ГАЗИНФОРМ СЕРВИС

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

Руководство пользователя
Часть 3

Контроль устройств

Санкт-Петербург, 2024

Аннотация

Данный документ входит в состав руководства пользователя для работы с программным комплексом по защите системно-технической инфраструктуры «Efros Defence Operations» (далее – ПК «Efros DO» или комплекс).

Руководство содержит сведения, необходимые для работы с возможностью «Контроль устройств» в соответствующем разделе веб-интерфейса комплекса.

Возможность «Контроль устройств» доступна при установленной лицензии хотя бы на один функциональный модуль: «Efros Network Assurance» («Efros NA»), «Efros Firewall Assurance» («Efros FA»), «Efros Vulnerability Control» («Efros VC»), «Efros Integrity Check Compliance» («Efros ICC»).

Для перехода в раздел «Контроль устройств» веб-интерфейса ПК «Efros DO» необходимо выбрать в панели главного меню раздел «Контроль устройств». Если панель свернута, активная иконка «  » информирует, что текущая страница входит в раздел «Контроль устройств».

Для работы с ПК «Efros DO» пользователи должны обладать высоким уровнем квалификации и практическим опытом выполнения работ по установке, настройке и администрированию программных средств, а также иметь профессиональные знания и практический опыт в области системного администрирования. Обязательны знакомство и практический опыт настройки и администрирования активного сетевого оборудования (АСО).

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 Предварительные настройки

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

Для работы с модулями «Efros NA», «Efros FA», «Efros VC» и «Efros ICC» необходимо произвести следующие подготовительные действия:

- загрузить внешние модули для работы с устройствами;
- перевести переключатель «Состояние» требуемых модулей в положение «Активен» « ».
- добавить учетные записи пользователей объектов защиты (устройств).

Для успешной работы с устройствами пользователь предварительно должен убедиться, что загрузка (установка) внешних модулей выполнена в полном объеме, иначе не удастся зарегистрировать в комплексе некоторые виды устройств. Установку внешних модулей можно проверить, перейдя в раздел «Настройки», затем подраздел «Модули» и проверить включение модулей – переключатель «Состояние» должен быть в положении активен « ». Более подробно см. документ «Руководство пользователя. Часть 1. Настройка и администрирование».

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

2 Раздел «Контроль устройств»

В разделе «Контроль устройств» доступны функции следующих модулей ПК «Efros DO»:

- модуль «Efros NA» – предназначен для контроля сетевой составляющей объектов защиты (ОЗ) с последующим отображением ОЗ на карте сети с возможностью моделирования прохождения трафика;
- модуль «Efros FA» – предназначен для анализа межсетевых экранов (МЭ) и предоставляет возможность использовать оптимизацию правил, стандарты МЭ, зонный анализ;
- модуль «Efros VC» – предназначен для контроля уязвимостей, обнаруженных на ОЗ, предоставляет возможность построения векторов атак;
- модуль «Efros ICC» – предназначен для контроля целостности файлов операционной системы и контроля их конфигураций, текстовых файлов и т.д.

Рекомендуемая последовательности работы для настройки возможностей контроля целостности функционального модуля «Efros ICC» приведена в приложении А.

2.1 Устройства

Отображаемые данные и доступная функциональность подраздела «Устройства» зависят от наличия хотя бы одной лицензии на функциональные модули «Efros NA», «Efros FA», «Efros VC» или «Efros ICC».

Подраздел «Устройства» (рис. 1) позволяет выполнять следующие действия с контролируемыми ОЗ (далее – устройствами):

- просмотр/изменение списка устройств;
- просмотр/изменение свойств групп устройств и отдельных устройств;
- загрузка отчетов с устройств;
- просмотр уведомлений, последних архивных отчетов и событий устройств;
- выполнение действий с устройствами;
- настройка списка доступных для запуска отчетов устройств.

Страница подраздела содержит следующие элементы:

- дерево устройств – иерархический список контролируемых в ПК «Efros DO» устройств;
- вкладка «Статус»;
- вкладка «Отчеты»;
- вкладка «События»;
- вкладка «Архив».

Для групп устройств в подразделе доступны вкладки:

- вкладка «Статус»;
- вкладка «События».

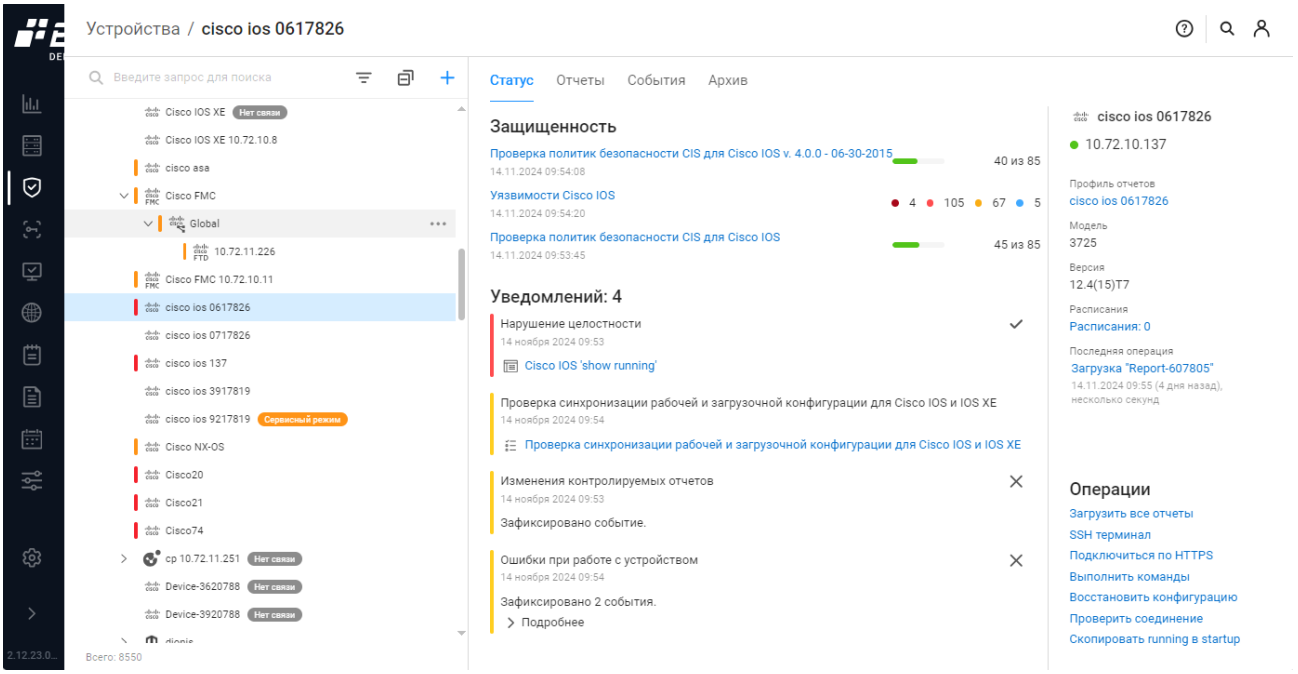


Рисунок 1 – Подраздел «Устройства»

2.1.1. Дерево устройств

Над деревом устройств (см. рис. 1) располагаются:

- поле поиска (Введите запрос для поиска);
- кнопка «Фильтр» ( );
- кнопка «Свернуть» ( ) для сворачивания дерева устройств до первого уровня;
- кнопка «Добавить» ( ) для создания нового устройства или новой группы устройств.

При наведении курсора на устройство в дереве устройств появится кнопка «Контекстное меню» ( ), при нажатии которой раскрывается меню с пунктами:

- «Изменить»;
- «Создать копию»;
- «Загрузить конфигурации» – выполнить действия по конфигурированию выбранного устройства;
- «Принять все изменения» – запустить подтверждение изменений всех конфигурационных файлов и списков выделенных устройств/групп устройств;
- «Остановить все операции» – остановить выполнение проверок и загрузку отчетов на выбранных устройствах или группах устройств;
- «Включить сервисный режим» – перейти в сервисный режим, в котором

устройство не опрашивается по заданному расписанию, не проверяется его доступность в автоматическом режиме, обновление данных выполняется только по запросу пользователя;

— «Удалить».

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.

2.1.1.1. Добавление устройства

Добавление устройств для контроля в комплексе может быть выполнено как в подразделе «Устройства» раздела «Контроль устройств», так и в подразделе «Объекты защиты» раздела «Объекты сети» с включением для устройства возможности «Контроль устройств» (более подробно см. документ «Руководство пользователя. Часть 2. Объекты сети и мониторинг»).

Для добавления устройства в подразделе «Устройства» раздела «Контроль устройств» пользователю необходимо выполнить следующие действия:

1) В дереве устройств нажать кнопку «Добавить» (+) и в контекстном меню выбрать пункт «Устройство».
2) Откроется страница «Создание устройства» (рис. 2). Заполнить поля вкладок страницы необходимыми параметрами:

— «Свойства» – вкладка активна по умолчанию, необходимо указать параметры добавляемого устройства. Состав полей вкладки «Свойства» зависит от типа добавляемого устройства. На рис. 2 приведен пример вкладки «Свойства» для типа устройств 3Com OS. Состав и описание полей вкладки для различных типов устройств приведены в таблице 1;
— «Расписания» – позволяет настроить параметры использования расписаний для

добавляемого устройства. Вкладка становится доступной только после создания устройства.

3) Нажать кнопку «Создать».

