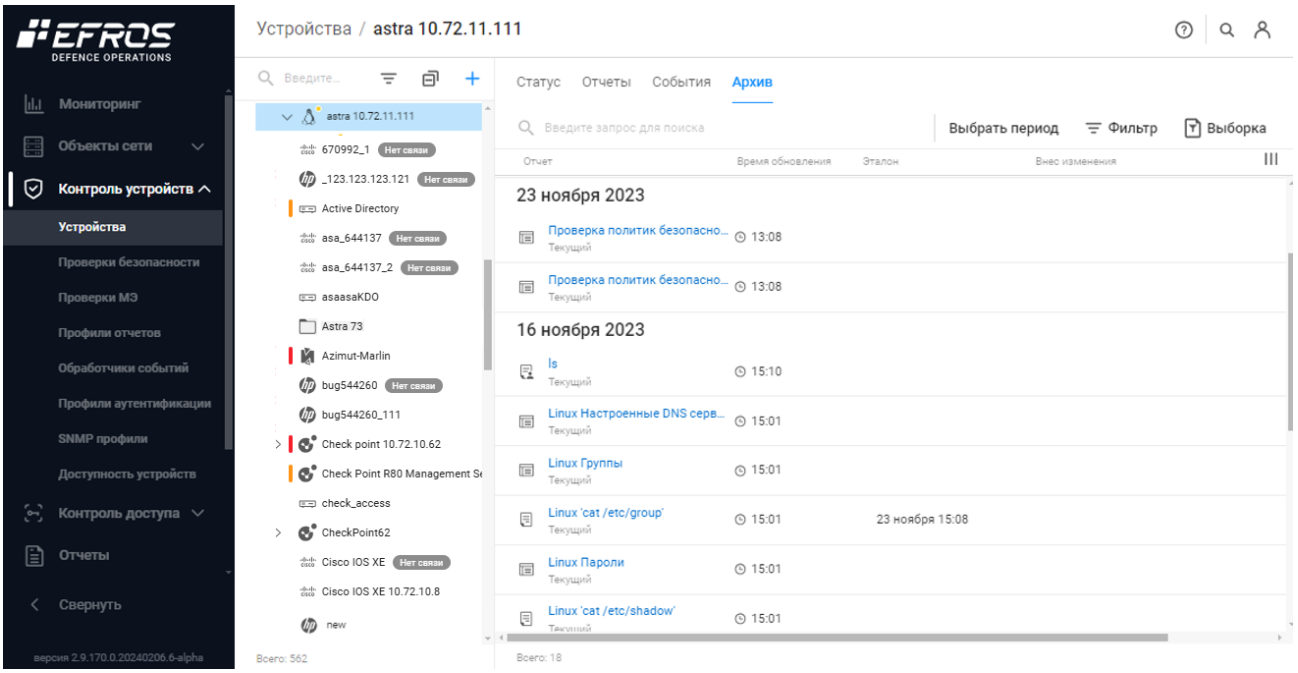


Рисунок 17 – Вкладка «Архив»

2.3.1. Создание и просмотра выборки данных архивных отчетов

Для создания выборки данных архивных отчетов необходимо выполнить следующие шаги:

1) Нажать на кнопку «Выборка» (**Выборка**) (см. рис. 17).
2) Откроется страница «Создание отчета (Выборка)», приведенная на рис. 18.

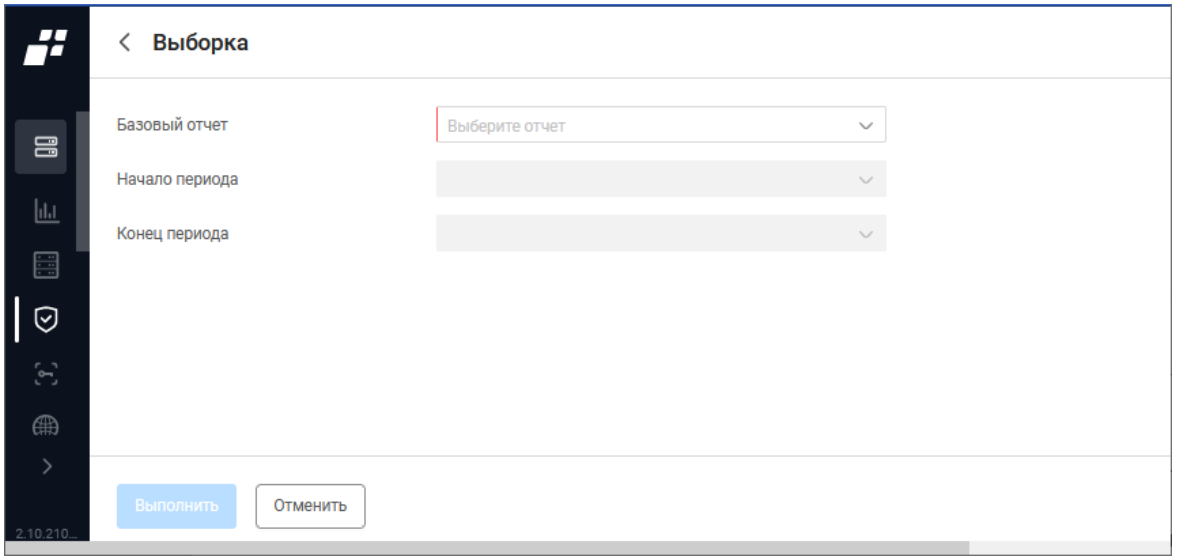
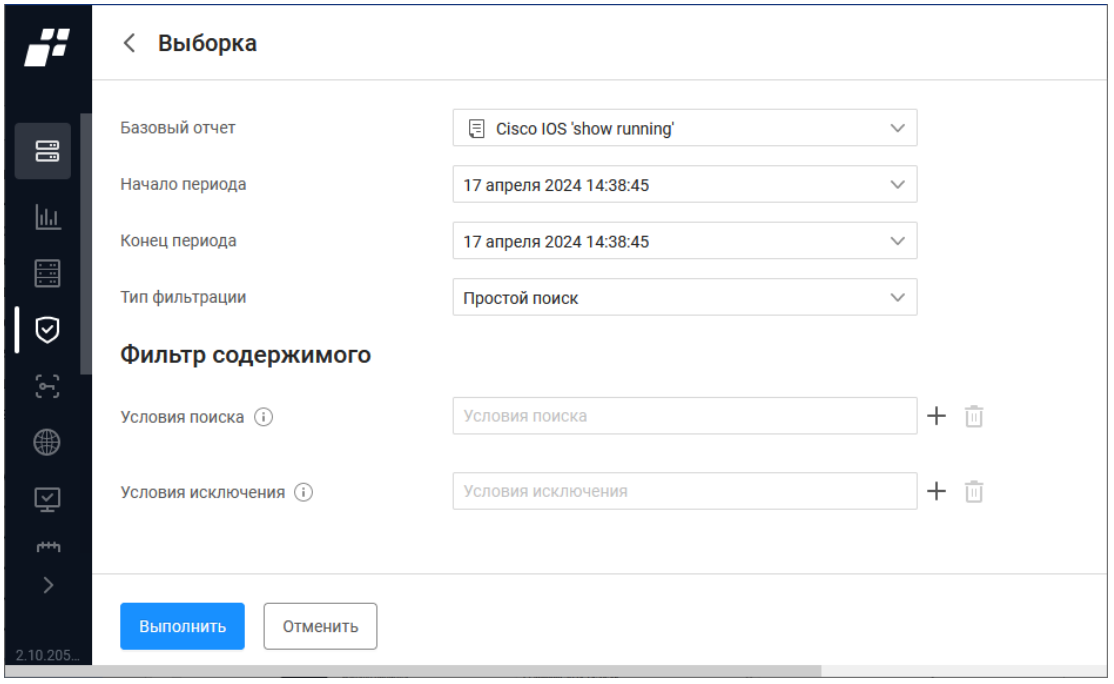
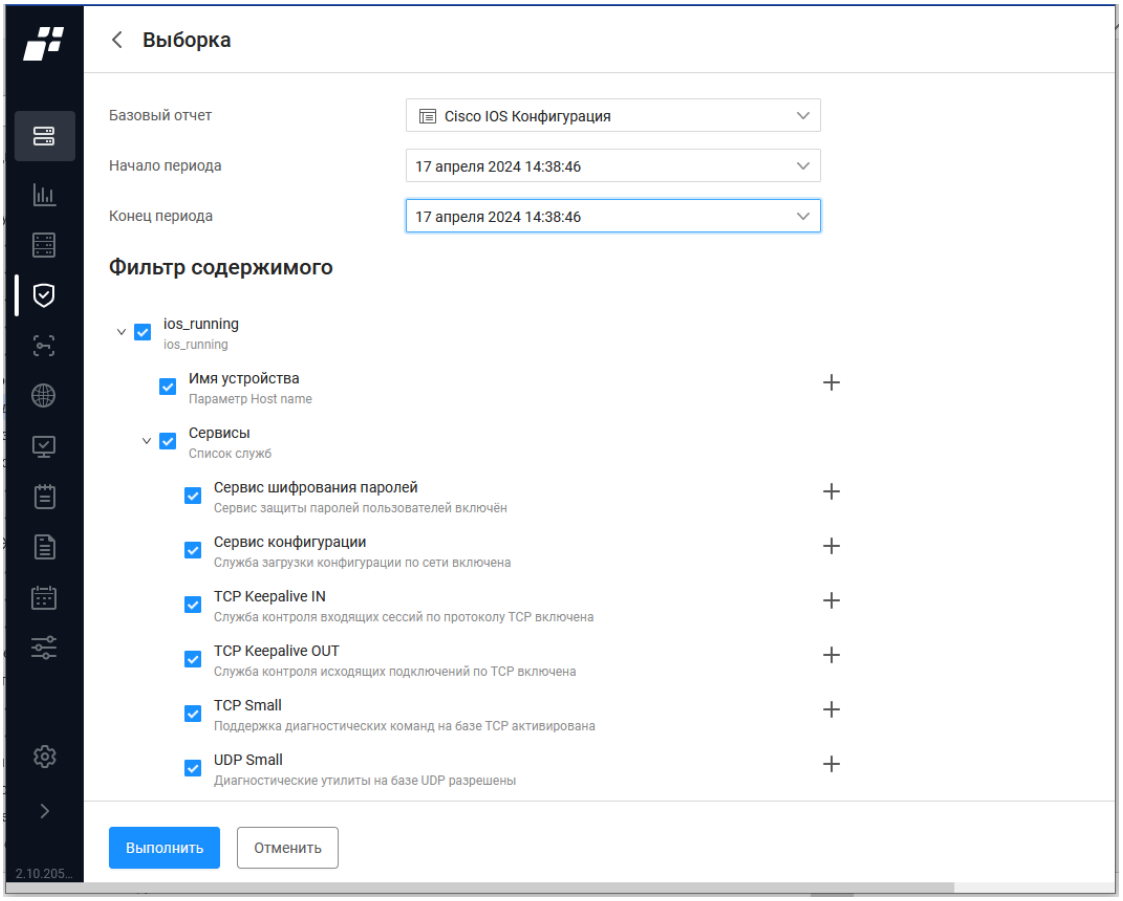


Рисунок 18 – Страница «Создание отчета (Выборка)»

3) Выбрать базовый отчет, на основании которого будет формироваться выборка. В окне дополнительно отобразятся поля ввода параметров выборки (рис. 19). Состав полей окна и правила их заполнения приведены в таблице 2.



а) для текстового отчета



б) для структурированного отчета

Рисунок 19 – Страница создания выборки с дополнительными полями

Таблица 2 – Состав и описание полей страницы создания выборки архивных отчетов

Поле	Описание
Поле «Базовый отчет»	Выбор варианта базового отчета, на основании которого будет формироваться отчет «Выборка»
Поля «Начало периода» и «Конец периода»	Поля становятся доступными только после выбора базового отчета. Предназначены для выбора дат и времени начала и окончания периода, за который должны быть отобраны архивные отчеты. Раскрывающиеся списки содержат все имеющиеся в таблице значения даты и времени сохранения в архиве версий выбранного типа отчета
Поле «Тип фильтрации»	Поле отображается только после выбора структурированного базового отчета. Предназначено для выбора типа фильтрации данных — «Простой поиск» – для выборки строк данных в тексте отчета в соответствии с введенными критериями отбора; — «Регулярные выражения (Поиск)» – для выполнения поиска введенных данных в тексте отчета; — «Регулярные выражения (Замена)» – для выполнения поиска введенных данных с заменой на другое значение
Блок полей «Фильтр содержимого»	
Для текстовых отчетов	В зависимости от выбранного ранее типа фильтрации содержит поля: 1. Для типа фильтрации «Простой поиск»: — «Условия поиска» – для ввода ключевого значения. Поиск будет выполняться по полному совпадению строки конфигурации введенному условию поиска.; — «Условия исключения» – для ввода значения исключения. При формировании отчета будут исключены строки, содержащие введенное значение. В полях поддерживается ввод символов «?» (один любой символ) и «*» (любые символы). Справа поля содержат кнопки «Добавить» (+) и «Удалить» () для добавления новых условий и удаления лишних. 2. Для типа фильтрации «Регулярные выражения (Поиск)»: — «Выражение поиска» – для ввода шаблона поиска данных; — «Только первое совпадение» – для поиска данных до обнаружения первого совпадения;

Поле	Описание
	— «Добавлять переводы строк между совпадениями» – для отображения каждого из найденных совпадений (при поиске всех совпадений) на новой строке отчета. 3. Для типа фильтрации «Регулярные выражения (Замена)»: — «Выражение поиска» – для ввода шаблона поиска данных; — «Выражение замены» – для ввода шаблона данных, которыми будут заменены искомые выражения; — ввести в поле Регулярное выражение шаблон для поиска искомых данных в загружаемом отчете, а в поле Выражение замены – данные, которыми будут заменены искомые выражения. При необходимости отметить требуемые параметры поиска: — «Только совпадения» – в форме просмотра отфильтрованного отчета в одну строку будут отображены только найденные и замененные выражения; — «Заменять только первое совпадение» – в форме просмотра отфильтрованного отчета будет изменено только первое из найденных выражений
Для структурированных отчетов	Содержит структурированный список параметров исходного отчета. В формируемый отчет попадут параметры, выбранные установкой флагов. Для выбранных параметров должны быть заданы правила отбора в полях, раскрывающихся при нажатии соответствующей параметру кнопки «+» : — для логических параметров – значение «Да» или «Нет» (выполняется или не выполняется); — для текстовых параметров – условия отбора. Может быть задано несколько условий типов «Равно», «Не равно», «Содержит» и «Не содержит» со значениями для отбора через логические условия «и»/«или». Справа поля параметров содержат кнопки «Добавить» (+) и «Удалить» (🗑) для добавления новых условий и удаления лишних
Элементы управления	
Выполнить	При нажатии кнопки открывается форма просмотра сформированного в соответствии с заданными параметрами отчета

Поле	Описание
Отменить	При нажатии кнопки окно закрывается без применения введенных данных

4) Заполнить поля страницы необходимыми параметрами и нажать кнопку «Выполнить». Откроется окно просмотра с данными загруженных версий выбранного типа отчета за указанный временной период с учетом установленных условий фильтра данных (рис. 20).

В отчете доступны:

- кнопка «Параметры» (Параметры) для перехода в окно редактирования заданных параметров отчета;
- кнопка «Экспорт» (Экспорт) для выгрузки данных отчета в файл формата .pdf;
- кнопки «Свернуть» (Свернуть) и «Раскрыть» (Раскрыть) для сворачивания\ раскрытия дерева;
- переключатель «Только нарушения» позволяет включить отображение только нарушений.

Описание регулярных выражений стандарта PCRE, допустимых к применению в ПК «Efros DO» при задании условий поиска для создания выборки, приведено в Приложении Б документа «Руководство пользователя. Часть 3. Контроль устройств».

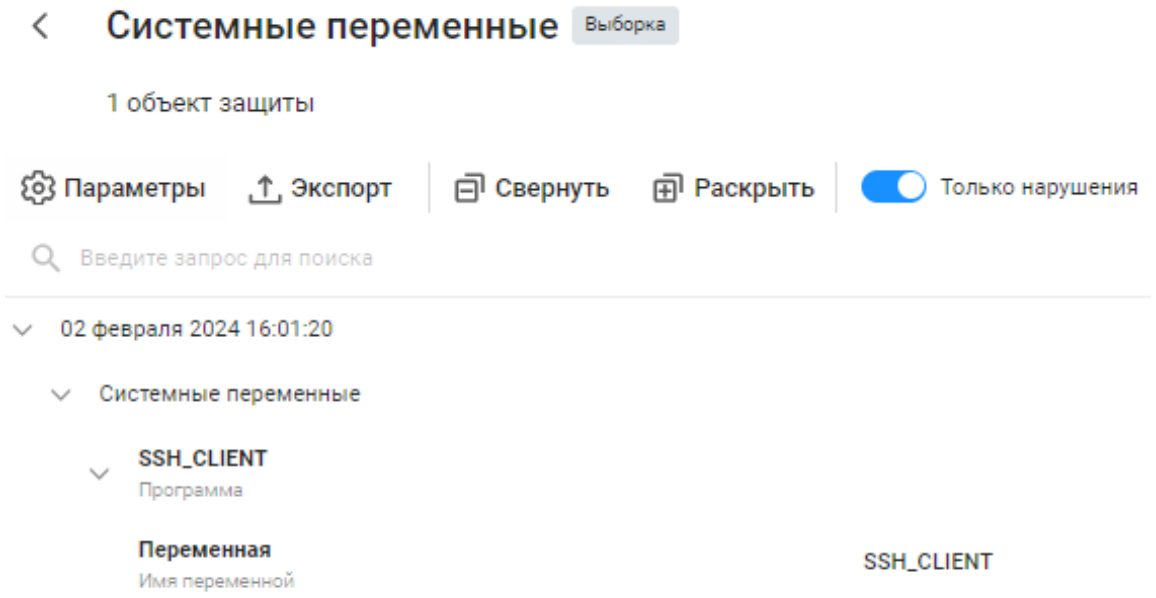


Рисунок 20 – Окно сформированной выборки архивных отчетов

2.4 Создание пользовательского профиля отчетов

Для создания пользовательского профиля отчетов необходимо выполнить следующие действия:

1) Перейти в раздел «Контроль устройств», подраздел «Профили отчетов», вкладка «Конфигурации».
2) В дереве со списком профилей отчетов навести курсор на требуемый тип устройства и нажать кнопку «Создать профиль отчетов» ( ) (рис. 21).