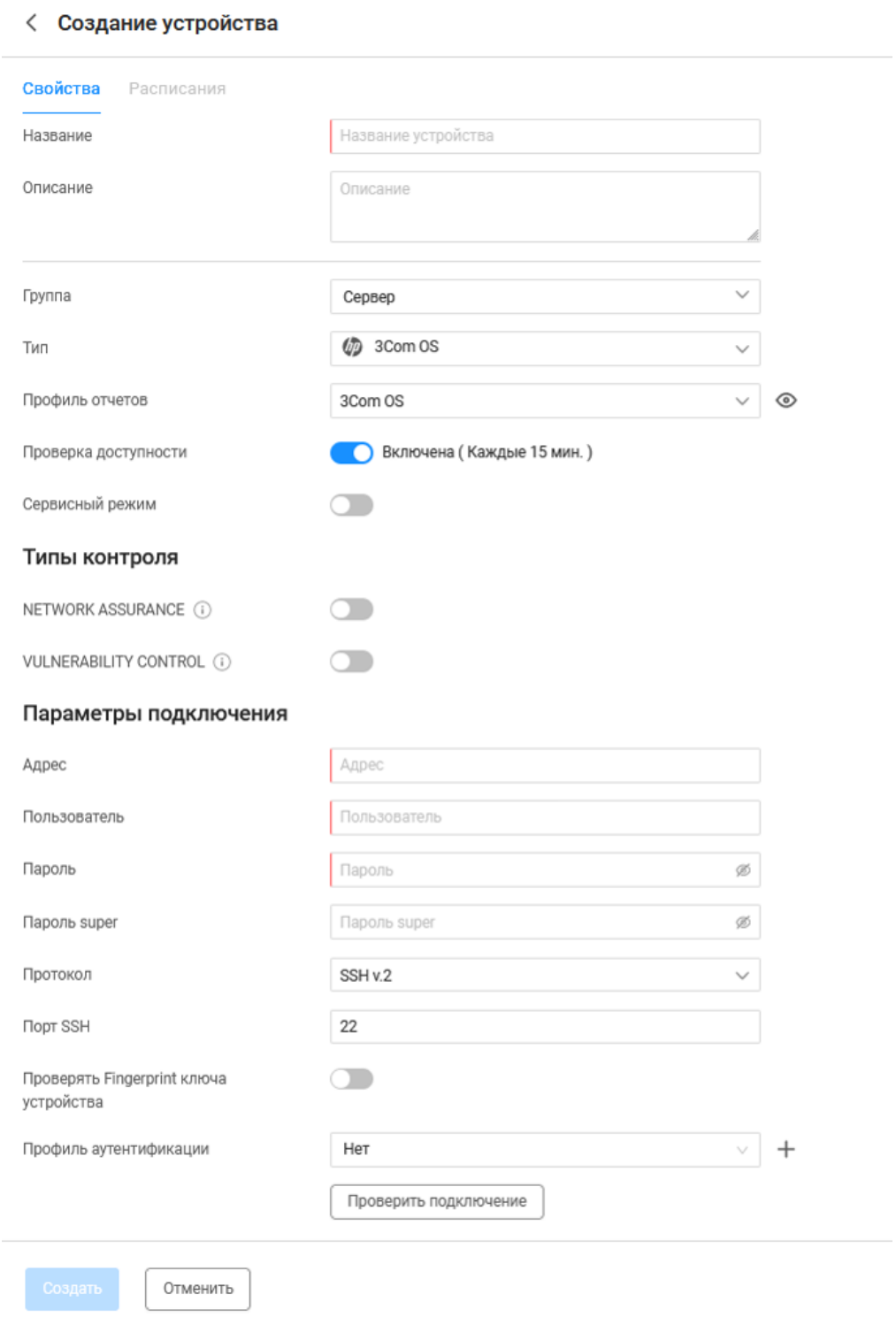


Рисунок 2 – Страница «Создание устройства». Вкладка «Свойства» для типа устройств 3Com OS

Таблица 1 – Состав и описание полей вкладки «Свойства»

Поле	Описание
Поле «Название»	Текстовое поле для ввода имени устройства. Параметры ввода текста: от 1 до 50 любых символов
Поле «Описание»	Текстовое поле для ввода описания устройства. Параметры ввода текста: от 1 до 250 любых символов
Поле «Группа»	Раскрывающийся список доступных для выбора групп. По умолчанию принимает значение «Сервер»
Поле «Тип»	Раскрывающийся список доступных для добавления на сервер ПК «Efros DO» типов устройств. Зависит от подключенных к серверу ПК «Efros DO» внешних модулей
Поле «Профиль отчетов»	Раскрывающийся список профилей отчетов. Позволяет задавать параметры контроля устройств. Зависит от выбранного типа устройства
Поле «Проверка доступности»	Переключатель: включение/отключение проверки доступности устройства с указанной периодичностью (каждые 15 мин.)
Поле «Сервисный режим»	Переключатель: включение/отключение сервисного режима для устройства. В сервисном режиме устройство не опрашивается по заданному расписанию и не проверяется в автоматическом режиме его доступность, обновление данных выполняется только по запросу пользователя
Группа полей «Типы контроля». Состав полей зависит от выбранного типа устройства в поле «Тип»	
Переключатель «Network Assurance»	Переключатели. По умолчанию выключены. Переключатель отображается, если для данного типа устройства поддерживается соответствующий тип контроля. Справа от переключателя расположен символ «ⓘ». При наведении на него курсора отображается всплывающая подсказка с описанием соответствующего типа контроля
Переключатель «Firewall Assurance»	
Переключатель «Integrity Check Compliance»	
Переключатель «Vulnerability Control»	
Переключатель «Change Manager»	Переключатель. По умолчанию выключен. Переключатель отображается при наличии лицензии на модуль «Efros CM» и только для устройств, поддерживающих тип контроля FA
Возможное информационное сообщение под переключателем	Сообщение при попытке включения переключателя: — «Достигнут лимит лицензий»; — «Превышен лимит лицензий (количество доступных и используемых лицензий)»
Группа полей «Параметры подключения». Состав полей зависит от выбранного типа устройства в поле «Тип». Ниже приведено описание основных используемых полей	
Поле «Адрес»	IP-адрес или доменное имя устройства. Параметры для ввода текста: от 1 до 50 символов, формат от 0.0.0.0 до

Поле	Описание
	255.255.255.255
Поле «Пользователь»	Логин пользователя для аутентификации на устройстве. Форматы ввода: — логин; — домен\логин; — логин@домен (в формате UPN)
Поле «Способ аутентификации»	Раскрывающийся список: — по паролю; — по закрытому ключу
Поле «Пароль»	Поле появляется при выборе в способе аутентификации значения «По паролю». Необходимо указать пароль пользователя для аутентификации на устройстве
Поле «Закрытый ключ»	Поле появляется при выборе в способе аутентификации значения «По закрытому ключу». По нажатию кнопки « » открывается диалоговое окно для выбора и загрузки файла с закрытым ключом
Поле «Закрытый ключ защищен паролем»	Переключатель: — «Включение»; — «Отключение»
Поле «Пароль закрытого ключа»	Поле появляется при активации переключателя «Закрытый ключ защищен паролем». Необходимо указать пароль
Поле «Порт SSH»	Указать используемый порт
Поле «Sudo пароль»	При выборе способа аутентификации «по закрытому ключу» необходимо указать пароль для аутентификации в sudo
Поле «Профиль аутентификации»	Раскрывающийся список поля содержит значение «Нет» и наименования профилей аутентификации, имеющихся в комплексе. В списке необходимо выбрать профиль аутентификации (имя учетной записи (логин) и пароль), который будет использоваться при аутентификации на контролируемом устройстве. Если требуемого профиля нет, то пользователь может добавить его, нажав кнопку «Добавить» (+) справа от поля или выбрав в списке профилей значение «Новый профиль». В появившейся вкладке заполнить поля для добавления в комплекс профиля аутентификации и нажать кнопку «Создать». Пользователь также имеет возможность внести изменения в выбранный в поле профиль, для чего необходимо после выбора профиля нажать справа в поле кнопку «Редактировать» (), внести изменения в открывшемся окне параметров профиля аутентификации и нажать кнопку «Сохранить» (более подробно описано в разделе 2.6)
Кнопка «Проверить подключение»	По нажатию кнопки выполняется проверка подключения устройства. После завершения проверки слева от кнопки отображается результат проверки: «Успешно» или «Ошибка подключения» и ссылка «Лог операции», при выборе которой открывается окно с отчетом о

Поле	Описание
	выполнении проверки
Элементы управления	
Создать	При нажатии на кнопку введенные данные сохраняются
Отменить	При нажатии на кнопку введенные данные не сохраняются

Для добавления некоторых типов устройств в список контролируемых на сервере комплекса необходимо предварительно создать или подключить внешний модуль, обеспечивающий взаимодействие устройств соответствующего типа с комплексом. В противном случае в поле «Тип» вкладки «Свойства» будет отсутствовать необходимый тип подключаемого устройства.

При подключении к добавленному оборудованию с помощью сторонних клиентов возможны следующие форматы ввода логина пользователя: логин; домен\логин; логин@домен (в формате UPN).

2.1.1.2. Добавление группы устройств

Для добавления группы устройств в список контролируемых комплексом групп устройств пользователю необходимо выполнить следующие действия:

1) В дереве устройств нажать кнопку «Добавить» (+) и в контекстном меню выбрать пункт «Группа».
2) Откроется страница «Создание группы» (рис. 3). Заполнить поля страницы необходимыми параметрами. Состав и описание полей приведены в таблице 2.
3) Нажать кнопку «Создать».

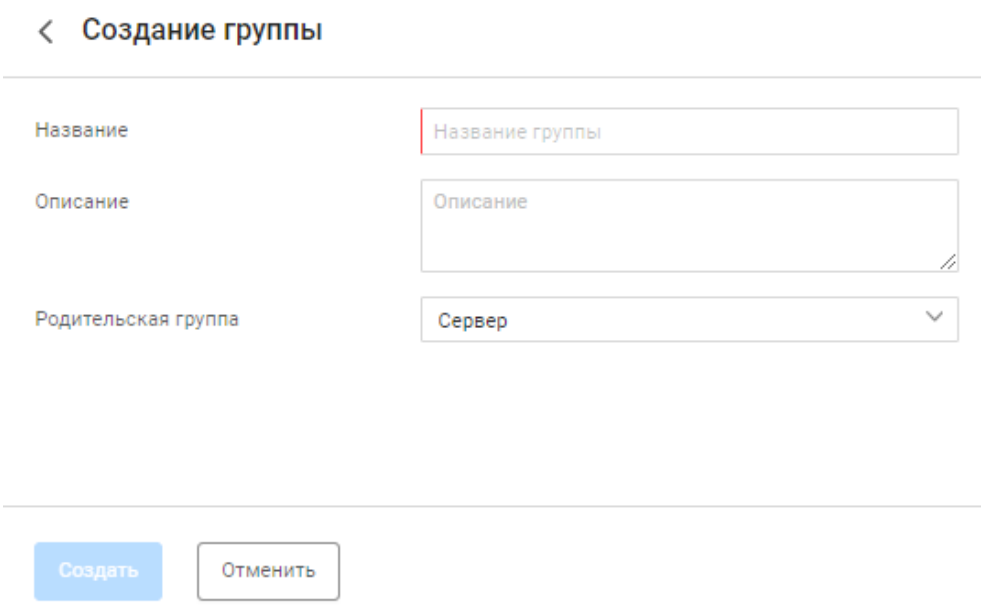


Рисунок 3 – Страница «Создание группы»

Таблица 2 – Состав и описание страницы «Создание группы»

Поле	Описание
Поле «Название»	Текстовое поле для ввода названия группы устройств. Параметры ввода текста: от 1 до 50 символов. Допустимые символы: буквы латинского и кириллического алфавитов, цифры, знак «пробел», «_», «–»
Поле «Описание»	Текстовое поле для ввода описания группы устройств. Параметры ввода текста: от 1 до 250 символов
Поле «Родительская группа»	Раскрывающийся список доступных для выбора групп, куда будет входить создаваемая группа устройств
Элементы управления	
Создать	При нажатии на кнопку введенные данные сохраняются
Отменить	При нажатии на кнопку введенные данные не сохраняются

2.1.2. Вкладка «Статус» для одного устройства

Вкладка «Статус» содержит сведения, относящиеся к устройству, выделенному в дереве устройств, и разделена на блоки:

- «Защищенность» (см. подпункт 2.1.2.1);
- «Уведомления» (см. подпункт 2.1.2.2);
- «Информация об устройстве» (см. подпункт 2.1.2.3);
- «Операции» (см. подпункт 2.1.2.4).

2.1.2.1. Блок «Защищенность»

Блок «Защищенность» отображает результаты выполнения проверок на выбранном устройстве (рис. 4).

Для группы устройств блок «Защищенность» на вкладке отсутствует.

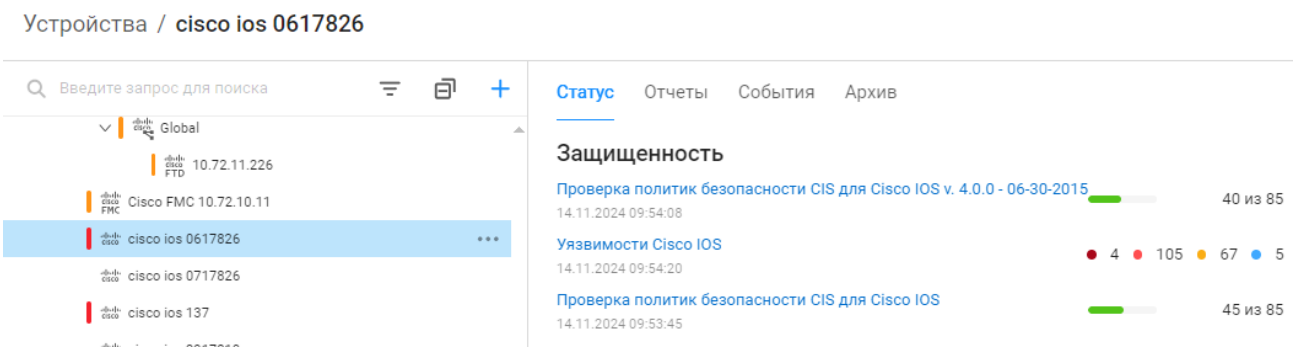


Рисунок 4 – Блок «Защищенность»

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

Результат выполнения проверок на наличие уязвимостей представлен в виде количества уязвимостей, найденных при выполнении проверки, по уровню критичности:

- «●» – критический;
- «●» – высокий;
- «●» – средний;
- «●» – низкий.

При отображении результатов проверки на наличие уязвимостей используется следующий принцип подсчета количества устройств по типам уязвимостей:

- устройство добавляется в число устройств с критическим уровнем выявленных уязвимостей, если при его проверке обнаружена хоть одна уязвимость с критическим уровнем;
- устройство добавляется в число устройств с высоким уровнем критичности выявленных уязвимостей, если при его проверке не обнаружено уязвимостей с критическим уровнем, а выявлена хоть одна уязвимость с высоким уровнем критичности;
- устройство добавляется в число устройств со средним уровнем критичности выявленных уязвимостей, если при его проверке не обнаружено уязвимостей с критическим или высоким уровнем, а выявлена хоть одна уязвимость со средним уровнем критичности;
- устройство добавляется в число устройств с низким уровнем критичности выявленных уязвимостей, если при его проверке не обнаружено уязвимостей с критическим, высоким или средним уровнем, а выявлена хоть одна уязвимость с низким уровнем критичности.

2.1.2.2. Блок «Уведомления»

Блок «Уведомления» отображает уведомления о произошедших событиях контроля устройства и об ошибках выполнения заданий, заданных на устройстве (рис. 5).

Уведомление содержит:

- заголовок – наименование уведомления;
- дату и время отправки уведомления;
- текст уведомления.

Слева от уведомления расположена полоса, цвет которой соответствует уровню критичности уведомления:

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

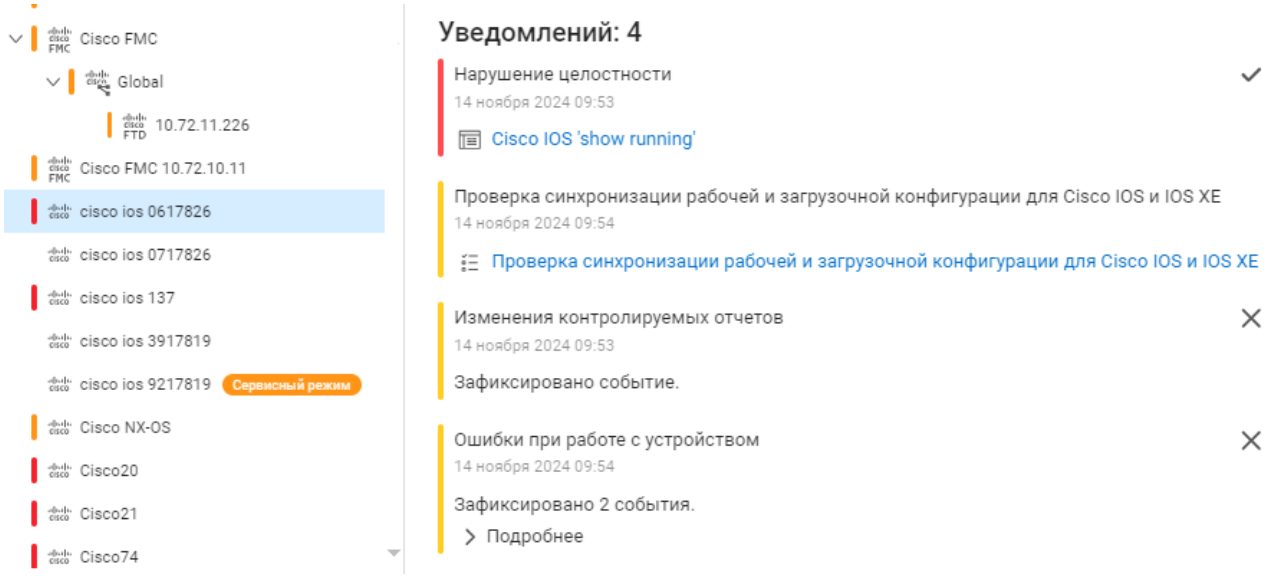


Рисунок 5 – Блок «Уведомления»

Существуют следующие типы уведомлений:

— уведомление по триггеру:
  - «Выполнение конфигурирования и восстановления»;
  - «Ошибка при работе с устройством» и др.

Названия уведомлений по триггеру указываются при включении обработчика событий.

— нарушение контроля целостности:
  - «Нарушение целостности» (текущий отчёт отличается от эталона);
  - «Ранее было зафиксировано нарушение целостности» (текущий отчёт не отличается от эталона, при этом нарушение было зафиксировано ранее).
— нарушение результата проверки:
  - «Проверка синхронизации рабочей и загрузочной конфигурации»;
  - «Рабочая и сохраненная конфигурации не синхронизированы».
— ошибка настройки проверки доступности:
  - «Ошибка настройки опроса по ICMP».

Быстрые действия с уведомлениями:

— «Удалить уведомление» (✕) для удаления соответствующего уведомления;

— «Принять новую версию за эталон» (✓) для принятия новой версии загруженного отчета за эталон;

— «Отключить проверку доступности» для выключения проверки доступности устройства по ICMP;

— «Переход к просмотру нарушений» – для перехода в окно сравнения текущего

отчета с эталоном с возможностью принятия текущего отчета за эталон;
— «Переход к отчету» – для перехода в окно просмотра отчета.