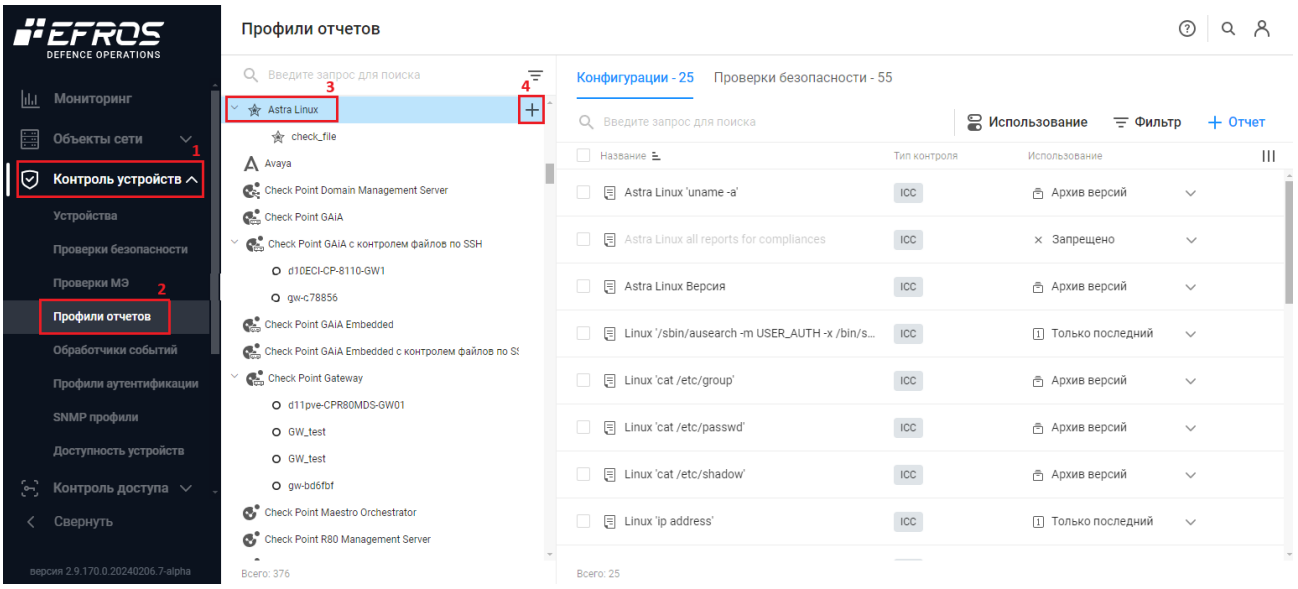


Рисунок 21 – Подраздел «Профили отчетов»

3) Откроется страница «Создание профиля отчетов» (рис. 22).

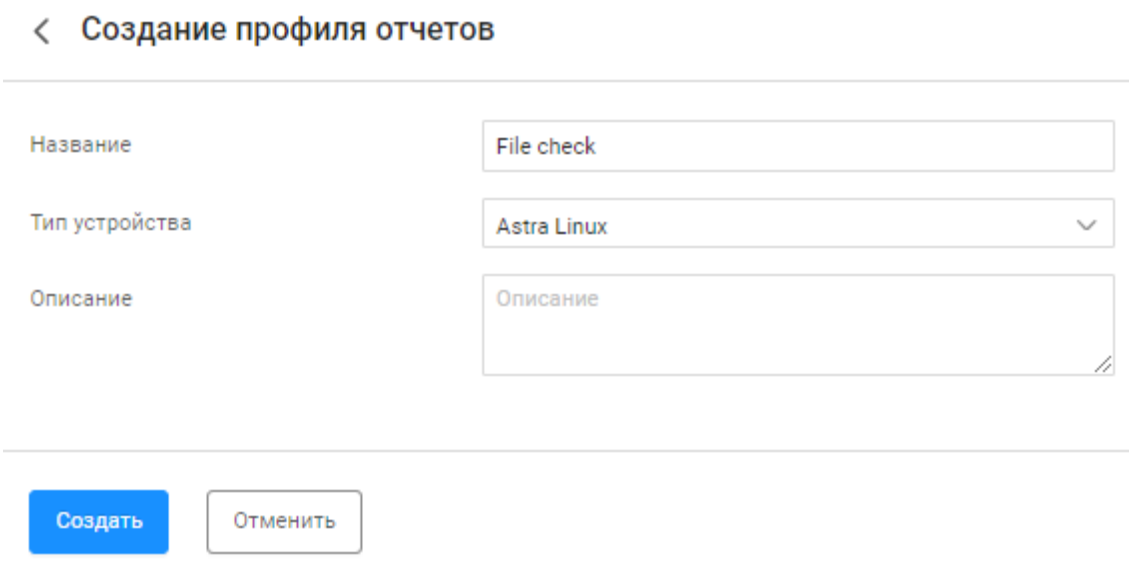


Рисунок 22 – Страница «Создание профиля отчетов»

4) Ввести название профиля отчетов. Поле «Тип устройства» будет заполнено автоматически.
5) Ввести при необходимости описание нового профиля отчетов и нажать кнопку «Создать». Откроется страница подраздела «Профили отчетов». В дереве профилей отчетов для выбранного в перечислении 1 профиля отчетов добавится вложенный профиль отчетов.

Созданный профиль содержит наследование настроек использования отчетов и проверок родительского профиля. При необходимости можно отредактировать использование отчетов и проверок в колонке «Использование» на вкладке «Конфигурации».

2.5 Создание пользовательского отчета конфигурации

Некоторые типы устройств не поддерживают возможность создания пользовательского отчета.

Для создания пользовательского отчета конфигурации необходимо выполнить следующие действия:

1) Перейти в раздел «Контроль устройств», подраздел «Профили отчетов», вкладка «Конфигурации».
2) В дереве со списком профилей отчетов выбрать требуемый профиль отчетов и нажать на вкладке «Конфигурации» (см. рис. 21) кнопку «Отчет» (+ Отчет).
3) В открывшемся окне «Создание отчета» состав значений поля «Тип отчета» зависит от типа устройства, соответствующего выбранному ранее профилю отчетов.

Для одного из типов ОС можно создать следующие типы отчетов:

— «Команда» – предназначена для выполнение команды на устройстве, на основе которого будет сформирован отчет (рис. 23);
— «Файлы» – предназначен для контроля файлов конфигурации устройств (см. подраздел 2.5);
— «Права доступа к файлам» (рис. 24).

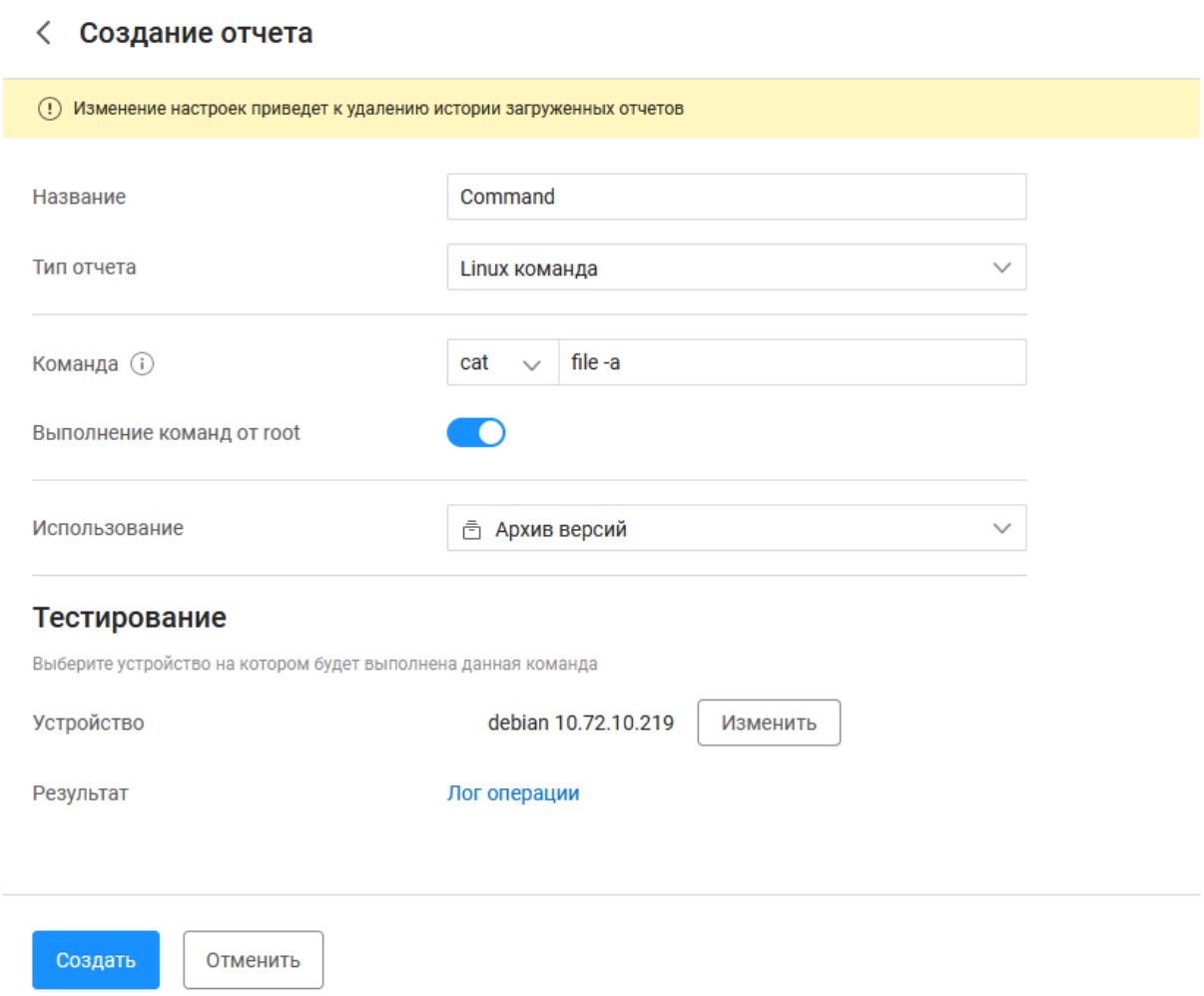


Рисунок 23 – Создание типа отчета «Команда»

Пример заполнения полей типа отчета «Команда» описаны ниже:

- поле «Название» – любое;
- поле «Тип отчета» – «<название типа устройства> команда»;
- блок полей «Команда»:
  - поле префикса – название команды;
  - текстовое поле команды – параметры команды;
- переключатель «Выполнение команд от root» – переключатель включен (необходимо использовать для выполнения команд sudo/pfexec);
- поле «Использование» – «Архив версий»/ «Контроль изменений»/ «Только последний»/ «Запрещено»/ «Наследовать (XXXXXX)»;
- блок полей «Тестирование»:
  - поле «Устройство» – для выбора устройства тестирования;
  - поле «Результат» – для просмотра лога операции.

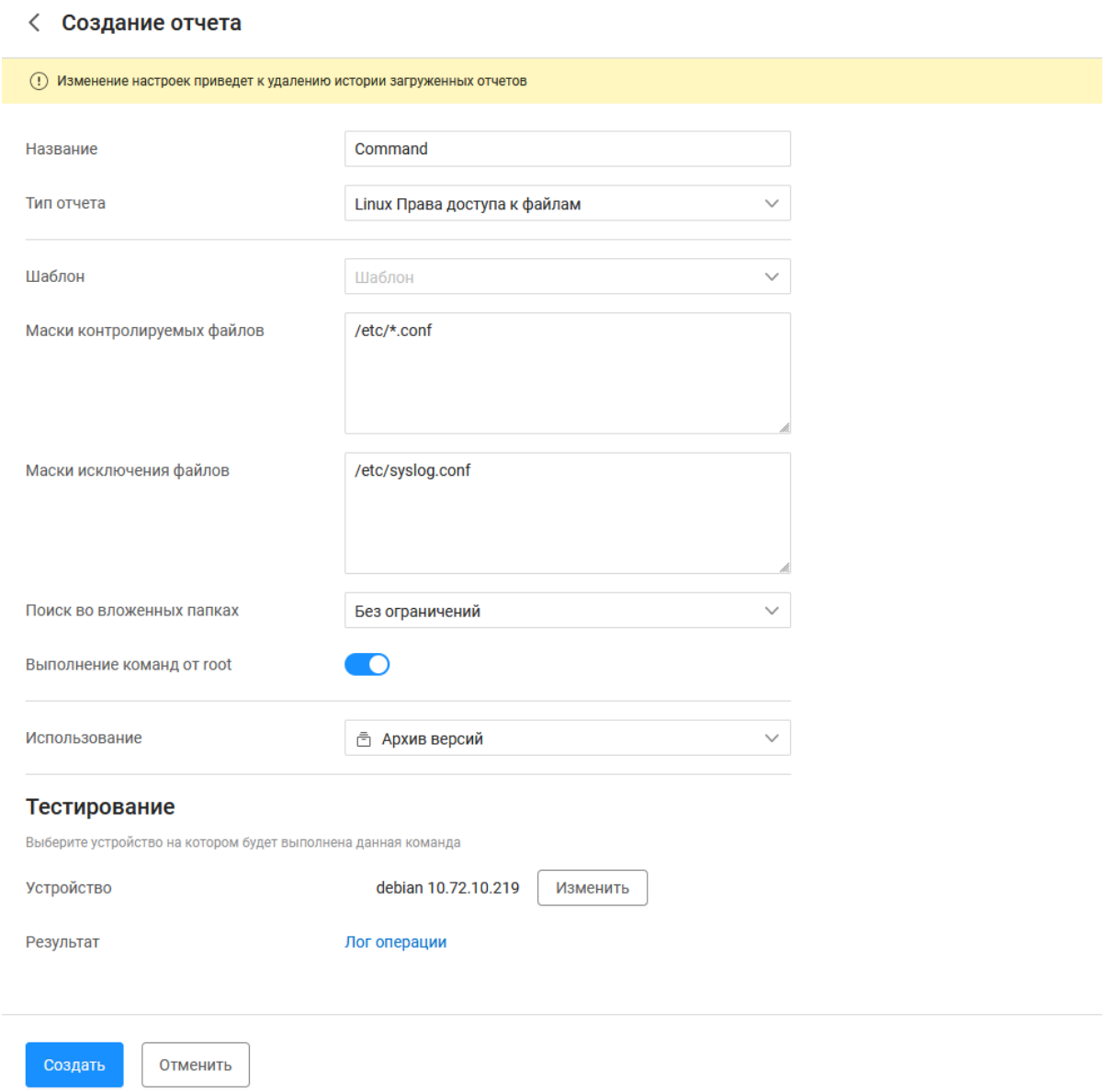


Рисунок 24 – Создание типа отчета «Права доступа к файлам»

Пример заполнения полей типа отчета «Права доступа к файлам» описаны ниже:

- поле «Название» – любое;
- поле «Тип отчета» – «<название устройства> Права доступа к файлам»;
- поле «Шаблон» – название одного из предустановленных списков файлов, которые необходимо контролировать;
- поле «Маски контролируемых файлов» – маски контролируемых файлов, заполняется автоматически, допускается вносить корректировки;
- поле «Маски исключения файлов» – маски исключаемых из контроля файлов, заполняется автоматически, допускается вносить корректировки;
- поле «Поиск во вложенных папках» – уровень вложенности в указанных папках для контроля (Уровень 1/ Уровень 2/ Без ограничений/ Выключен);

— переключатель «Выполнение команд от root» – переключатель включен (необходимо использовать для выполнения команд sudo/pfexec);
— поле «Использование» – «Архив версий»/ «Контроль изменений»/ «Только последний»/ «Запрещено»/ «Наследовать (XXXXXX)»;
— блок полей «Тестирование»:
  - поле «Устройство» – для выбора устройства тестирования;
  - поле «Результат» – для просмотра лога операции.

Описание запуска процесса опроса устройства по данным отчетам и описание просмотра созданных отчетов приведено в подразделе 2.1.

2.6 Создание пользовательского отчета конфигурации типа «Фильтр»

Отчет «Фильтр» создается на основе просматриваемого средствами подраздела «Устройства» отчета конфигурации путем фильтрации параметров исходного отчета.
Для создания отчета «Фильтр» необходимо выполнить следующие шаги:

1) Перейти в раздел «Контроль устройств», подраздел «Устройства».
2) В дереве со списком устройств выбрать требуемое устройство и выбрать в списке отчетов «Конфигурации» (см. рис. 2) название исходного отчета.
3) Нажать во вкладке «Отчет» страницы просматриваемого отчета (рис. 25) кнопку «Фильтр отчета» (Фильтр отчета).