2.1.2.3. Блок «Информация об устройстве»

Блок «Информация об устройстве» (рис. 6) содержит следующую информацию:

— иконка производителя;
— название устройства;
— IP-адрес устройства;
— текущий статус устройства:
  - недоступен (серый круг рядом с IP-адресом устройства) – устройство не доступно (более подробно описано в подразделе 2.7);
  - активен (зеленый круг рядом с IP-адресом устройства) – устройство доступно (более подробно описано в подразделе 2.7).
— профиль отчетов;
— модель устройства;
— версия установленного на устройстве программного обеспечения, если оно есть у устройства;
— серийный номер (при наличии);
— расписания, если они настроены для устройства;
— последняя операция, выполненная с устройством.

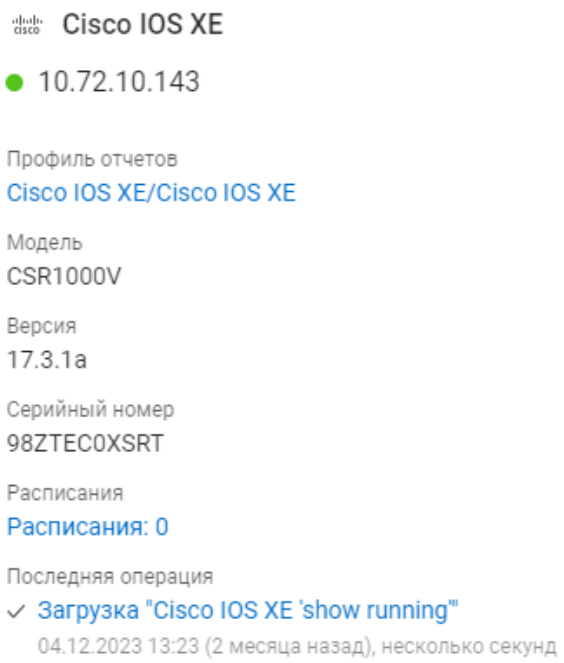


Рисунок 6 – Блок «Информация об устройстве»

Поле «Профиль отчетов» является ссылкой на подраздел «Профили отчетов» (более подробно описано в подпункте 2.3.3.2).

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

Поле «Последняя операция» содержит информацию о результатах выполнения последней операции с устройством с указанием наименования выполненной операции, даты, времени и длительности выполнения операции. Наименование операции является ссылкой, при выборе которой открывается окно с отчетом о выполнении операции.

2.1.2.4. Блок «Операции»

Блок «Операции» (рис. 7) содержит перечень основных операций, которые доступны для выполнения на выбранном устройстве. Перечень операций отличается в зависимости от типа устройства. Возможны следующие типы операций:

- «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.

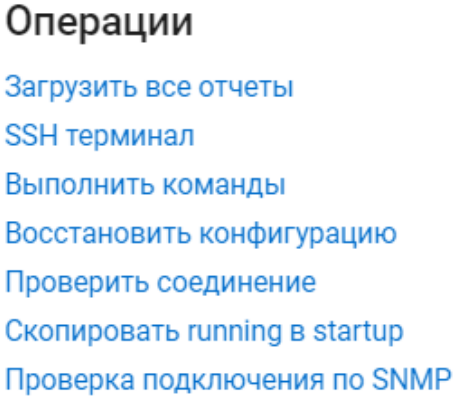


Рисунок 7 – Блок «Операции»

2.1.2.5. Конфигурирование устройства

Вкладка «Статус» страницы «Устройства» содержит блок «Операции», в котором доступен перечень операций для выполнения на выбранном устройстве (см. подпункт 2.1.2.4, рис. 7).

Операции изменения и восстановления конфигурации устройств доступны только после подключения сервисного модуля «Управление устройствами» и только для устройств, поддерживающих возможность выполнения этих операций. Для включения модуля необходимо перейти в раздел «Настройки», подраздел «Модули», вкладка «Сервисные». Перевести переключатель «Состояние» в строке модуля в положение активен « ». Более подробно см. документ «Руководство пользователя. Часть 1. Настройка и администрирование».

Для изменения конфигурации устройства необходимо выполнить следующие действия:

1) В блоке «Операции» нажать на ссылку «Выполнить команды».
2) Откроется окно «Конфигурирование оборудования» (рис. 8).

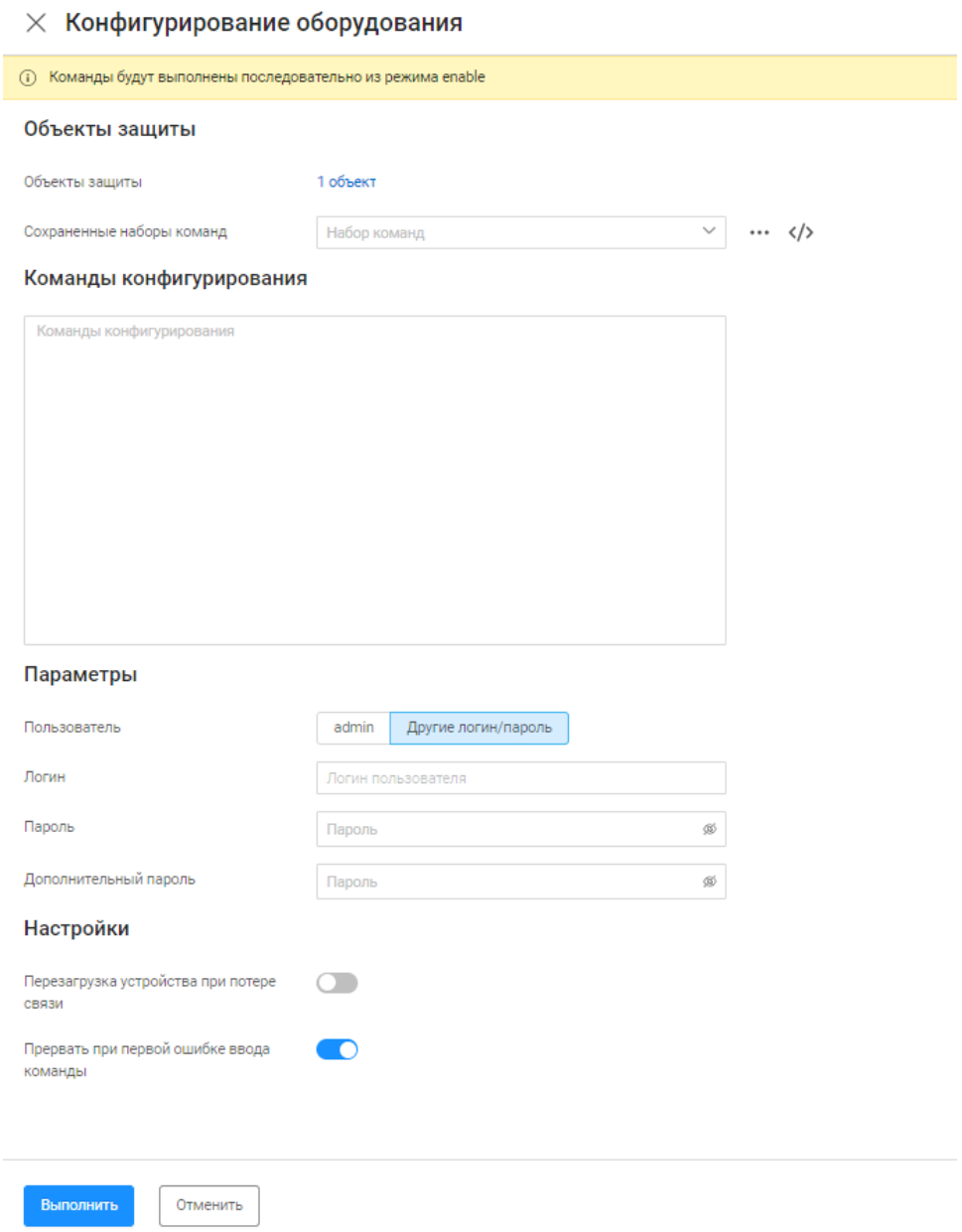


Рисунок 8 – Окно «Конфигурирование оборудования»

3) В поле «Объекты защиты» выбрать при необходимости дополнительно устройства для изменения конфигурации, для чего:
— нажать ссылку-количество выбранных устройств;
— в открывшемся окне «Выбор объектов» (рис. 9) установить флаг в полях, соответствующих требуемым устройствам;
— нажать кнопку «Выбрать». В поле «Объекты защиты» отобразится количество выбранных устройств.

В окне «Выбор объектов» пользователь может выполнить поиск устройств и фильтрацию списка устройств с использованием поля поиска и окна фильтрации,

которое открывается по нажатию кнопки «Фильтр». При наведении курсора на пиктограммы в колонке «Метки» отображается название метки[1] для соответствующего устройства.

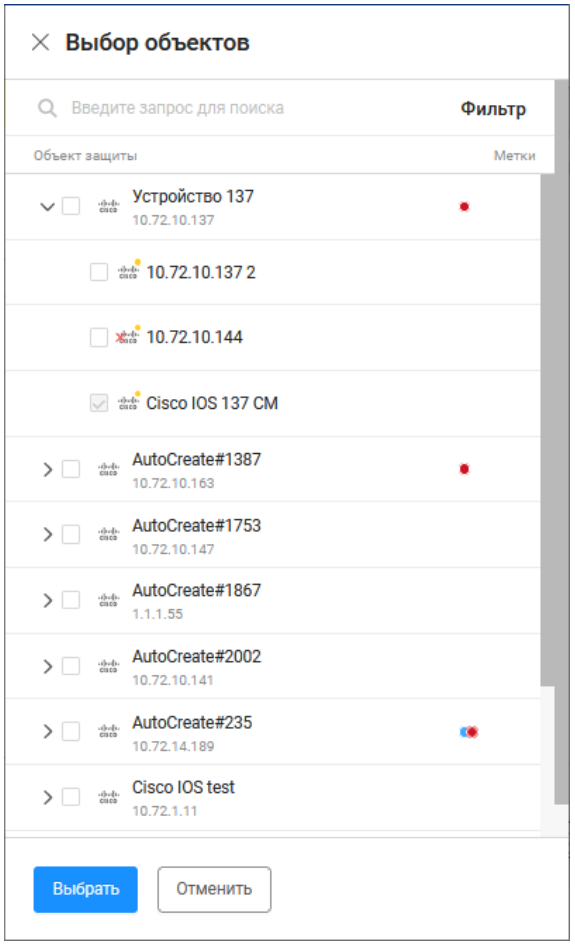


Рисунок 9 – Окно «Выбор объектов»

4) В поле «Сохраненные наборы команд» выбрать из сохраненных список команд конфигурирования или задать в поле «Команды конфигурирования» перечень команд конфигурирования, характерный для типа выбранного устройства. Поддерживается сохранение/изменение/удаление списков команд конфигурирования.
5) В группе полей «Параметры» выбрать тип учетной записи, используя переключатель «Пользователь». При выборе «Другие логин\пароль» – заполнить появившиеся поля «Логин», «Пароль», «Дополнительный пароль».

При выборе «Другие логин\пароль» учетная запись должна быть предварительно заведена на устройстве.

[1] Метки для устройств назначаются в разделе «Объекты защиты» и позволяют пользователю уточнить фильтрацию в дереве устройств

6) В группе переключателей «Настройки» включить требуемые настройки поведения устройства при появлении нештатной ситуации.
7) Нажать кнопку «Выполнить».

В случае необходимости восстановления работоспособности устройства доступна команда по восстановлению загрузочной конфигурации устройства с использованием ранее сохраненной настройки конфигурации.

Для восстановления конфигурации устройства необходимо выполнить следующие действия:

1) В блоке «Операции» нажать на ссылку «Восстановить конфигурацию».
2) В окне «Восстановление конфигурации» установкой переключателя выбрать сохраненную ранее конфигурацию (рис. 10).

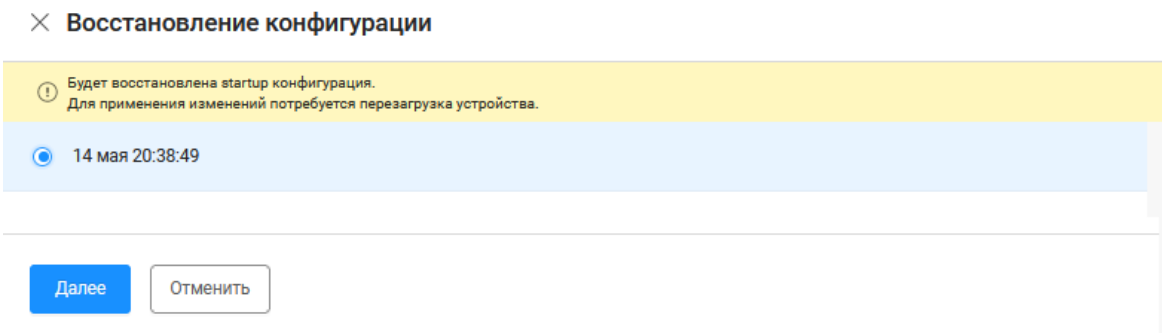


Рисунок 10 – Окно «Восстановление конфигурации»

3) Нажать кнопку «Далее».
4) Чтобы посмотреть выбранную для восстановления конфигурацию необходимо нажать кнопку «Показать отличия» (рис. 11). Состав и описание полей окна «Подтверждение восстановления конфигурации» приведены в таблице 3.

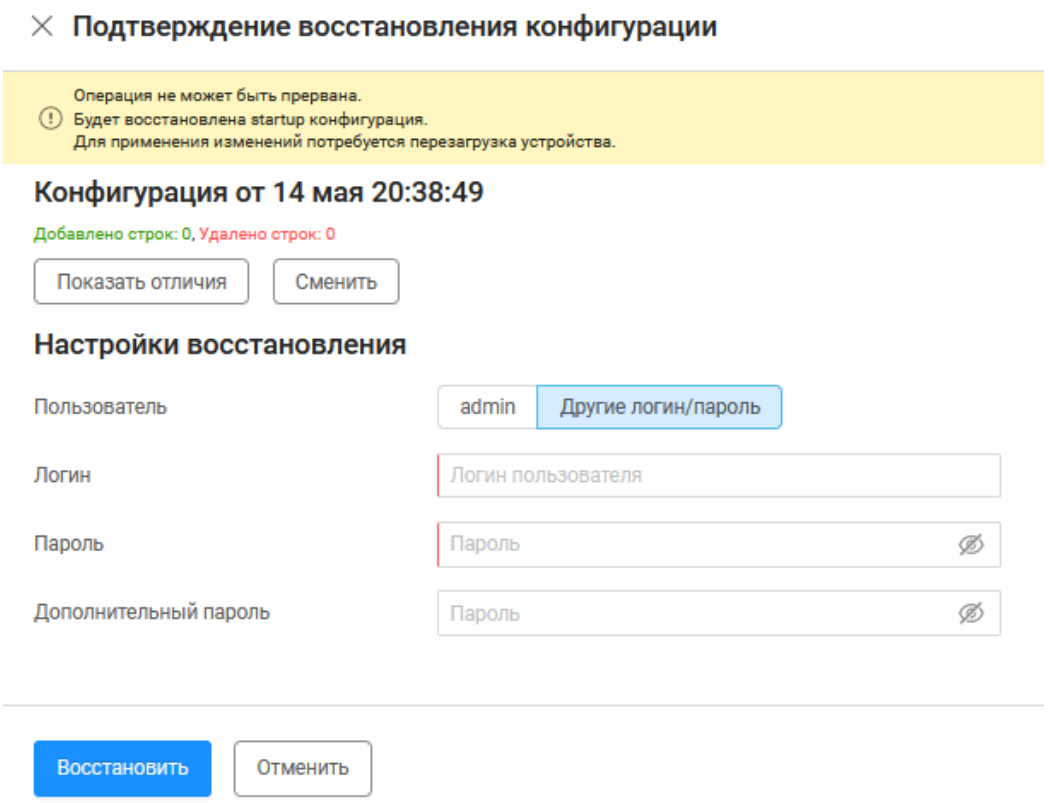


Рисунок 11 – Окно «Подтверждение восстановления конфигурации»

Таблица 3 – Состав и описание полей окна «Подтверждение восстановления конфигурации»

Поле	Описание
Поле «Информационный блок»	Информация о выбранной конфигурации (дата и время), количество добавленных и удаленных строк
Кнопка «Показать отличия»	При нажатии отображается окно с различиями в конфигурациях устройства
Кнопка «Сменить»	При нажатии происходит возвращение в окно выбора конфигурации для восстановления
Группа полей «Настройки восстановления»	
Поле «Пользователь»	Поле выбора пользователя: — «admin» – пользователь, указанный при заведении устройства в комплекс; — «Другой пользователь» – пользователь, который создан на устройстве
Поле «Логин»	Логин пользователя, работающего с устройством. Форматы ввода: — логин;

Поле	Описание
	— домен\логин; — логин@домен (в формате UPN)
Поле «Пароль»	Пароль пользователя, работающего с устройством
Поле «Дополнительный пароль»	Дополнительный пароль для привилегированного режима

5) На открывшейся странице можно сравнить архивную версию отчета, выбранного для восстановления конфигурации, и текущую версию конфигурации (рис. 12).
6) Вернуться в окно «Подтверждение восстановления конфигурации» и нажать кнопку «Восстановить».

В результате произойдет обновление конфигурации выбранного устройства.

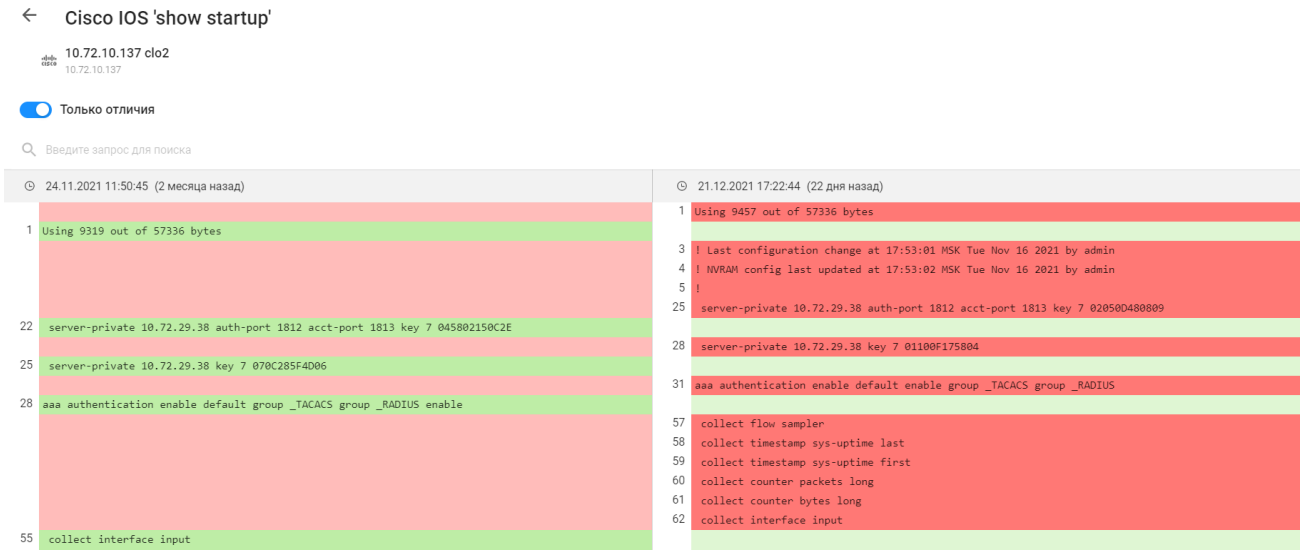


Рисунок 12 – Страница «Сравнение отчетов»

2.1.3. Вкладка «Статус» для группы устройств

Вкладка «Статус» (рис. 13) содержит сведения, относящиеся к группе устройств, выделенной в дереве устройств, и разделена на блоки:

— «Уведомления» (см. подпункт 2.1.3.1);
— «Проверки безопасности» (см. подпункт 2.1.3.2);
— «Уязвимые устройства» (см. подпункт 2.1.3.3);
— «Доступность устройств» (см. подпункт 2.1.3.4);
— «Операции» (см. подпункт 2.1.2.4).