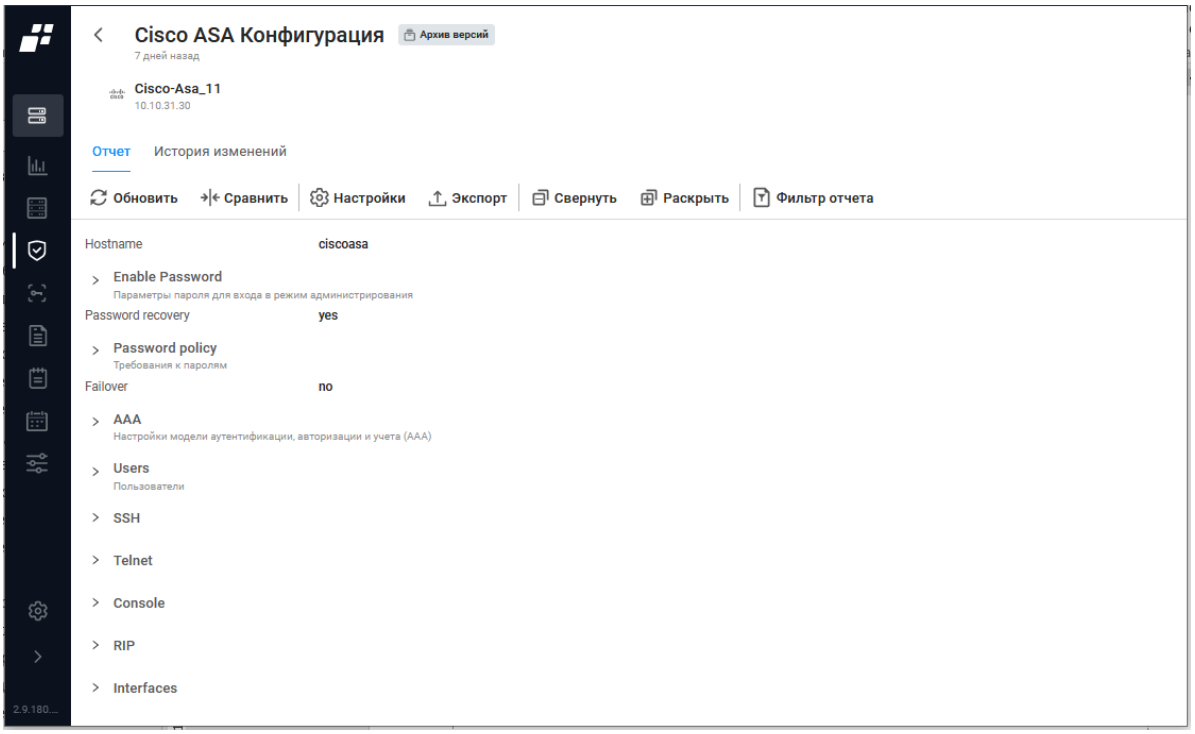
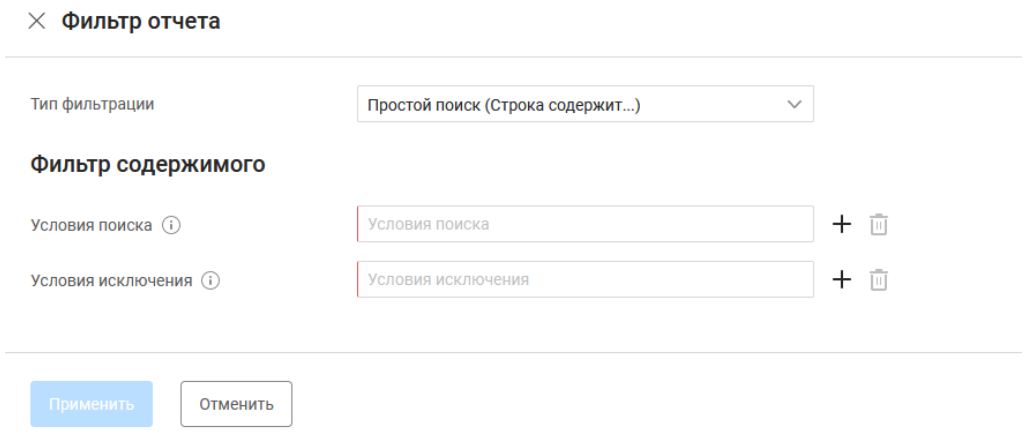
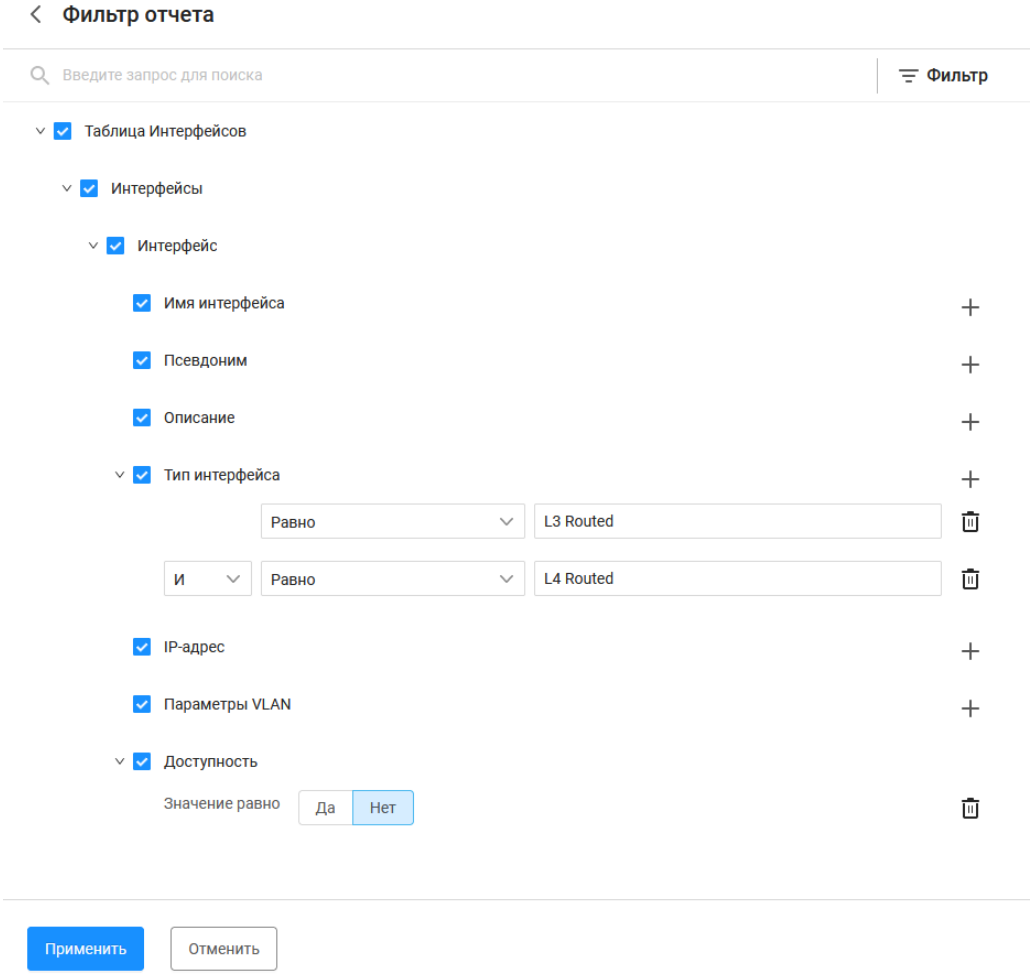


Рисунок 25 – Окно просмотра отчета конфигурации

4) Откроется окно задания фильтров для создания отчета, приведенное на рис. 26. Правила заполнения полей окна аналогичны правилам, приведенным в таблице 2, для страницы создания выборки архивных отчетов (см. пункт 2.3.1).



а) для текстового отчета



б) для структурированного отчета

Рисунок 26 – Окно задания фильтров для отчета «Фильтр»

5) Заполнить поля окна необходимыми параметрами и нажать кнопку «Применить». Откроется страница со сформированным отчетом рис. 27.

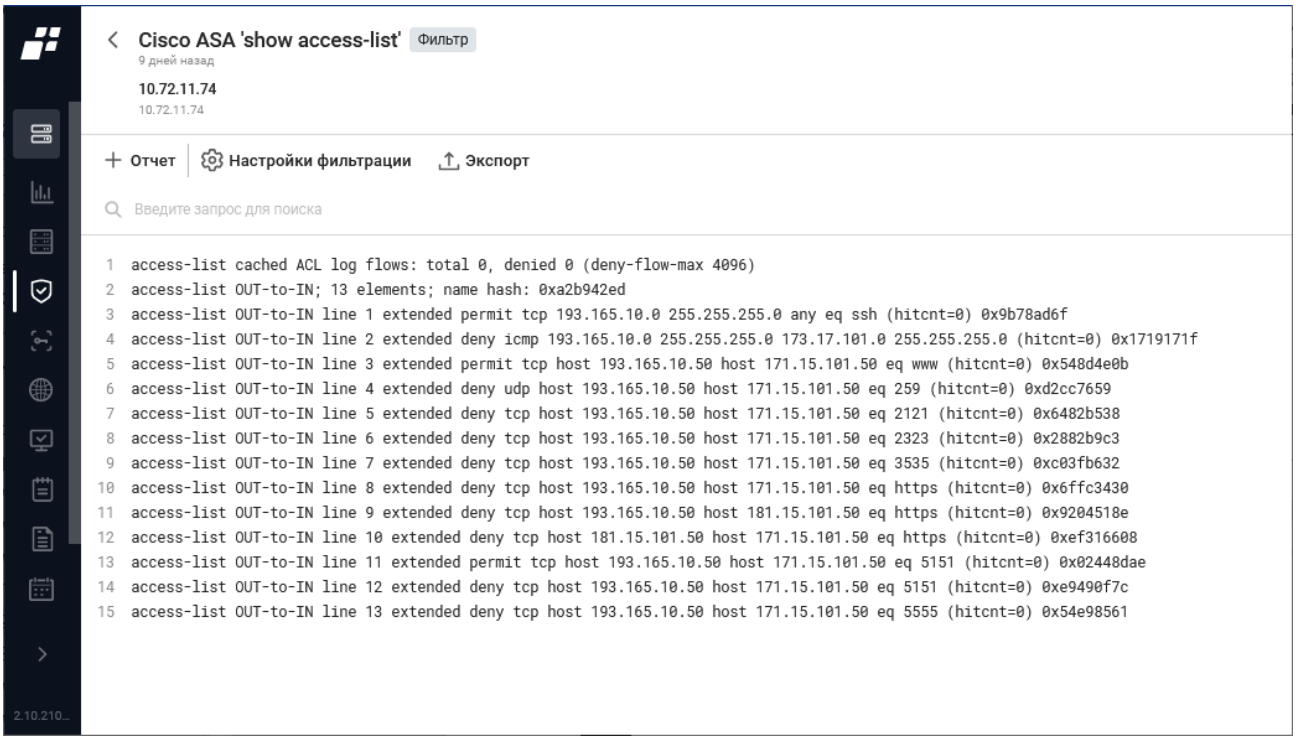


Рисунок 27 – Страница просмотра отчета «Фильтр»

6) Просмотреть отчет. При необходимости скорректировать настройки фильтрации отчета в окне, которое открывается по нажатию кнопки «Настройки фильтрации» (**Настройки фильтрации**).
7) Выгрузить при необходимости отчет на рабочую машину по нажатию кнопки «Экспорт» (**Экспорт**).
8) Создать новый отчет для устройства на основе сформированного отчета «Фильтр», для чего:

— нажать кнопку «Отчет» (**Отчет**);
— в открывшемся окне (рис. 28) ввести имя нового отчета, задать настройки использования отчета:
  - на текущем устройстве или на всех устройствах соответствующего типа;
  - вариант использования (см. подраздел 2.2);
— изменить при необходимости условия фильтрации;
— нажать кнопку «Сохранить».

Созданный отчет добавится в списке отчетов устройства (на вкладке «Отчеты»), а также в списке отчетов профиля отчетов, назначенного в текущий момент для устройства.

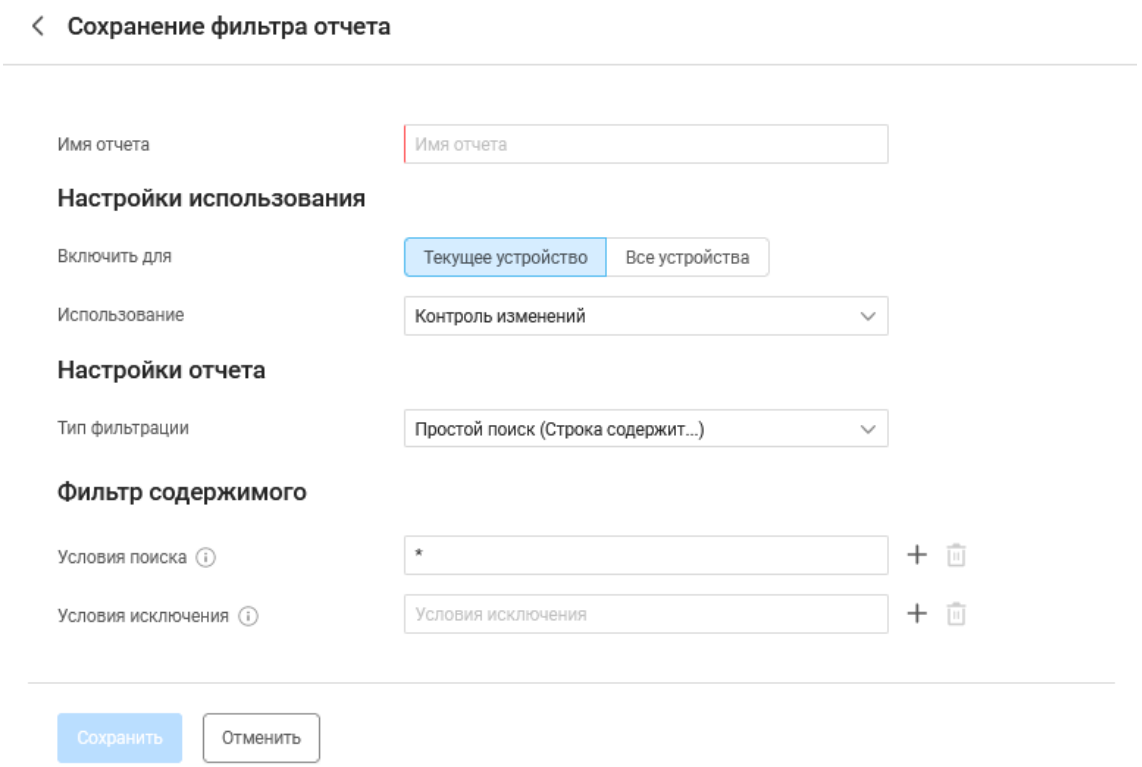


Рисунок 28 – Окно «Сохранение фильтра отчета»

2.7 Создание пользовательского типа отчета проверки целостности файлов устройства

Возможность контроля целостности файлов является составной частью возможности контроля изменений конфигурации.

Некоторые типы устройств не поддерживают возможность создания пользовательского отчета.

Для создания пользовательского отчета проверки целостности файлов устройства необходимо выполнить следующие действия:

1) Перейти в раздел «Контроль устройств», подраздел «Профили отчетов».
2) В дереве со списком профилей отчетов устройств выбрать необходимый профиль отчетов либо создать новый в соответствии с подразделом 2.4.
3) На вкладке «Конфигурации» (см. рис. 21) нажать кнопку «Отчет» (+ Отчет).
4) В открывшемся окне «Создание отчета» состав значений поля «Тип отчета» зависит от типа устройства, соответствующего выбранному ранее профилю отчетов.
5) Для одного из типов ОС для создания отчета проверки целостности файла (проверки контрольной суммы файла) – выбрать тип отчета «<наименование ОС>Файлы» (рис. 29).