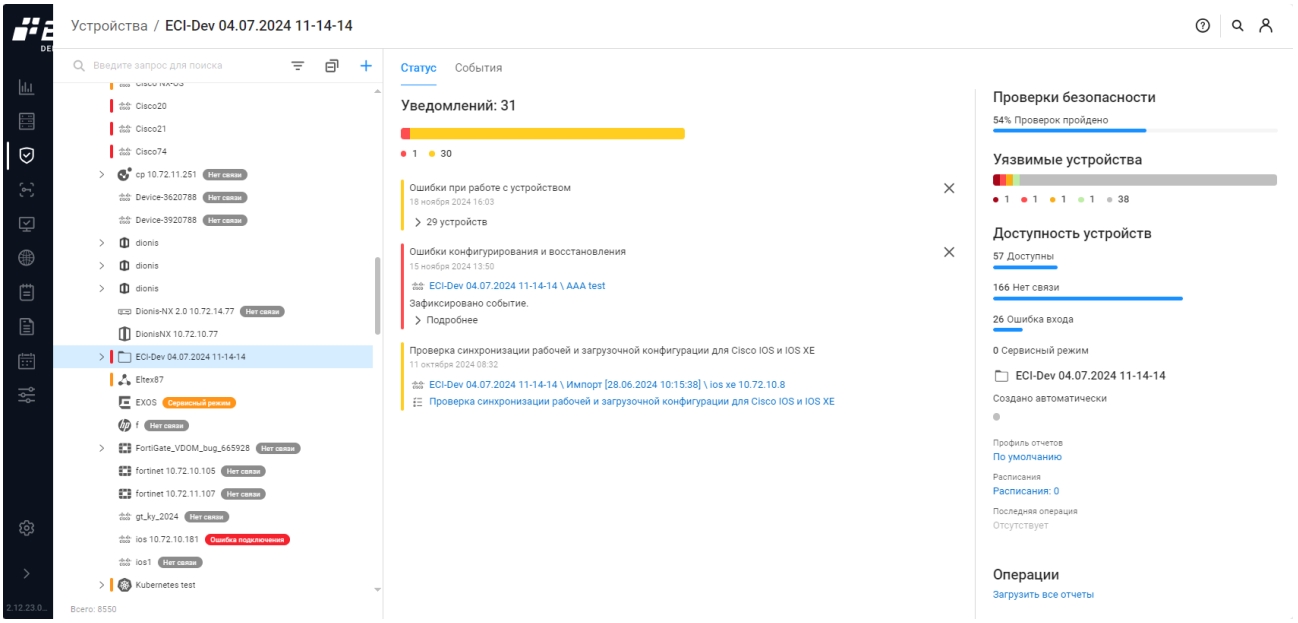


Рисунок 13 – Вкладка «Статус» для группы устройств

2.1.3.1. Блок «Уведомления»

Блок «Уведомления» отображает уведомления о произошедших событиях контроля группы устройств и об ошибках выполнения заданий, заданных для устройств в группе устройств (рис. 14).

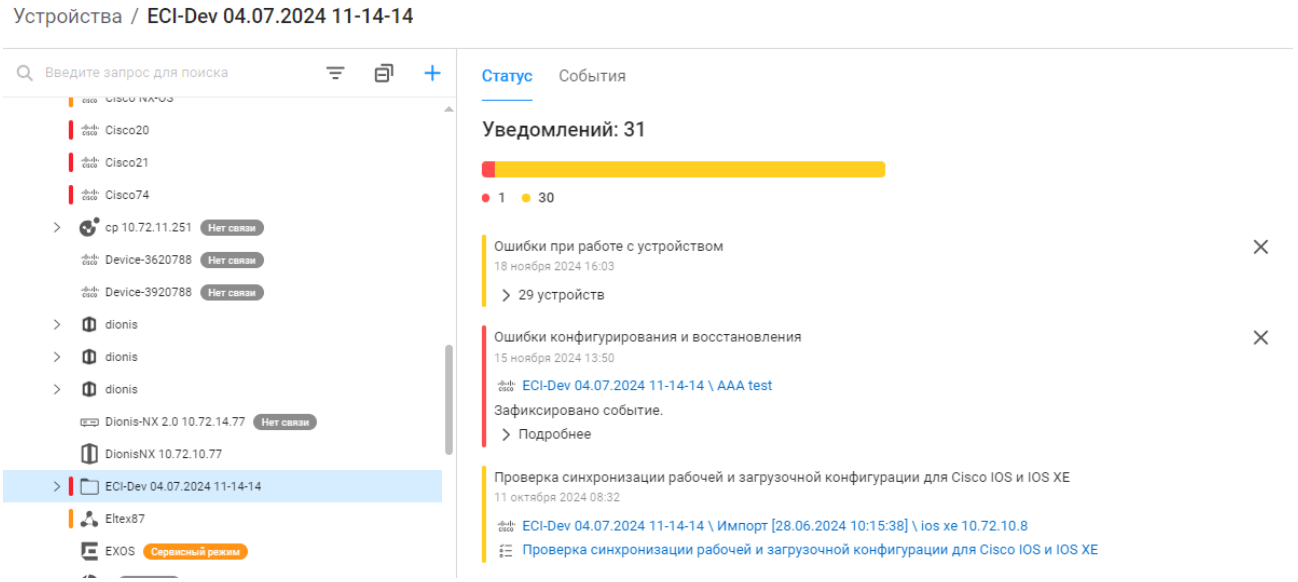


Рисунок 14 – Блок «Уведомления» для группы устройств

Состав отображаемых данных в уведомлениях для группы устройств аналогичен составу данных для одного устройства (см. подпункт 2.1.2.2), за исключением того, что в уведомлении для группы доступен для просмотра список устройств, с которыми оно связано.

2.1.3.2. Блок «Проверки безопасности»

Блок «Проверки безопасности» отображает результаты выполнения проверок выбранной группы устройств (рис. 15).

Рисунок 15 – Блок «Проверки безопасности»

Результат выполнения проверок безопасности представлен в виде процента положительно выполненных правил, содержащихся в проверке группы устройств.

2.1.3.3. Блок «Уязвимые устройства»

Блок «Уязвимые устройства» содержит информацию о количестве уязвимых устройств в группе и степени их уязвимости (рис. 16).

Рисунок 16 – Блок «Уязвимые устройства»

Результат выполнения проверок на наличие уязвимостей представлен в виде количества уязвимостей, найденных при выполнении проверки, по уровню критичности:

- «●» – при проверке обнаружена хоть одна уязвимость с критичным уровнем;
- «●» – при проверке не обнаружено уязвимостей с критичным уровнем, но выявлена хотя бы одна уязвимость с высоким уровнем критичности;
- «●» – при проверке не обнаружено уязвимостей с критичным или высоким уровнем, но выявлена хотя бы одна уязвимость со средним уровнем критичности;
- «●» – при проверке не обнаружено уязвимостей с критичным, высоким или средним уровнем, но выявлена хотя бы одна уязвимость с низким уровнем;
- «●» – при проверке не обнаружено уязвимостей;
- «●» «Данные отсутствуют» – проверки не производились.

2.1.3.4. Блок «Доступность устройств»

Блок «Доступность устройств» (рис. 17) содержит графическое представление информации о статусах контролируемых устройств, которые входят в выделенную группу.

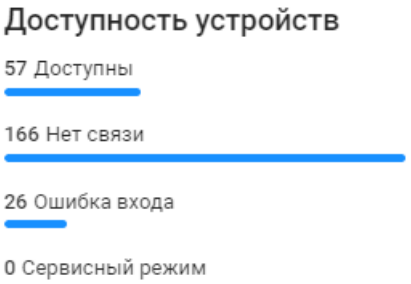


Рисунок 17 – Блок «Доступность устройств» для группы устройств

В блоке приводятся сведения о количестве устройств выделенной группы для каждого из возможных состояний в ПК «Efros DO»:

- «Доступны» – последняя операция с устройством, входящим в выделенную группу, выполнена успешно;
- «Нет связи» – последняя операция с устройством (загрузка отчетов, проверка связи и др.), входящим в выделенную группу, завершилась ошибкой;
- «Ошибка входа» – при выполнении операции с устройством (загрузка отчетов, проверка связи и др.), входящим в выделенную группу, произошла ошибка аутентификации;
- «Сервисный режим» – устройство не опрашивается по заданному расписанию и не проверяется в автоматическом режиме его доступность, обновление данных выполняется только по запросу пользователя.

2.1.4. Вкладка «Отчеты»

Вкладка «Отчеты» (рис. 18) содержит список отчетов, разрешенных для загрузки с выбранного устройства и содержащих значения параметров контролируемого устройства. На вкладке список отчетов группируется по двум типам: «Конфигурации» и «Проверки».