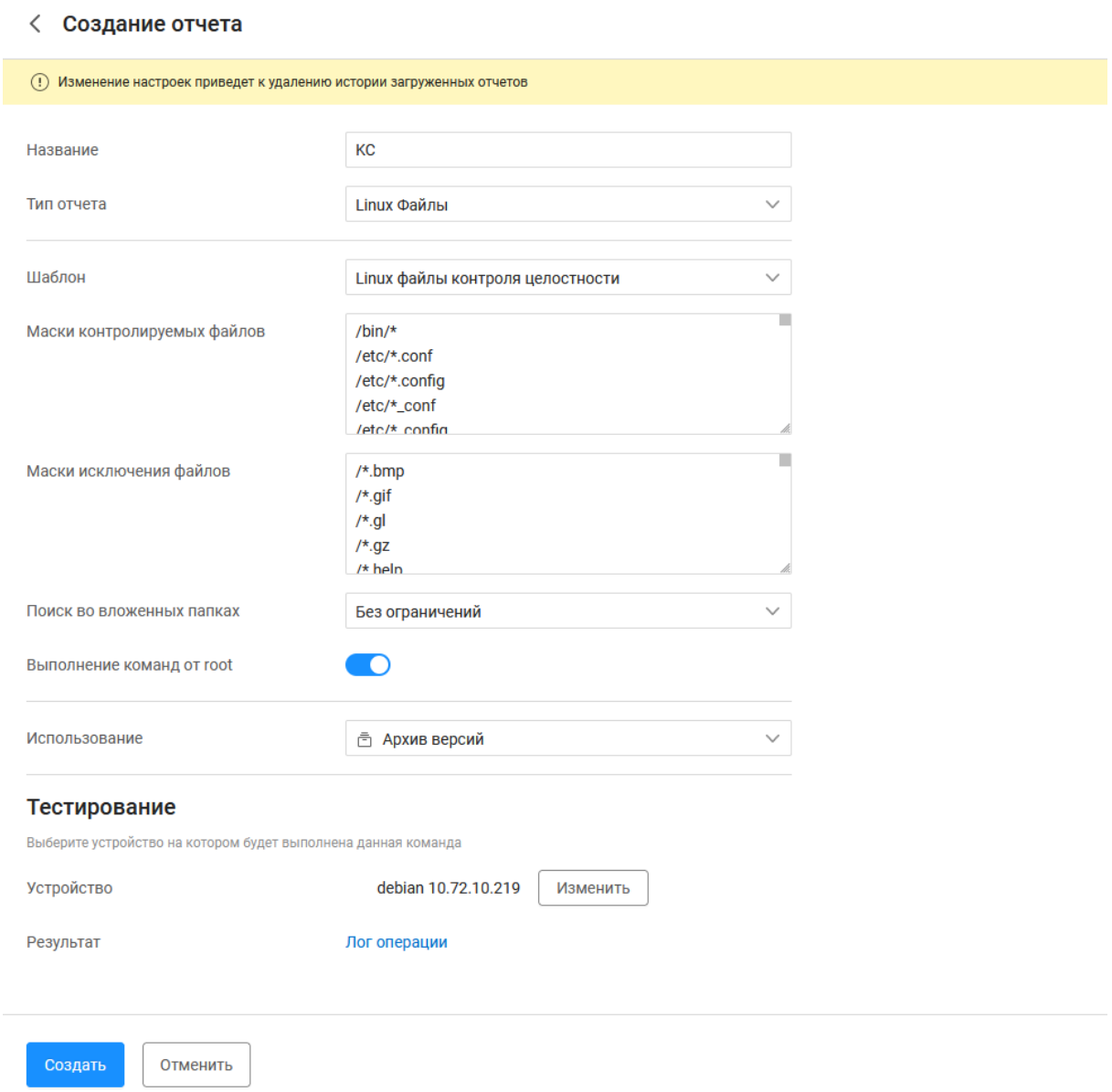


Рисунок 29 – Создание типа отчета «Файлы»

Пример заполнения полей типа отчета «Файлы» для контроля целостности файлов ОС описаны ниже:

- поле «Название» – любое;
- поле «Тип отчета» – «<название типа устройства> файлы»;
- поле «Шаблон» – «<название типа устройства> файлы контроля целостности»;
- поле «Маски контролируемых файлов» – маски контролируемых файлов, заполняется автоматически, допускается вносить корректировки;
- поле «Маски исключения файлов» – маски исключаемых из контроля файлов, заполняется автоматически, допускается вносить корректировки;
- поле «Поиск во вложенных папках» – уровень вложенности в указанных папках для контроля (Уровень 1/ Уровень 2/ Без ограничений/ Выключен);

— переключатель «Выполнение команд от root» – переключатель включен (необходимо использовать для выполнения команд sudo/pfexec);
— поле «Использование» – «Архив версий»/ «Контроль изменений»/ «Только последний»/ «Запрещено»/ «Наследовать (XXXXXX)»;
— блок полей «Тестирование»:
  - поле «Устройство» – для выбора устройства тестирования;
  - поле «Результат» – для просмотра лога операции.

Описание запуска процесса опроса устройства по данным отчетам и описание просмотра созданных отчетов приведено в подразделе 2.1.

3 Возможности контроля соответствия безопасности

Ниже приведена рекомендуемая последовательность работы для реализации возможности контроля соответствия безопасности на примере ОС. Для виртуализации и ППО процесс аналогичный.

3.1 Просмотр отчетов проверок устройства

Для просмотра отчета проверок устройства необходимо выполнить следующие действия:

1) Перейти в раздел «Контроль устройств», подраздел «Устройства», в дереве устройств выбрать требуемое устройство, затем перейти на вкладку «Отчеты», список «Проверки».
2) В строке требуемой проверки нажать кнопку «Обновить» ( ) для запуска процесса загрузки отчета с устройства, после чего отчет будет обновлен (рис. 30).

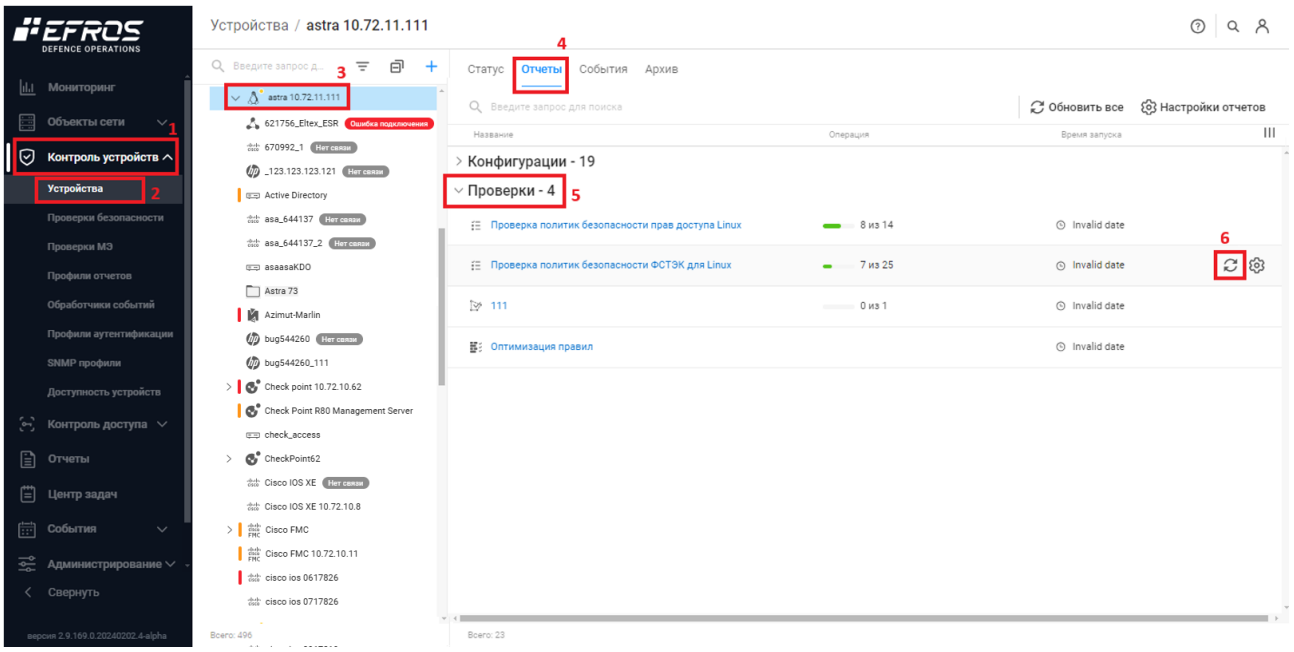


Рисунок 30 – Список отчетов типа «Проверки»

3) В списке отчетов проверок нажать на название требуемого отчета. Откроется форма просмотра отчета с активной вкладкой «Отчет» (рис. 31).

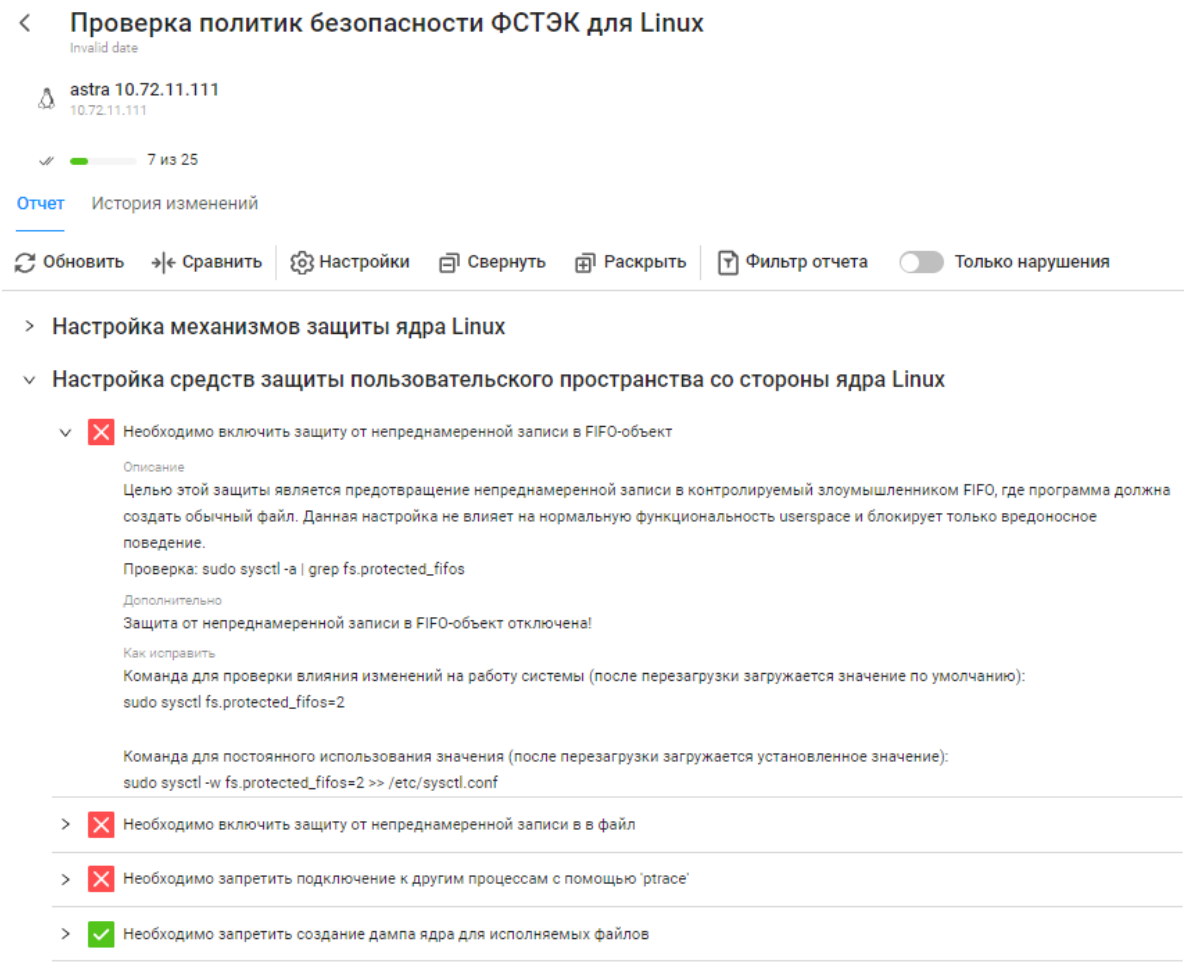


Рисунок 31 – Страница отчета проверки

В отчете «Проверка политик безопасности» приведены сгруппированные списки требований политики безопасности:

- знак крестика ( ) обозначает, что требование не выполнено;
- знак галочки ( ) обозначает, что требование выполняется.

Для требования политики безопасности, при разворачивании списка, приведены следующие данные:

- описание;
- дополнительная информация;
- варианты исправления для выполнения требования.

В верхней части страницы приведено количество выполняемых требований политики безопасности.

Для исправления невыполненных требований можно применить предложенные варианты исправления на устройстве.

Список требований политик безопасности задается в подразделе «Проверки безопасности» (см. подраздел 3.3).

Описание основных функций формы просмотра отчета приведены в подразделе 2.1.

4) Для просмотра изменений необходимо перейти на вкладку «История изменений» (рис. 32).

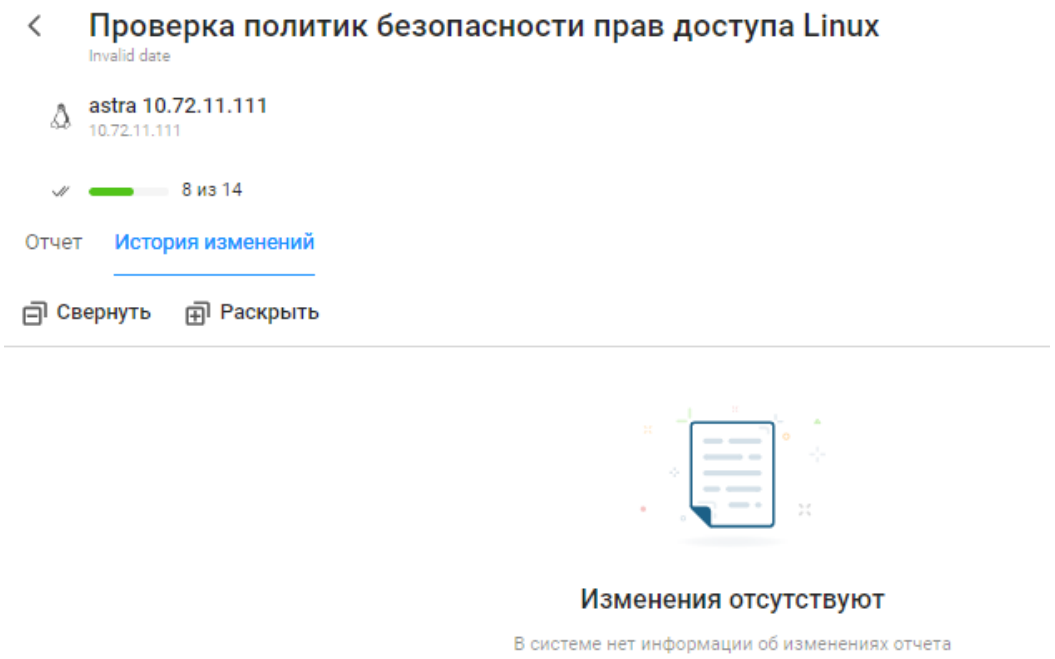


Рисунок 32 – Страница отчета стандартной проверки, вкладка «История изменений»

Зеленым выделяются добавленные элементы. Красным выделяются удаленные элементы.

При отсутствии изменении выводится соответствующая надпись.

3.2 Настройка отчетов проверки безопасности устройств

Для настройки одного отчета для выбранного устройства пользователю необходимо выполнить следующие действия:

1) Перейти в раздел «Контроль устройств», подраздел «Устройства», в дереве устройств выбрать требуемое устройство, затем перейти на вкладку «Отчеты», список «Проверки».

2) В строке требуемого отчета проверки нажать кнопку «Настройки» ( ) (рис. 33).

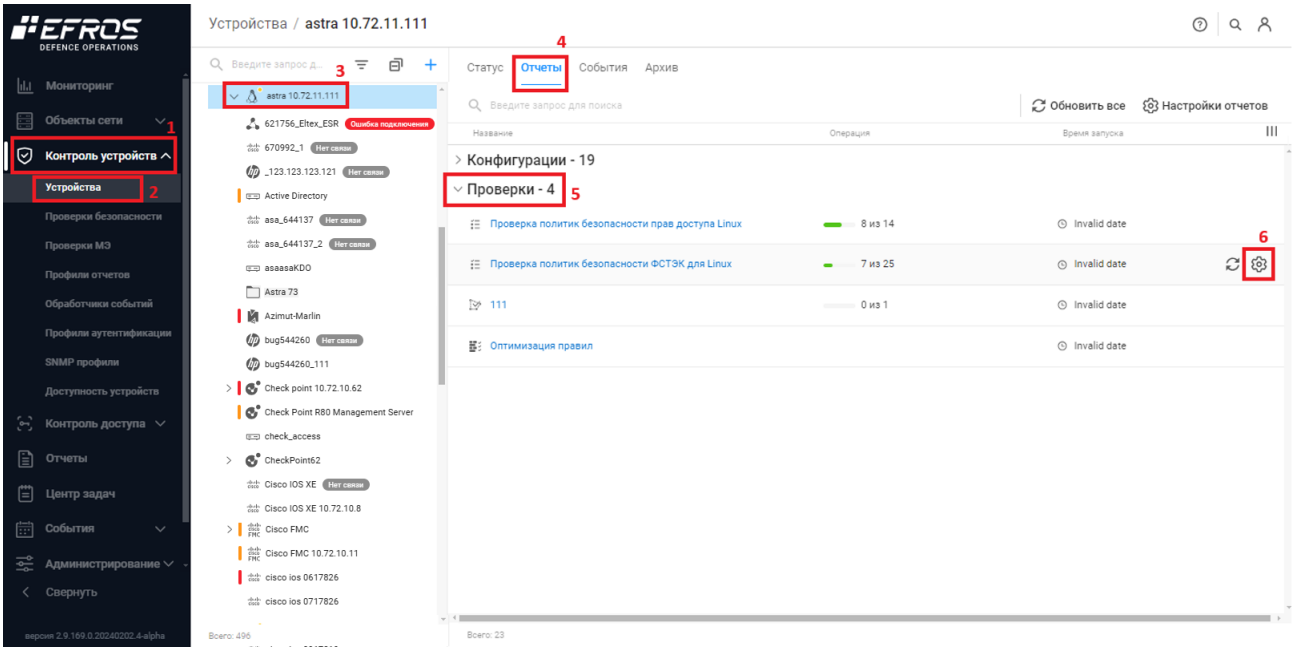


Рисунок 33 – Вкладка «Отчеты»

3) В открывшемся окне из раскрывающегося списка поля «Использование» выбрать необходимое значение (рис. 34).