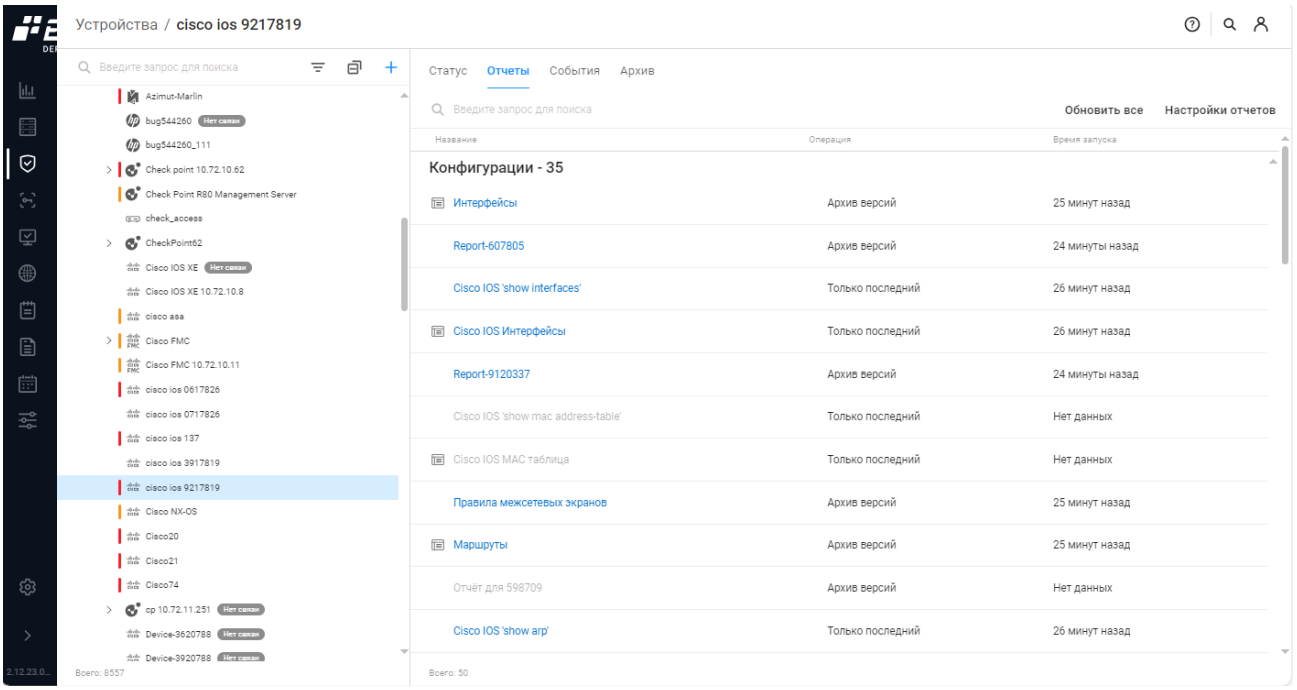


Рисунок 18 – Вкладка «Отчеты»

Каждый тип отчета представлен в виде раскрывающегося списка. Для каждой записи списка отображаются следующие данные:

- пиктограммы отчетов типа «Конфигурации», например:
  - текстовый «»;
  - структурированный «»;
  - пользовательский отчет « »;
  - отчет типа «Фильтр» « », созданный на основе другого отчета путем фильтрации данных;
  - отчет «Правила межсетевых экранов» « »;
  - правила NAT « »;
  - отчет «Объекты межсетевых экранов» « »;
- пиктограммы отчетов типа «Проверки», например:
  - пользовательская проверка « »;
  - стандартная проверка « »;
  - зонный анализ « »;
  - проверка на уязвимости « »;
  - оптимизация правил « »;
- название – является ссылкой, при переходе открывается окно для просмотра отчета;
- операции – для отчетов типа «Конфигурации» содержит назначенный для отчета вариант его использования (см. таблицу 4), для отчетов типа «Проверки» в зависимости от их типа:

- 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;
- 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;

— время запуска – время, прошедшее с момента загрузки последней версии отчета.

Таблица 4 – Варианты использования отчетов типа «Конфигурации» для устройства

Варианты использования	Описание
«Архив версий»	В БД комплекса хранятся все измененные версии отчета, загруженные с устройства
«Контроль изменений»	При загрузке отчета выполняется контроль целостности загружаемых версий и их сравнение с эталоном. 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 с возможностью принять текущую версию за эталон; — в БД комплекса будут храниться все измененные версии отчета в виде архива
«Только последний»	в БД комплекса хранится только последняя измененная версия отчета, загруженного с устройства

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.

В отчетах «Правила межсетевых экранов» и «Правила NAT» отображаются только те правила МЭ, которые влияют на обработку трафика. Состав колонок отчета «Правила

NAT» зависит от типа устройства (от поддерживаемых вендором устройства полям отчета).

Отчеты, запрещенные к загрузке с выбранного устройства, на вкладке «Отчеты» не отображаются, доступны для просмотра и настройки в разделе «Профили отчетов» (см. подраздел 2.4).

Тип отображаемого отчета зависит от установленной лицензии. Отчет, содержащий критическую информацию по устройству, отображается всегда, но только в режиме «Только последний». Данный отчет нельзя сохранить в архив для сравнения.

Над списком отчетов располагаются:

- поле поиска (Введите запрос для поиска);
- кнопка «Обновить все» (Обновить все);
- кнопка «Настройки отчетов» (Настройки отчетов).

При наведении курсора на строку с отчетом появляются кнопки:

- «Обновить» ( ) – позволяет обновить выбранную версию отчета;
- «Настройки» ( ) – позволяет настроить использование отчета (более подробно см. подпункт 2.1.4.2).

2.1.4.1. Просмотр отчета

Для просмотра отчета необходимо выбрать наименование требуемого отчета. В результате откроется форма просмотра отчета. На рис. 19 приведена страница с текстовой формой отчета.

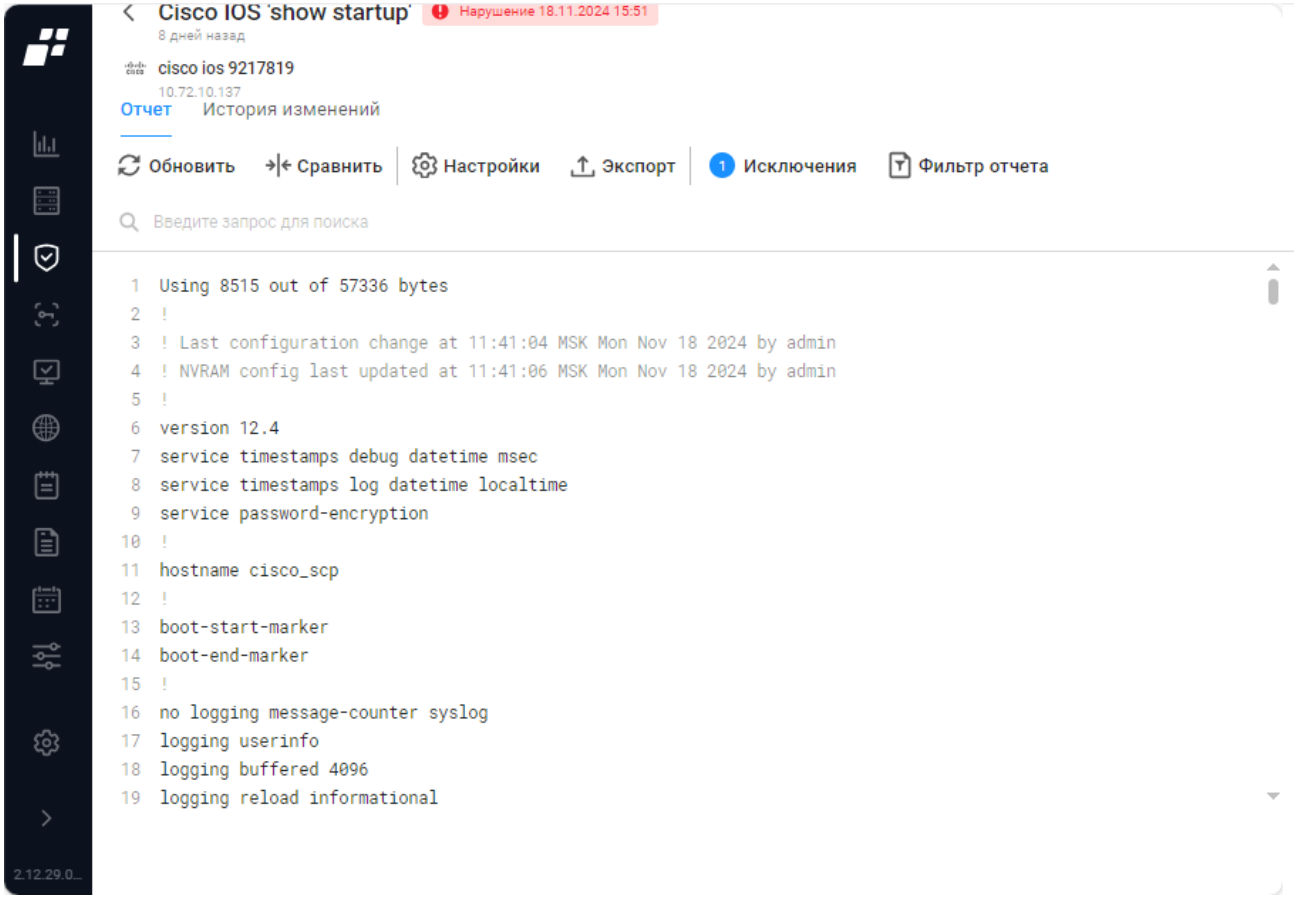


Рисунок 19 – Страница текстовой формы отчета

Страница содержит вкладки «Отчет» и «История изменений».

На вкладке «Отчет» в зависимости от типа отчета могут быть доступны следующие функции:

- кнопка «Обновить» (**Обновить**) позволяет обновить версию отчета;
- кнопка «Сравнить» (**Сравнить**) позволяет сравнить ранее загруженные на сервер ПК «Efros DO» версии этого отчета;
- кнопка «Настройки» (**Настройки**) позволяет настроить использование отчета;
- кнопка «Экспорт» (**Экспорт**) позволяет выгрузить отчет на рабочую машину;
- кнопка «Исключения» (**Исключения**) позволяет установить правила игнорирования изменений параметров устройства в загружаемом отчете в ПК «Efros DO». После добавления исключений в пиктограмме кнопки отображается количество исключений (2 **Исключения**);
- 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.