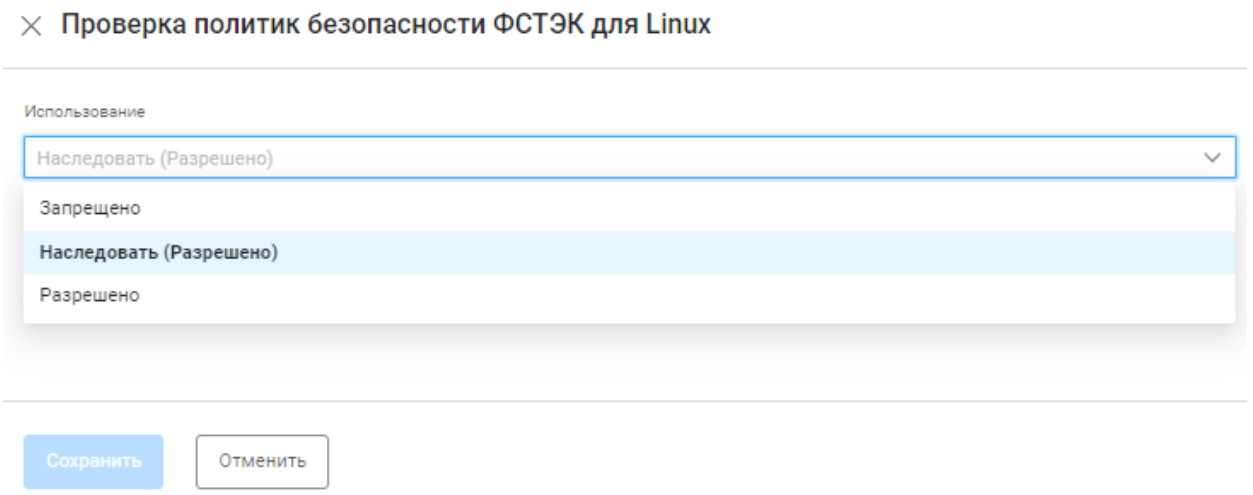


Рисунок 34 – Окно настройки отчета типа «Конфигурации»

В поле «Использование» приведены следующие режимы использования отчета «Проверки»:

- «Запрещено» – загрузка отчета с устройств запрещена вне зависимости от настроек профиля отчетов. Отчет будет скрыт с вкладки «Отчеты»;
- «Наследовать» – применить настройки профиля отчетов. В скобках отображается значение, установленное для отчета в профиле отчетов;
- «Разрешено» – загрузка отчета с устройств разрешена.

Для настройки всех отчетов для выбранного устройства пользователю необходимо выполнить следующие действия:

1) Выбрать в дереве устройств требуемое устройство. Перейти на вкладку «Отчеты».
2) В заголовке вкладки «Отчеты» нажать кнопку «Настройки отчетов» (Настройки отчетов) (см. рис. 33). Откроется окно настройки отчетов выбранного устройства (рис. 35).
3) Выбрать в поле «Профиль отчетов» из раскрывающегося списка требуемый профиль отчета.
4) Перейти на вкладку «Проверки безопасности» (рис. 35).

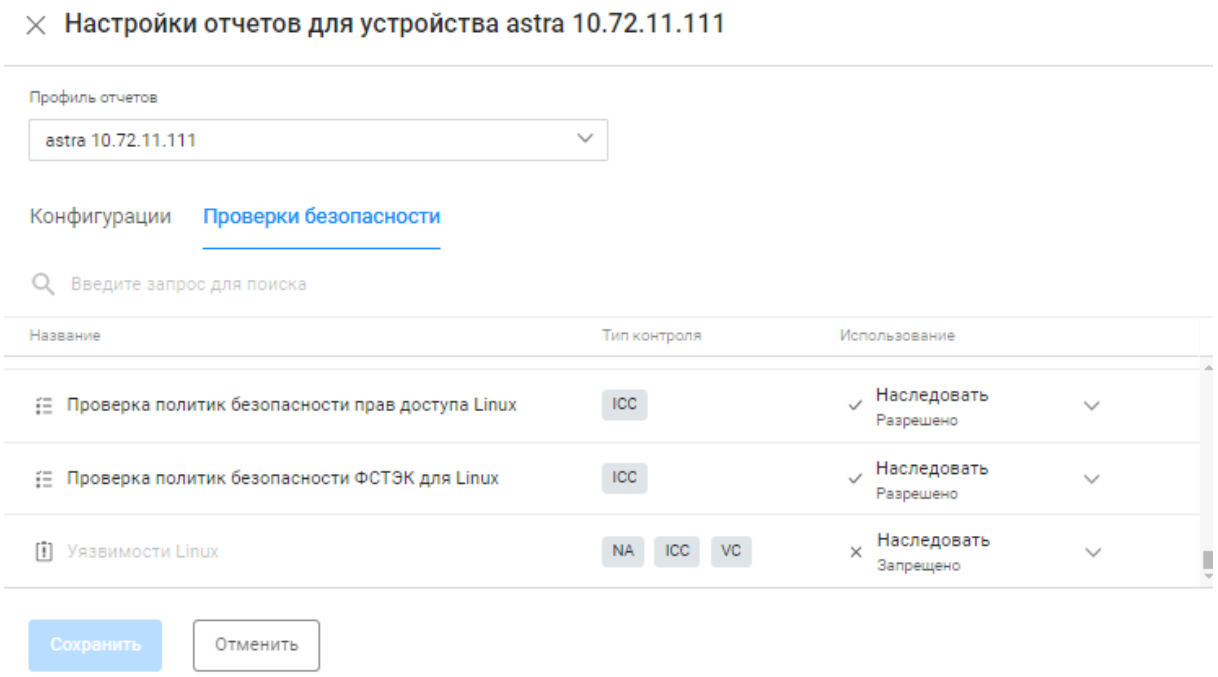


Рисунок 35 – Окно настройки отчетов выбранного устройства, вкладка «Проверки безопасности»

5) Из раскрывающегося списка столбца «Использование» выбрать необходимое значение для каждого отчета.

3.3 Просмотр стандартов и требований проверки безопасности

Перечень стандартов и требований проверки безопасности доступен для просмотра в разделе «Контроль устройств», подраздел «Проверки безопасности» (рис. 36).

Список стандартов проверок безопасности формируется динамически при подключении к комплексу внешних модулей для работы с контролируемыми устройствами, по умолчанию группируется по типам устройств (предустановленные стандарты).

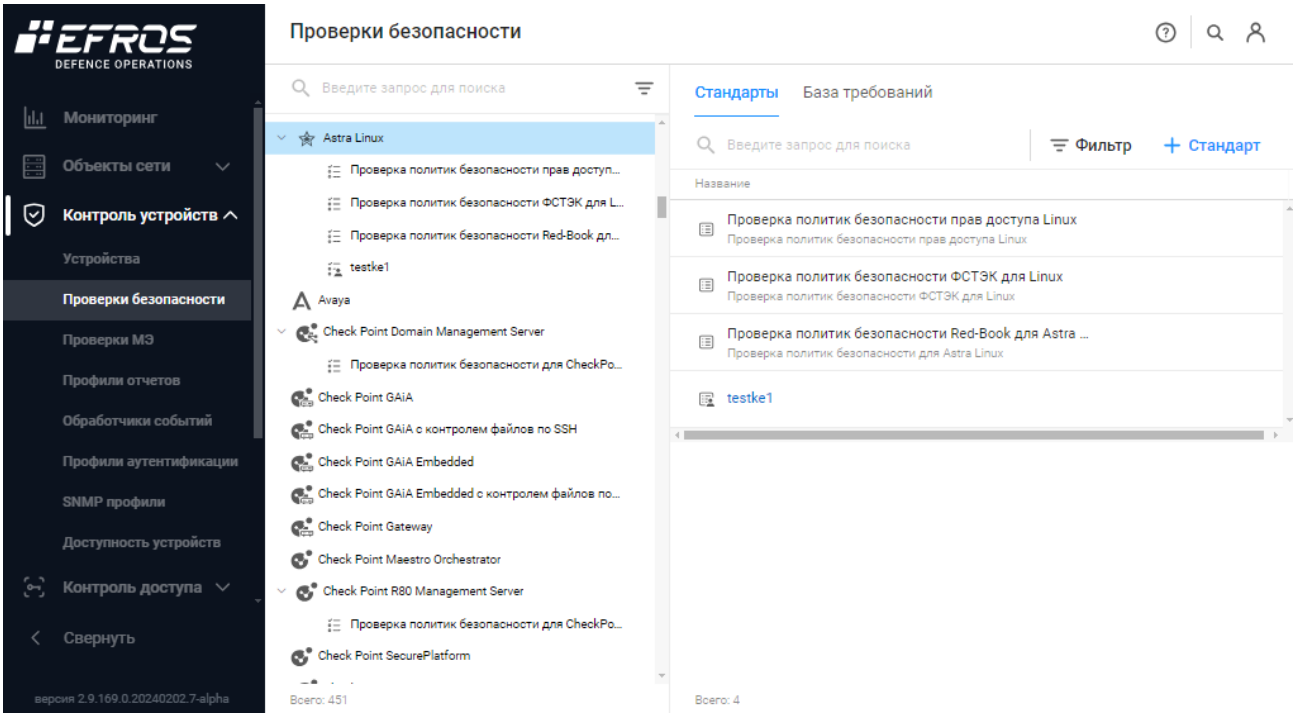


Рисунок 36 – Страница подраздела «Проверки безопасности»

Для стандартов реализован механизм редактирования исключений, что позволяет создавать новые пользовательские стандарты в комбинации с существующими стандартами или с использованием пользовательских настроек.

Страница подраздела «Проверки безопасности» содержит дерево со списком стандартов, сгруппированных по типу устройств, и в зависимости от типа выбранной в дереве сущности:

- для типа устройства – вкладки:
  - «Стандарты» – содержит перечень стандартов проверок безопасности для соответствующего типа устройств;
  - «База требований» (рис. 37) – содержит список требований безопасности для выделенного в дереве типа устройства, сгруппированный по категориям.
- для стандарта (предустановленного или пользовательского) – список требований безопасности стандарта, сгруппированный по категориям.

Для стандартов применены следующие иконки:

- « » – предустановленный стандарт;
- « » – стандарт, созданный пользователем.

В списке требований типа устройства (во вкладке «База требований») пользователь имеет возможность добавить новое пользовательское требование в стандарт. В списке требований для отдельного предустановленного стандарта может выполнить настройку использования стандарта проверки для всех устройств, к которым он может быть применен, для пользовательского стандарта – выполнить настройку

использования стандарта и добавить новое требование.

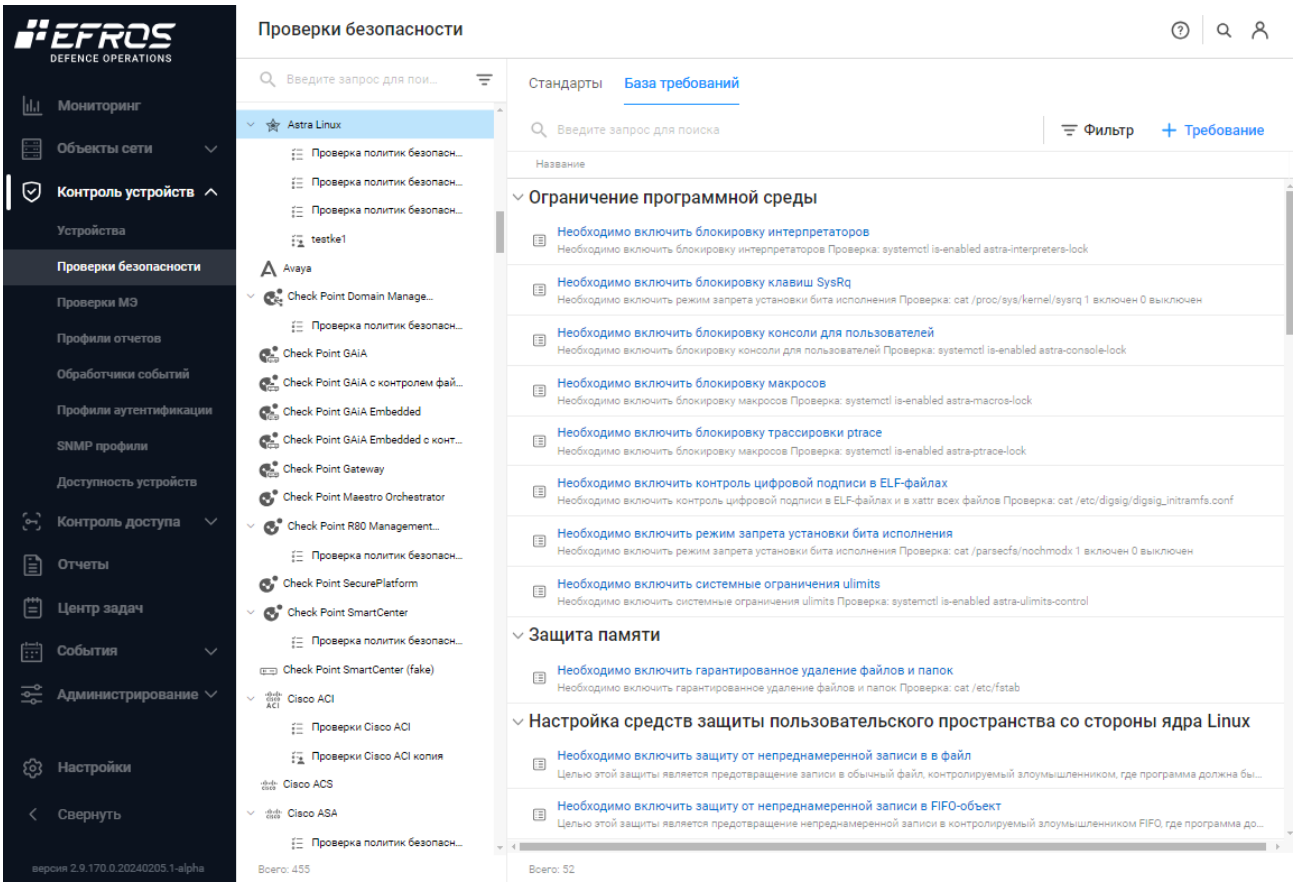


Рисунок 37 – Вкладка «База требований»

3.4 Создание пользовательской проверки безопасности

В ПК «Efros DO» реализована возможность формирования пользовательских стандартов проверок безопасности:

- на основе базы проверок модулей «Efros ICC»;
- существующих пользовательских проверок (включая проверки с помощью регулярных выражений);
- с помощью копирования и последующего редактирования уже созданных проверок.

Для стандартов реализован механизм редактирования исключений, что позволяет создавать новые пользовательские стандарты в комбинации с существующими стандартами или с использованием пользовательских настроек.

Для создания пользовательской проверки безопасности необходимо выполнить следующие действия:

1) Перейти в раздел «Контроль устройств», подраздел «Проверки безопасности».

В дереве со списком стандартов выбрать требуемый тип устройства и нажать в его строке кнопку «Добавить стандарт» (+) или нажать на вкладке «Стандарты» кнопку «Стандарт» (+ Стандарт) (рис. 38).

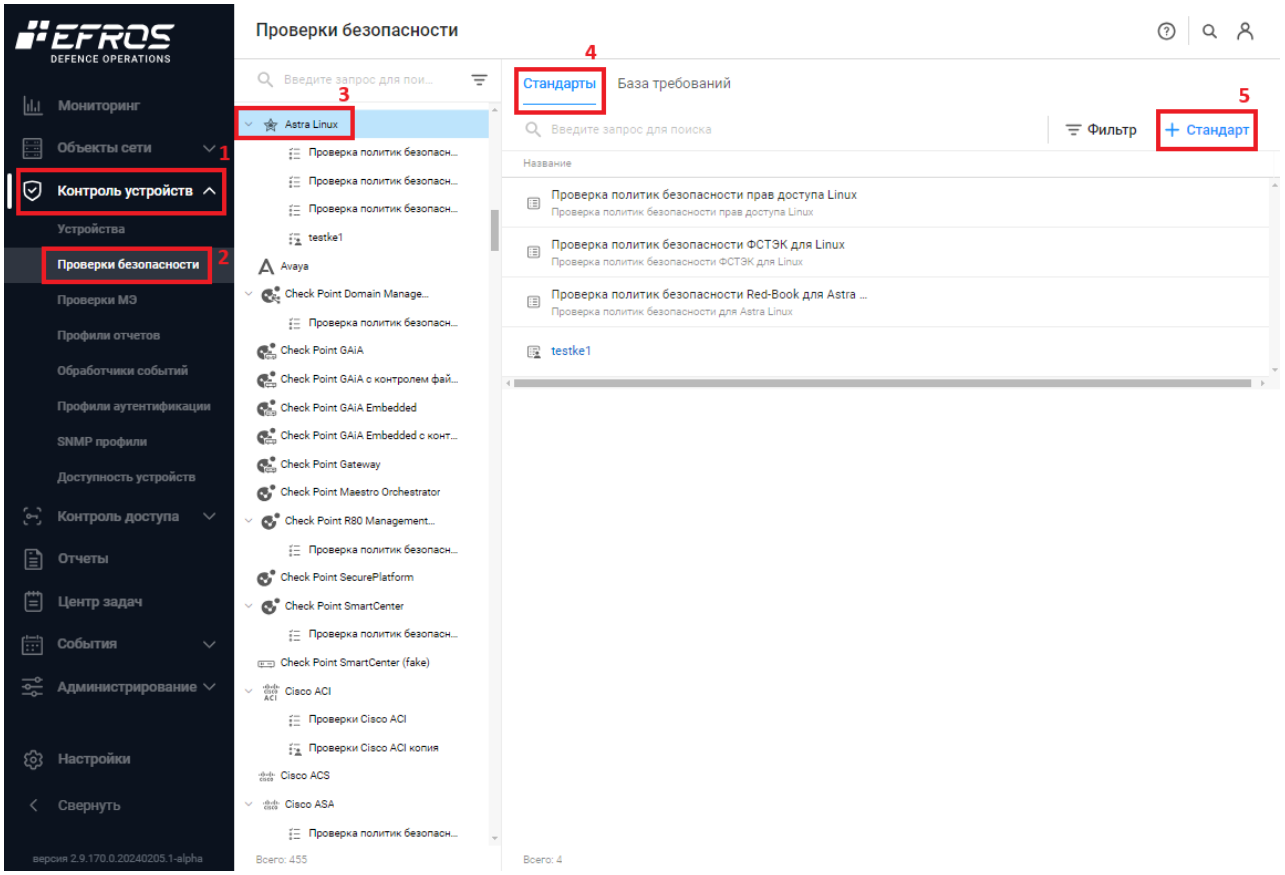


Рисунок 38 – Подраздел «Проверка безопасности»

2) Откроется страница «Создание стандарта безопасности» (рис. 39).

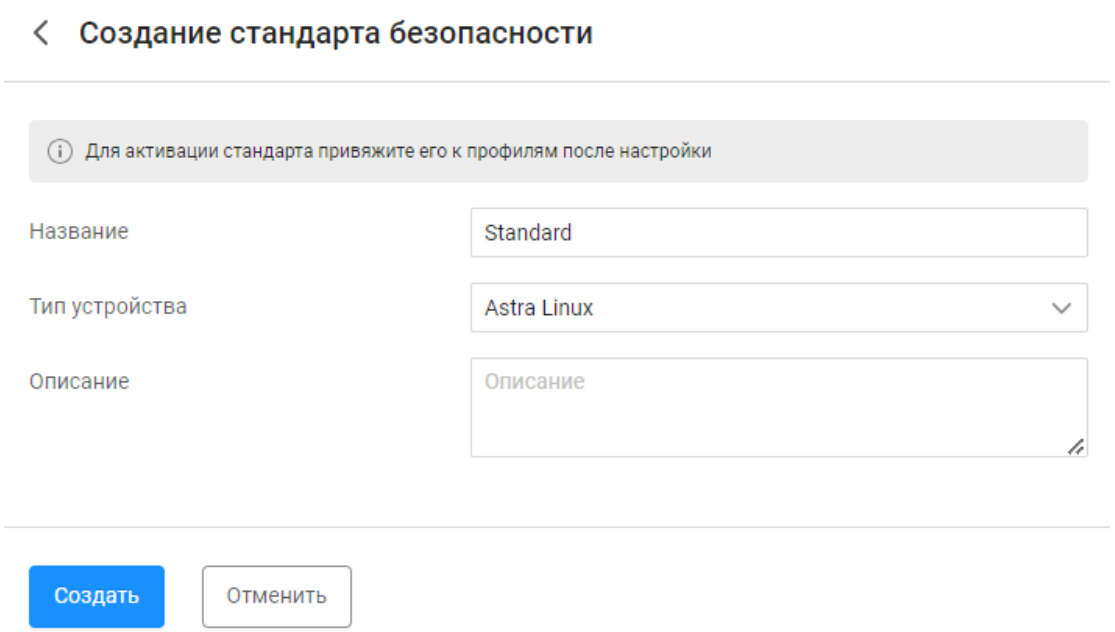


Рисунок 39 – Страница «Создание стандарта безопасности»

3) Ввести название стандарта безопасности. Поле «Тип устройства» будет заполнено автоматически.
4) Ввести при необходимости описание нового стандарта безопасности.
5) Нажать кнопку «Создать». Откроется страница подраздела «Проверка безопасности». В дереве стандартов для выбранного в перечислении 1 типа устройства добавится вложенный стандарт безопасности.

Созданный стандарт безопасности не содержит требований. Созданные пользовательские требования появятся на вкладке «База требований» после их добавления в соответствии с пунктами .

По умолчанию для созданного стандарта безопасности применяется использование «Запрещено». Для изменения использования необходимо перейти в настройки профиля отчетов.

3.4.1. Создание требования стандарта безопасности на основе выбора из базы требований

Для добавления требований в пользовательский стандарт из общей базы требований или из требований для определенного типа устройства, необходимо выполнить следующие действия:

1) В дереве подраздела «Проверки безопасности» выделить тип устройства, для которого был создан пользовательский стандарт. Затем выделить созданный

стандарт и нажать кнопку «Требование» (+ Требование), в раскрывшемся меню выбрать пункт «Выбрать» (рис. 40).

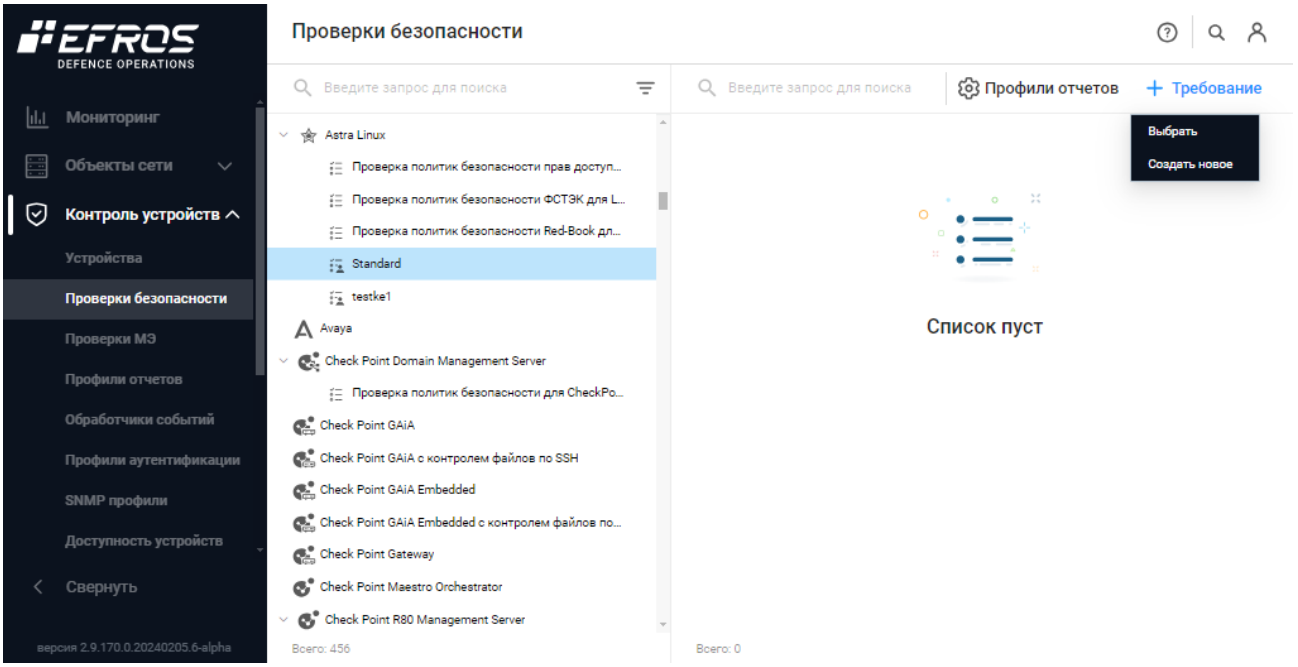


Рисунок 40 – Страница с пользовательским стандартом

2) Откроется окно «Выбор требований» (рис. 41).

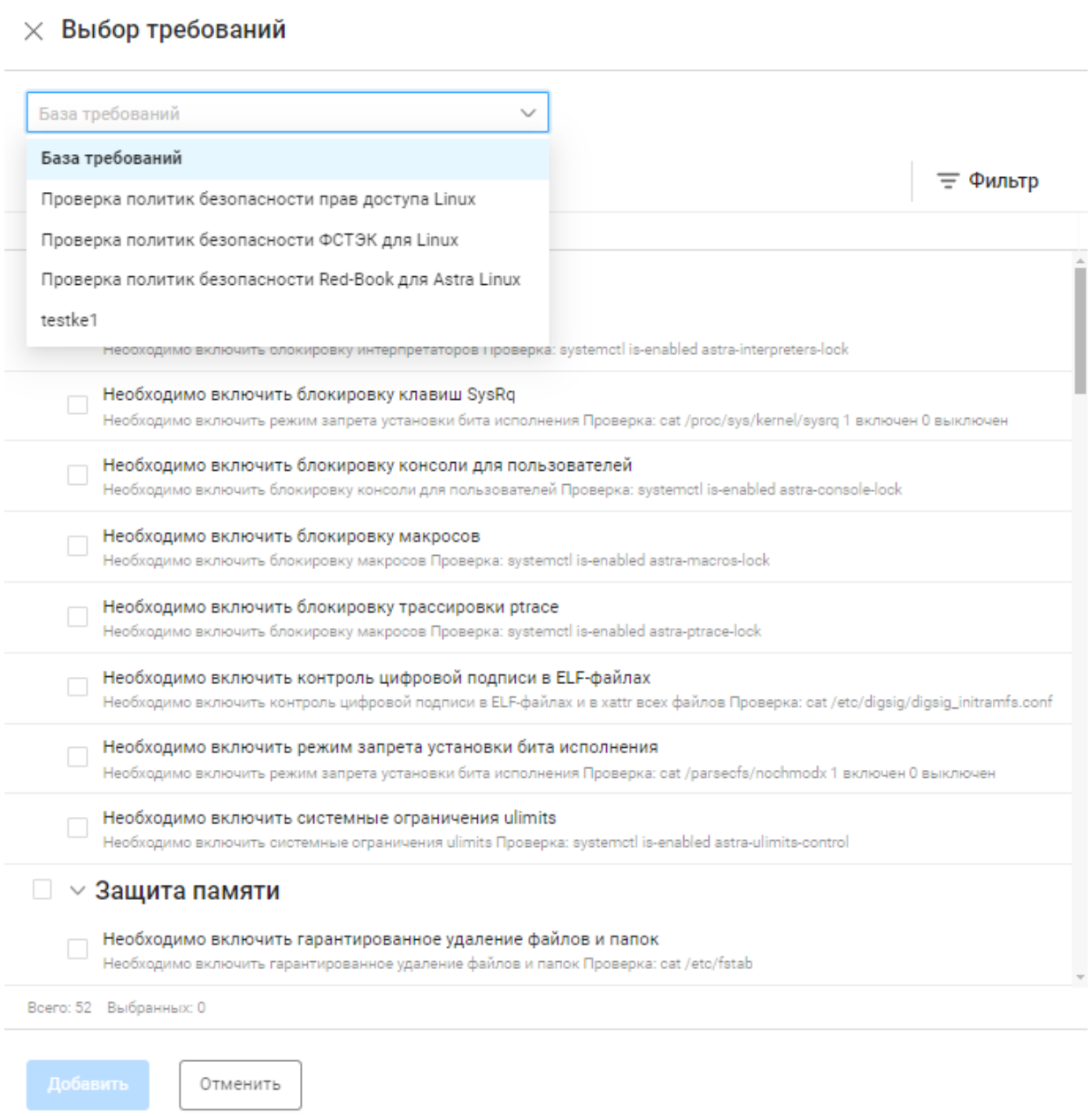


Рисунок 41 – Окно «Выбор требований»

3) В поле раскрывающегося списка «Источник требований» выбрать в качестве источника требований общую базу требований (значение «База требований») или наименование одного из существующих стандартов выбранного ранее типа устройства.
4) С помощью флагов выбрать необходимые требования (рис. 42).
5) Нажать кнопку «Добавить»

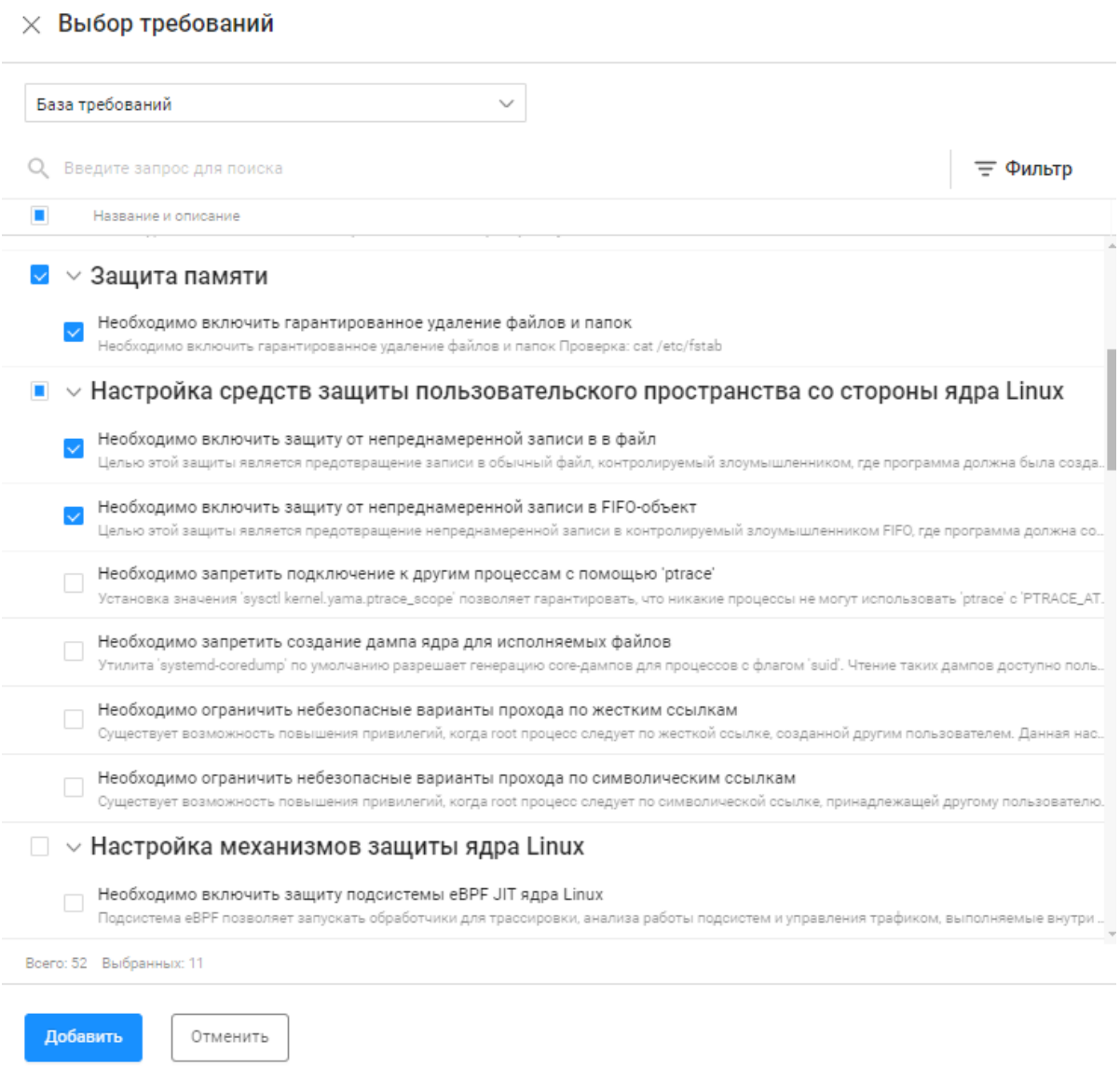


Рисунок 42 – Окно «Выбор требований»

3.4.2. Создание нового пользовательского требования стандарта безопасности

Для создания нового пользовательского требования необходимо:

1) В дереве подраздела «Проверки безопасности» выделить тип устройства, для которого был создан пользовательский стандарт. Выделить созданный стандарт (см. рис. 40).
2) Нажать кнопку «Требование» (+ Требование) и выбрать в раскрывшемся меню пункт «Создать новое». Откроется страница «Создание требования» (рис. 43).

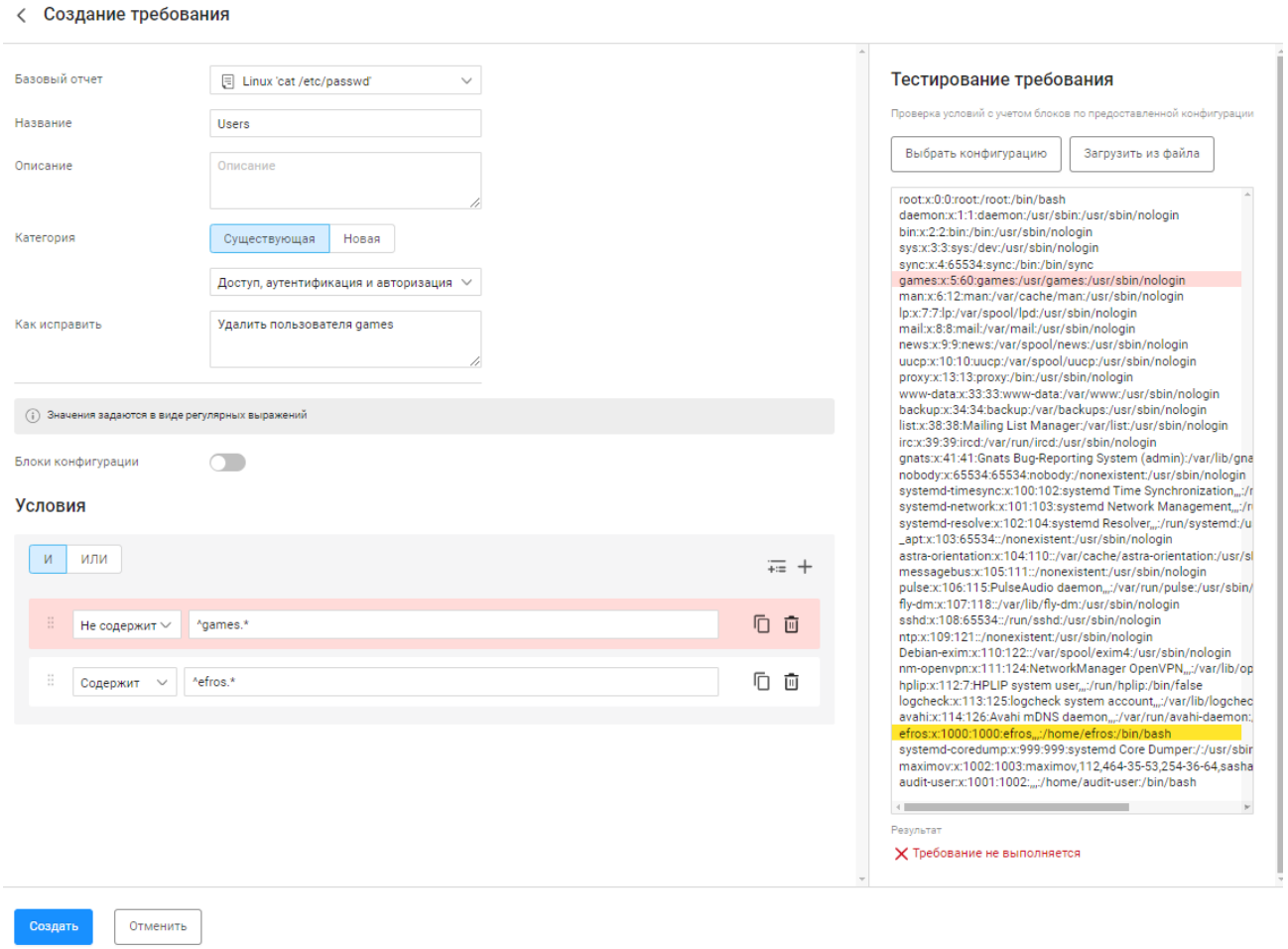


Рисунок 43 – Страница «Создание требования»

3) Заполнить поля страницы «Создание требования». Правила заполнения:

— поле «Базовый отчет» – выбрать из раскрывающегося списка;

— поле «Название» – любое;

— переключатель поля «Категория»:

- положение «Существующая» – выбрать в раскрывающемся списке категорию из существующих категорий базы требований для выбранного типа устройства (рис. 44);
- положение «Новая» – ввести название новой категории;

— поле «Как исправить» – краткое описание как исправить ошибку при невыполнении требования;

— переключатель «Блоки конфигурации» – при включении отображаются дополнительные поля для ввода начальной и конечной частей блока конфигурации и условия их поиска («в любом блоке» или «во всех блоках»), что предоставляет пользователю возможность выделить в конфигурации несколько одинаковых частей, в которых в дальнейшем можно контролировать наличие или отсутствие необходимого текста;

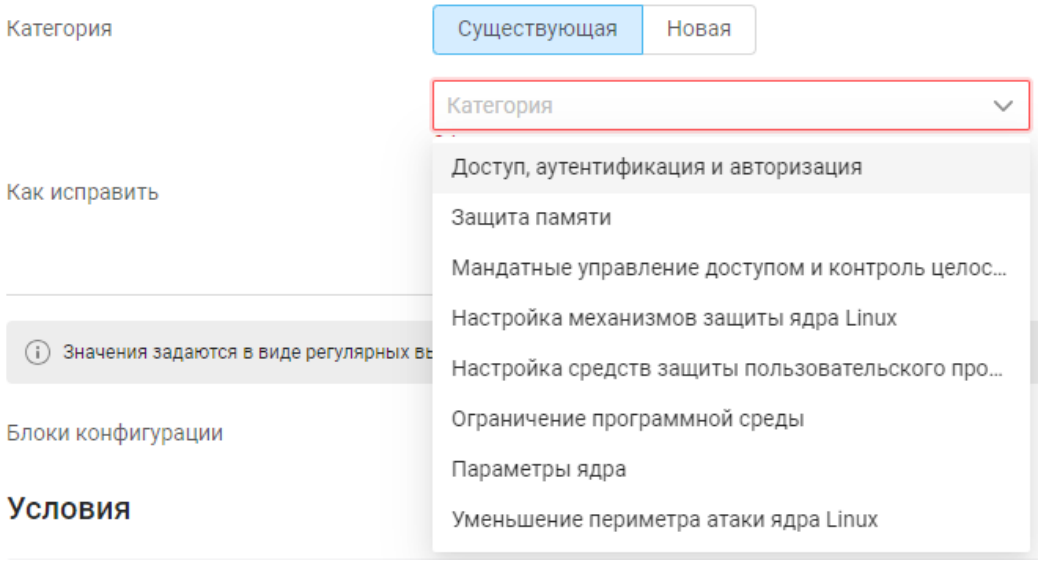


Рисунок 44 – Выбор существующей категории

— группа полей «Условия» – назначение/выбор условий выполнения требований. Блоки условий добавляются по нажатию кнопки «Добавить блок» (), отдельные условия в блоки – по нажатию кнопки «Добавить» (+) или «Копировать» (). Блоки условий выполнения требований добавляются через логические условия «и»/«или» (по выбору пользователя). В блоке может быть задано несколько условий типов «Содержит» и «Не содержит» со значениями для проверки выполнения требований Блоки условий и условия удаляются по нажатию соответствующей им кнопки «Удалить» ();
— группа полей «Тестирование требования» – проверка условий с учетом блоков по предоставленной конфигурации. Результат проверки выводится после добавления конфигурационного файла. Варианты добавления конфигурационного файла:
  - кнопка «Выбрать конфигурацию» – для выбора файла конфигурации существующего устройства;
  - кнопка «Загрузить из файла».

4 Настройка планировщика

Подраздел «Планировщик» позволяет автоматизировать действия для постоянно повторяющихся процессов или операций.

Подробное описание веб-интерфейса подраздела «Планировщик» (раздел «Администрирование») приведено в документе «Руководство пользователя. Часть 1. Настройка и администрирование».

Ниже приведена рекомендуемая последовательность работы для настройки планировщика.

4.1 Настройка расписаний для загрузки отчетов

Для автоматизации действий загрузки отчетов с устройств необходимо настроить планировщик по расписанию, для чего выполнить следующие действия:

1) Перейти в раздел «Администрирование», подраздел «Планировщик», на вкладке «По расписанию» нажать кнопку «Задача» (+ Задача) (рис. 45).

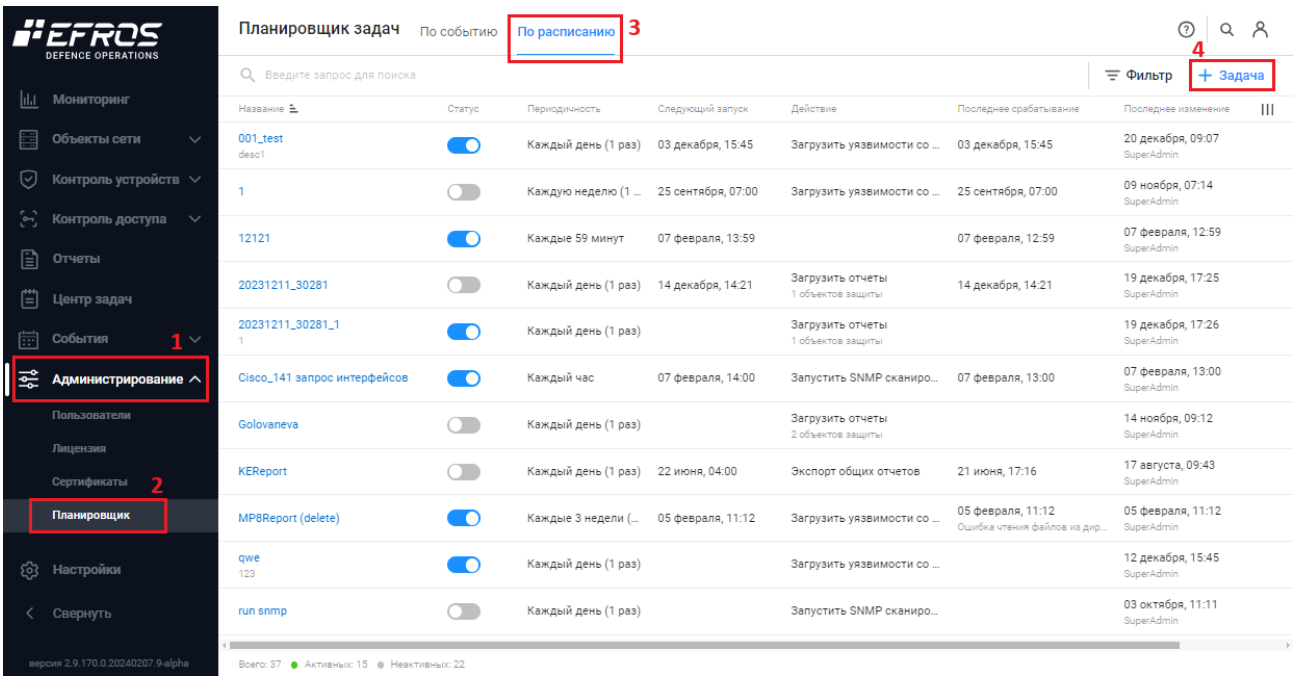


Рисунок 45 – Подраздел «Планировщик», вкладка «По расписанию»

2) Откроется страница «Создание задачи по расписанию» (рис. 46).
3) Заполнить поля страницы. Правила заполнения:
— поле «Статус» – переключатель включен (расписание активно);
— поле «Название» – любое;

— поле «Описание» – любое;
— блок полей «Действие»:
- поле «Действие» – выбрано значение «Загрузить отчеты»;
- поле «Загружать» – установлен флаг для значений «Конфигурации» и «Проверки безопасности»;
- поле «Объекты защиты» – поле для выбора устройств, для которых настраивается расписание. Устройства выбираются в окне, которое открывается по нажатию ссылки-количества объектов защиты (рис. 47).

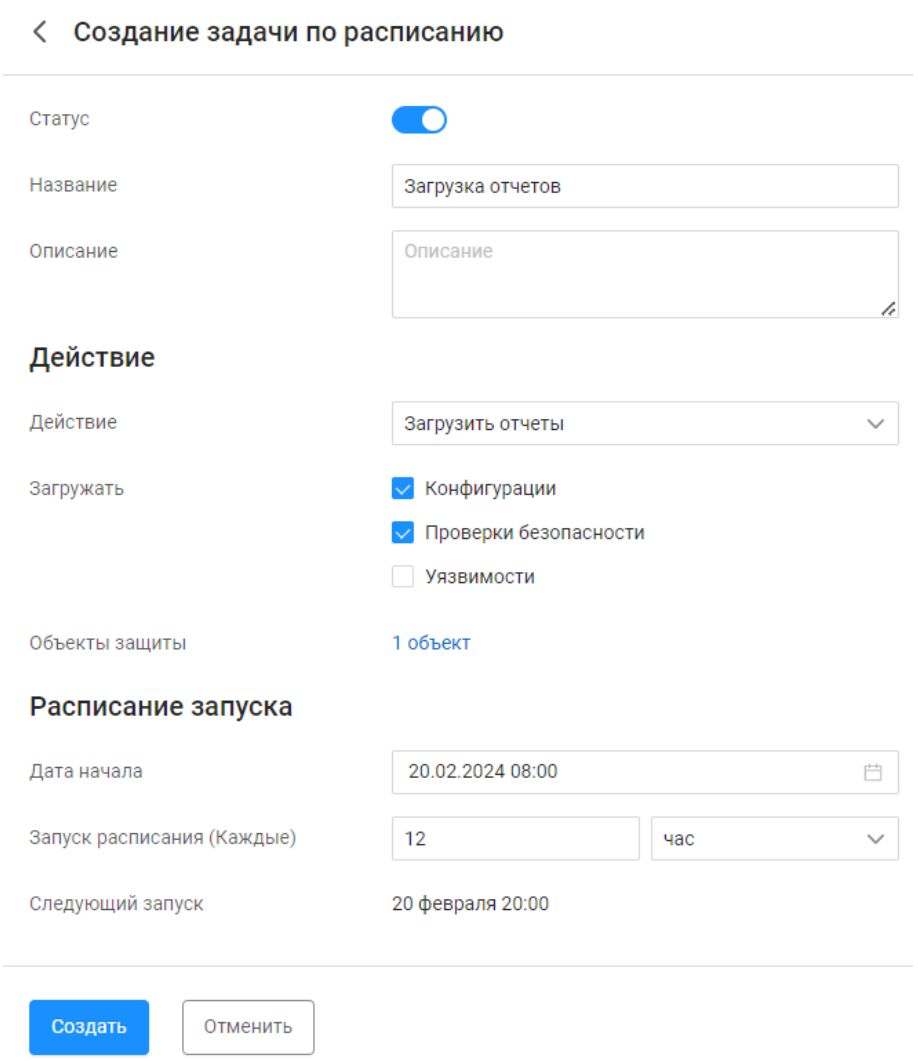


Рисунок 46 – Страница «Создание задачи по расписанию»

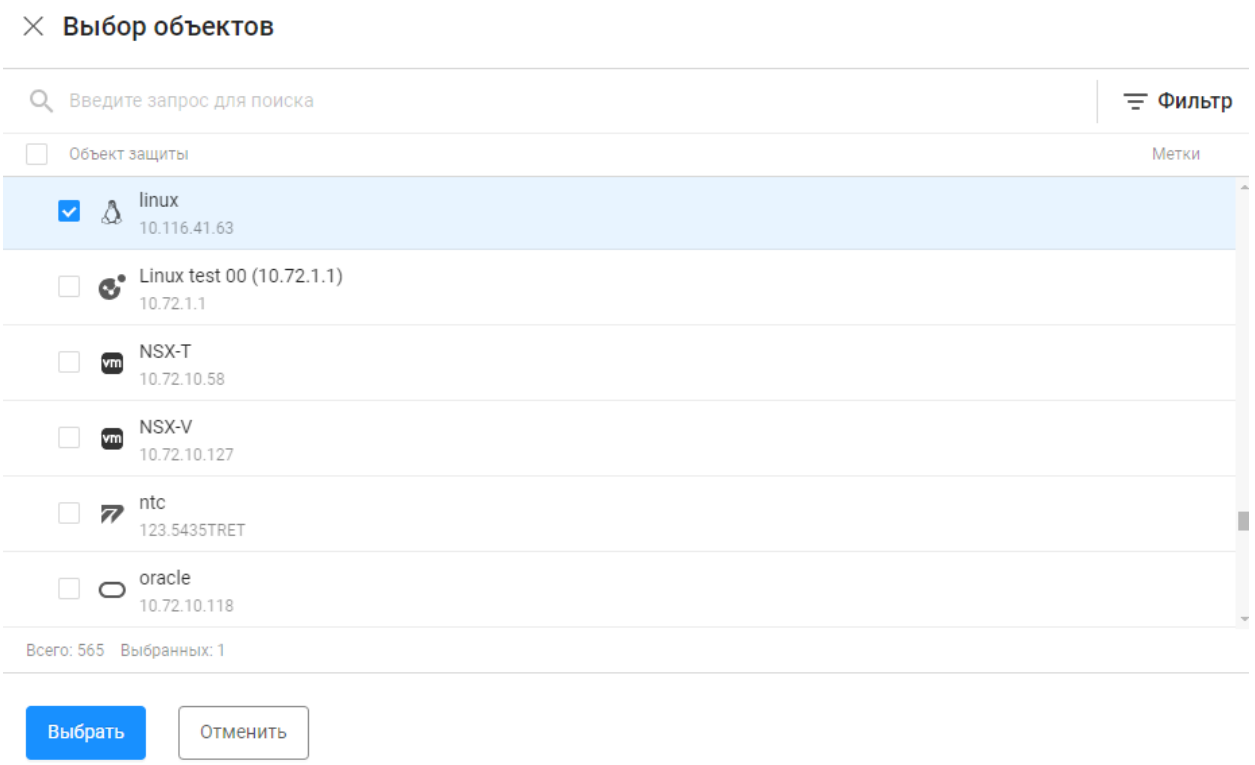


Рисунок 47 – Выбор объектов защиты

— блок полей «Расписание запуска»:

- поле «Дата начала» – требуемая дата начала работы расписания;
- поле «Запуск расписания (Каждые)» – для выбора временного интервала – количество и тип: «минута», «час», «день», «неделя», «месяц». Для периодичности «минута» или «час» устанавливается интервал времени между запусками операции соответственно в минутах или часах, «день» – в дополнительных полях ниже устанавливаются ежедневные значения времени запуска операции, «неделя» или «месяц» –в дополнительных полях ниже устанавливаются дни недели и время запуска операции;
- поле «Время старта» или «День и время старта» – для интервала «день» позволяет выбрать время запуска операции, для интервала «неделя» или «месяц» – дни недели и время запуска операции. Строки для ввода дополнительных значений добавляются по нажатию кнопки «Добавить» (+), удаляются по нажатию кнопки «Удалить» (🗑) в правой части поля.

4.2 Настройка оповещений

Для настройки оповещения об изменении конфигурации устройств необходимо настроить планировщик по событиям, для чего выполнить следующие действия:

1) Перейти в раздел «Администрирование», подраздел «Планировщик», на вкладке «По событию» нажать кнопку «Задача» (+ Задача) (рис. 48).

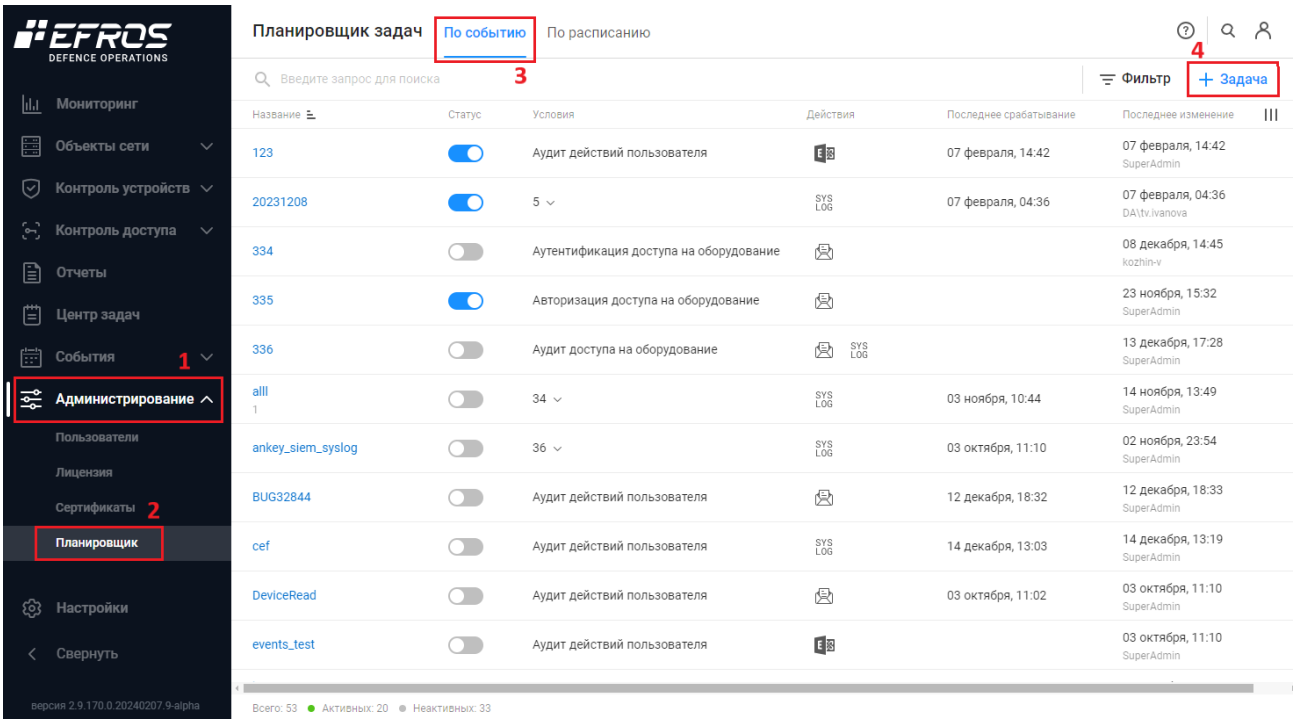


Рисунок 48 – Подраздел «Планировщик», вкладка «По событию»

2) Откроется страница «Создание задачи по событию» (рис. 49).
3) Заполнить поля страницы. Правила заполнения:

— поле «Статус» – переключатель включен (задача активна);
— поле «Название» – любое;
— поле «Описание» – любое;
— блок полей «Условия»:

- нажать кнопку «Условие» (+ Условие), из раскрывающегося списка (рис. 50) выбрать тип события «Изменение отчета»;
- нажать кнопку «Дополнительные условия», из раскрывающегося списка выбрать условие «Контроль целостности» и значение «Нарушение» (рис. 51);

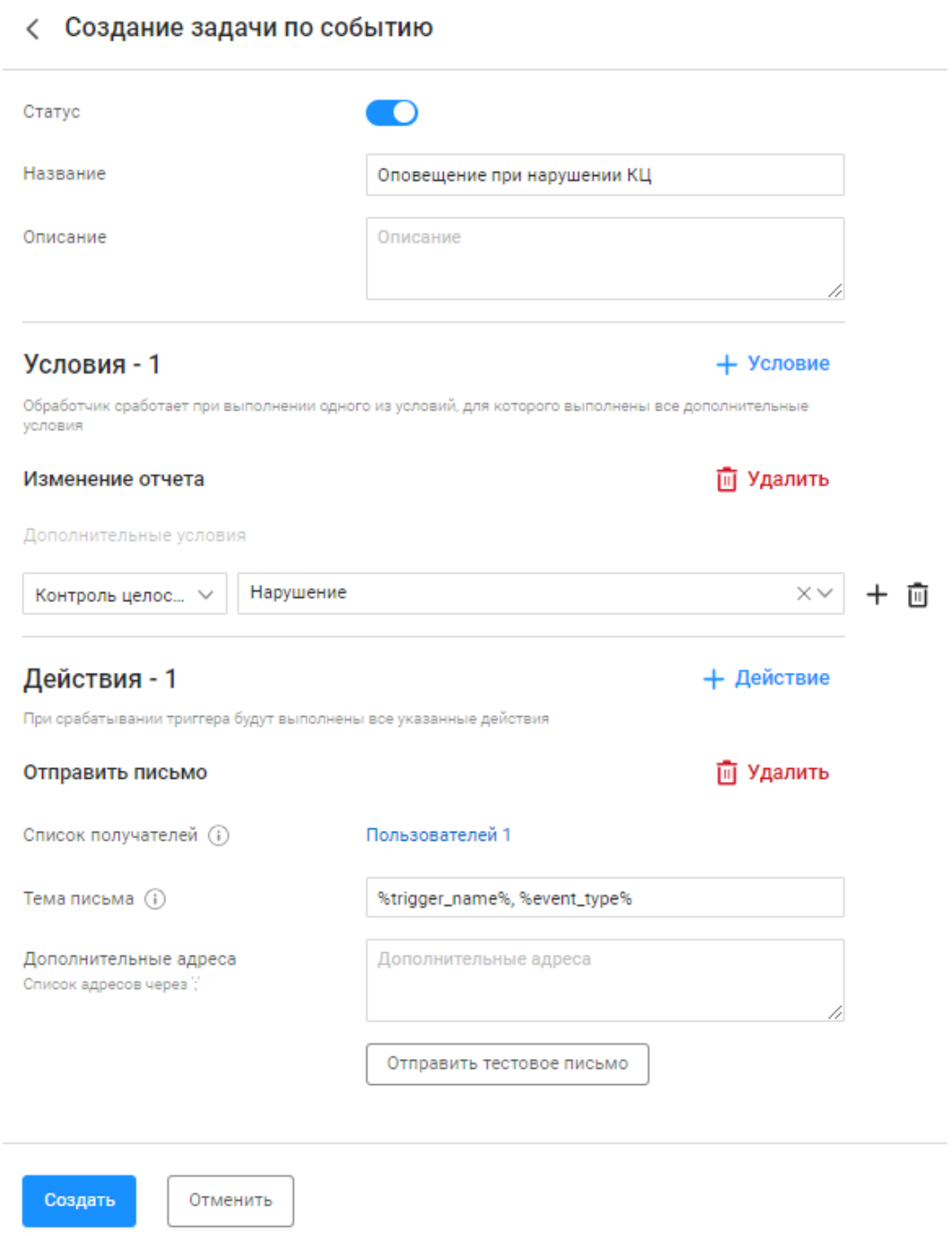


Рисунок 49 – Страница «Создание задачи по событию»

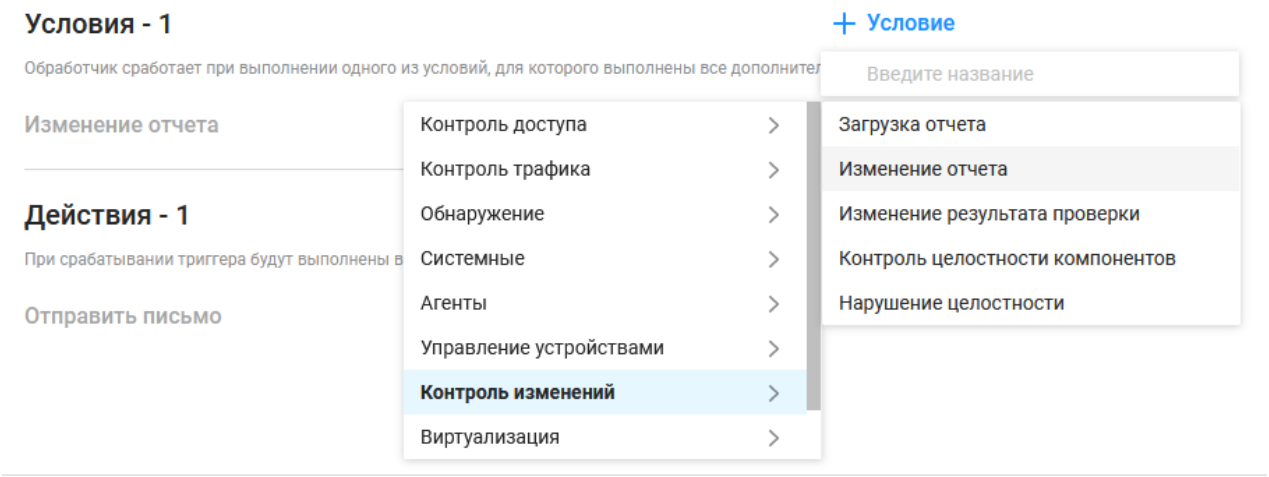


Рисунок 50 – Выбор условия

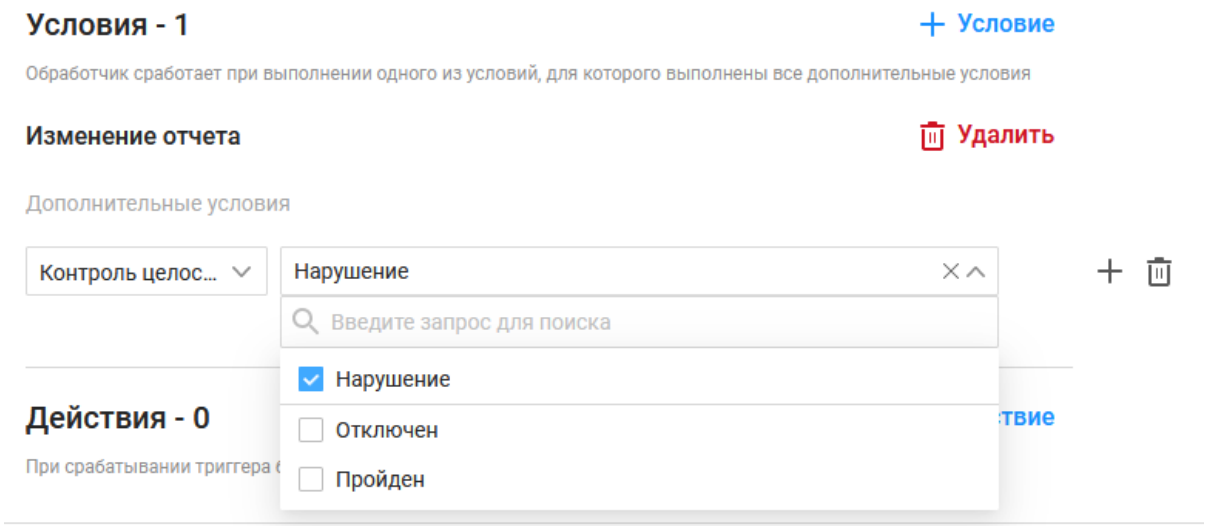


Рисунок 51 – Выбор дополнительного условия

— блок полей «Действие»:

- нажать кнопку «Действие» (+ Действие) и из раскрывающегося списка выбрать значение «Отправить письмо» (рис. 52);
- поле «Список получателей» – нажать в поле ссылку и выбрать в открывшемся окне (рис. 53) установкой флагов требуемых пользователей;
- поле «Тема письма» – ввод темы в формате: %event_type% (Название условия), %event_message% (Текст события), %trigger_name% (Название задачи), %so_name% (Название устройства);
- поле «Дополнительные адреса» – ввод дополнительных электронных адресов (ввод выполняется через символ «;»;

- кнопка «Отправить тестовое письмо» – на e-mail выбранных в поле «Список получателей» и указанных в поле «Дополнительные адреса» пользователей будет отправлено тестовое письмо.

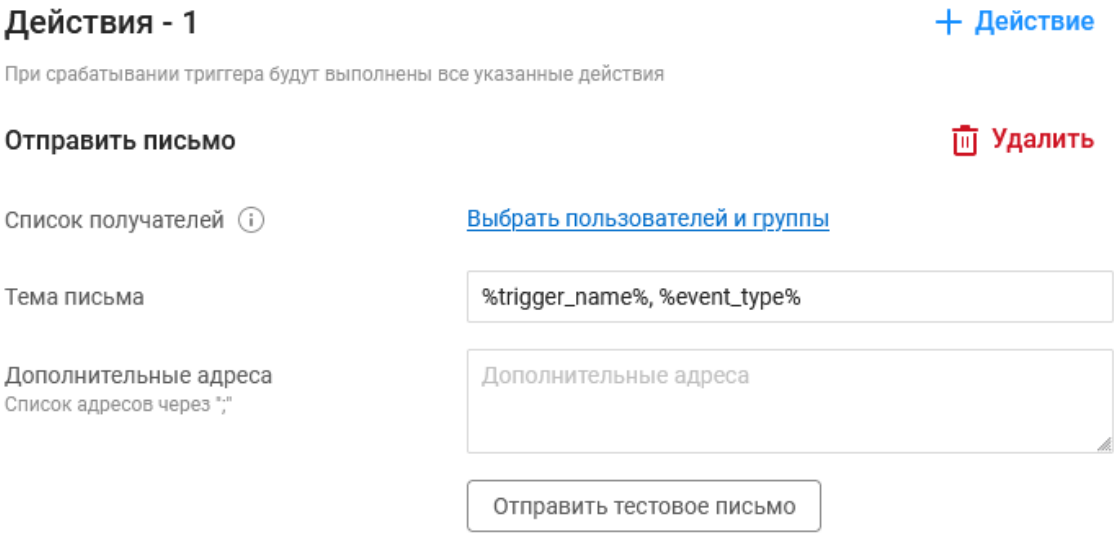


Рисунок 52 – Выбрано действие «Отправить письмо»

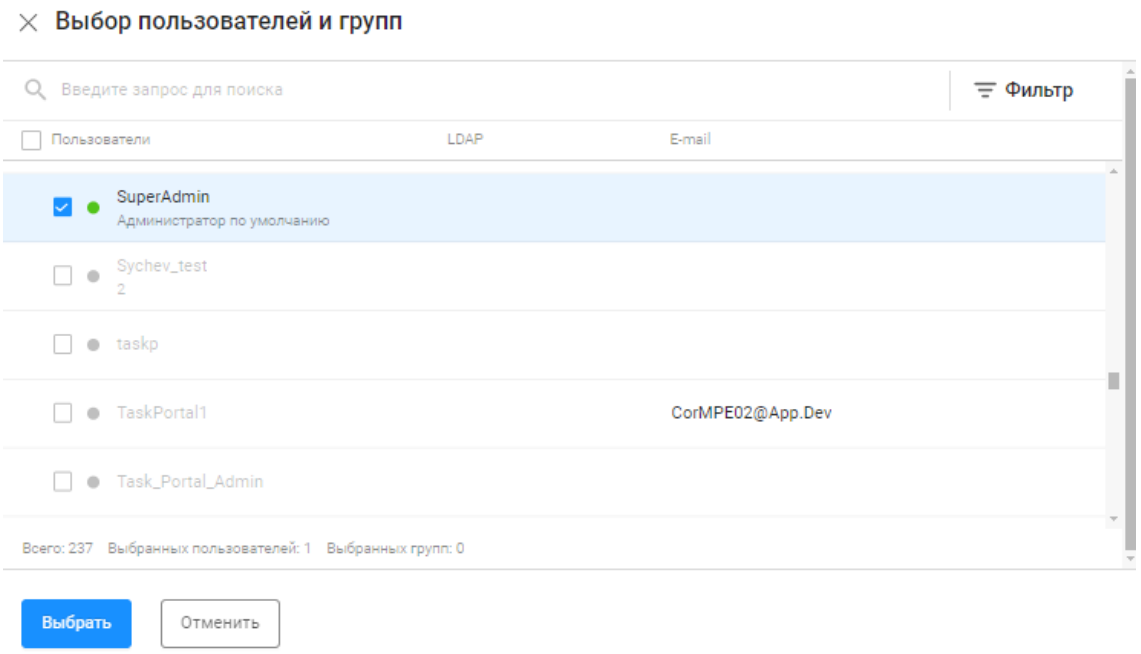


Рисунок 53 – Окно выбора пользователей и групп

Настроить оповещения об изменении конфигурации отчетов также можно с помощью обработчика событий («Контроль устройств» → «Обработчики событий»).

Перечень сокращений

ICC	–	Integrity Check Compliance
Syslog	–	System Log
БД	–	База данных
ОЗ	–	Объект защиты
ОС	–	Операционная система
ПК	–	Программный комплекс
ППО	–	Прикладное программное обеспечение
СУБД	–	Система управления базами данных