Для просмотра изменений необходимо перейти на вкладку «История изменений». Вкладка содержит список изменений отчета, изменения сгруппированы по дате и времени их внесения. По умолчанию список свернут, на рис. 20 приведен пример вкладки «История изменений» с раскрытым элементом списка. Изменения, зафиксированные в отчете, выделяются цветом фона или шрифта:

- красным цветом – удаленные и старые значения версии отчета;
- зеленым цветом – добавленные и новые значения версии отчета.

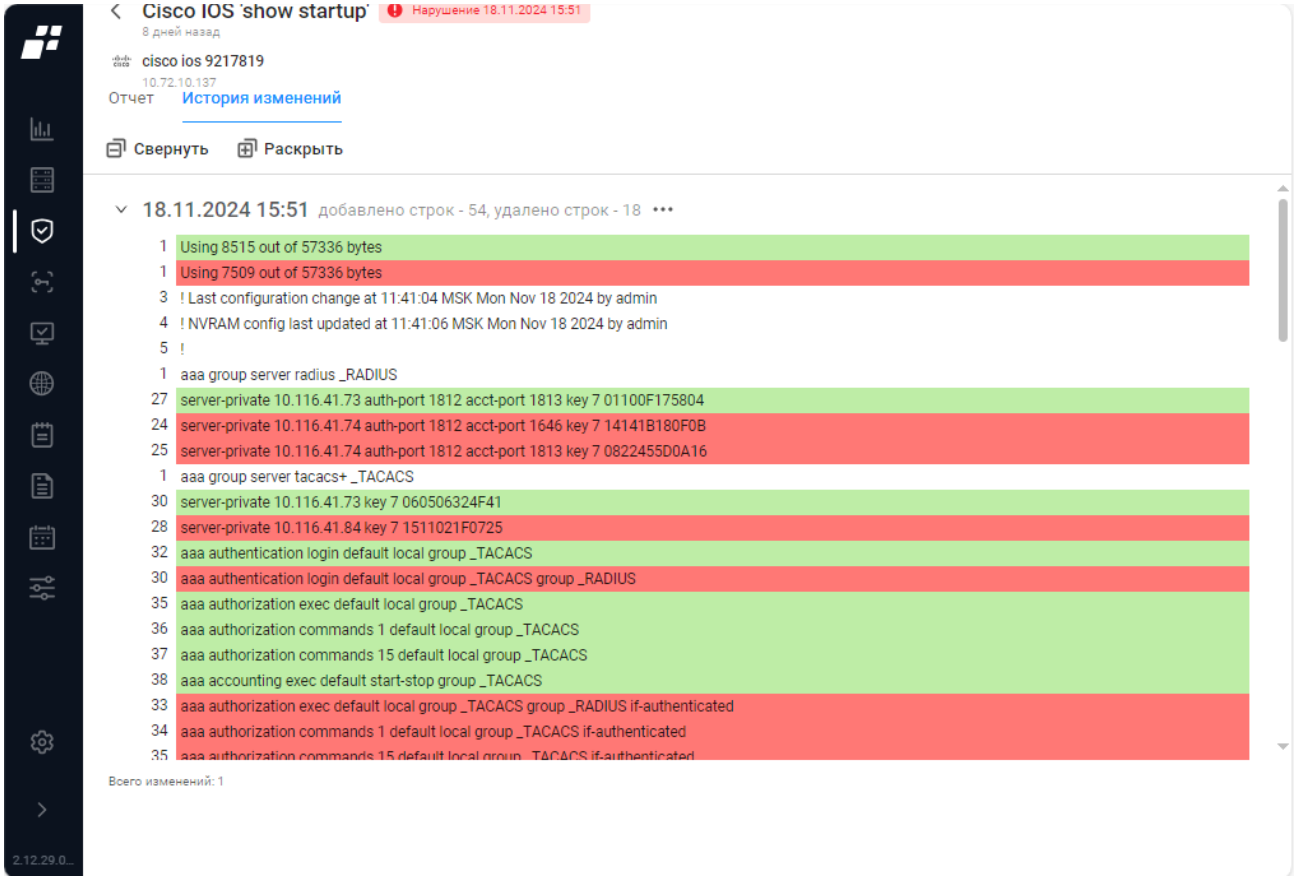


Рисунок 20 – Страница текстовой формы отчета, вкладка «История изменений»

Заголовок каждого измененного отчета содержит дату и время его изменения, обобщенные количественные данные изменений, а также кнопку «•••», по нажатию которой раскрывается панель меню с пунктами:

- «Перейти к отчету» – для перехода к просмотру соответствующего отчета;
- «Сравнить с текущим» – для перехода на страницу сравнения выбранного и текущего отчетов;
- «Добавить комментарий» – для перехода в окно добавления/редактирования комментария к отчету (рис. 21).

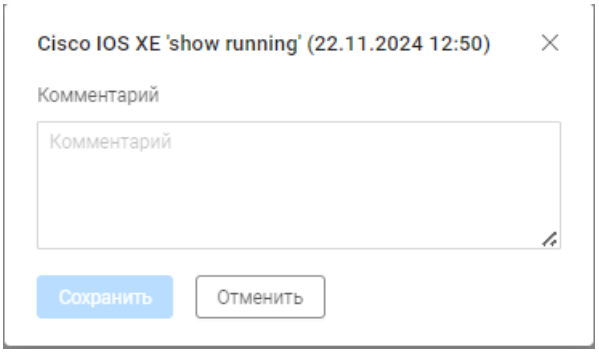


Рисунок 21 – Окно добавления/редактирования комментария к отчету

Над страницей во всех отчетах, кроме отчета «Правила межсетевых экранов» доступны кнопки:

- «Свернуть» (**Свернуть**) – позволяет свернуть отчет;
- «Раскрыть» (**Раскрыть**) – позволяет развернуть отчет в виде дерева.

Особенности форм просмотра различных типов отчетов:

1) Для форм просмотра отчетов типа «Отчет о проверке»:
- в заголовке отчета дополнительно отображается индикатор защищенности устройства;
- во вкладке «Отчет» пользователь, используя переключатель «Только нарушения», может выполнить фильтрацию результатов проверок для просмотра.

2) Для форм просмотра отчетов типа «Отчет о проверке на наличие уязвимостей»:
- в заголовке отчета дополнительно отображаются результаты выполнения проверок на наличие уязвимостей;
- во вкладке «Отчет» пользователь может выполнить переход на различные сайты (при наличии на них описания выявленной уязвимости) с подробным описанием выявленной уязвимости.

Используемые в ПК «Efros DO» графические обозначения уровня критичности уязвимости:

- «» – Критический;
- «» – Высокий;
- «» – Средний;
- «» – Низкий.

- во вкладке «История изменений» отчета пользователь может просмотреть списки новых выявленных и измененных уязвимостей. Уязвимости сгруппированы по датам обновления БДУ и категориям. В заголовке каждой группы отображается дата и время изменения.

3) Для форм просмотра отчетов типа «Оптимизация правил»:
- в заголовке форм просмотра отчетов для устройств, поддерживающих подсчет срабатываний правил, дополнительно отображается количество теневых, избыточных, неиспользуемых, нулевых и устаревших правил МЭ, а также правил МЭ, срок действия которых заканчивается;
- в отчете пользователь может перейти по нажатию в строке правила кнопки «Просмотр» () из отчета по оптимизации в форму просмотра отчета по ACL устройства с позиционированием на соответствующем правиле.

4) Для форм просмотра отчетов типа «Правила межсетевых экранов»:
- пользователь может во вкладке «Отчет» просмотреть список политик устройства и для каждой политики список правил;
- пользователь может настроить состав отображаемых столбцов таблицы правил (по кнопке «  »);
- пользователь может настроить во вкладке «История изменений», используя переключатель «Только отличия», отображение списка правил МЭ, соответствующего выбранной политике;
- если для правила задано расписание его работы, то оно отображается в столбце «Additional»;
- если устройством поддерживается подсчет срабатываний правил, то в столбце «HitCount» отображается количество срабатываний правила;
- в отчетах для некоторых типов устройств под заголовком политики (например, для Check Point и Fortinet) или правила (например, для Cisco ASA), если в него внесены изменения, могут отображаться данные менявшего ACL пользователя и время изменения (данные берутся из последнего syslog, примененного к политике).

5) Для форм просмотра отчетов, созданных пользователями на основе стандартов безопасности МЭ:
- пользователь может во вкладке «Отчет» просмотреть для каждого требования стандарта безопасности соответствующего типу устройства его статус (успешно выполнен или с нарушением), а также обнаруженные по требованию правила МЭ, при этом для требований с нарушением параметры, по которым найдено правило, будут отображены красным цветом шрифта, для успешных требований – зеленым.
- аналогично отчетам типа «Оптимизация правил» пользователь может перейти по нажатию в строке правила кнопки Просмотр () в форму просмотра отчета по ACL устройства с позиционированием на соответствующем правиле.

2.1.4.2. Создание отчета «Фильтр»

Отчет «Фильтр» создается на основе просматриваемого отчета путем фильтрации параметров исходного отчета.

Для создания отчета «Фильтр» необходимо выполнить следующие шаги:

1) Нажать на вкладке «Отчет» страницы просматриваемого отчета (см. рис. 19) кнопку «Фильтр отчета» (Фильтр отчета).
2) Откроется окно задания фильтров для создания отчета. Примеры текстового и структурированного отчетов приведены на рис. 22, 23. Состав полей окна и правила их заполнения приведены в таблице 5.

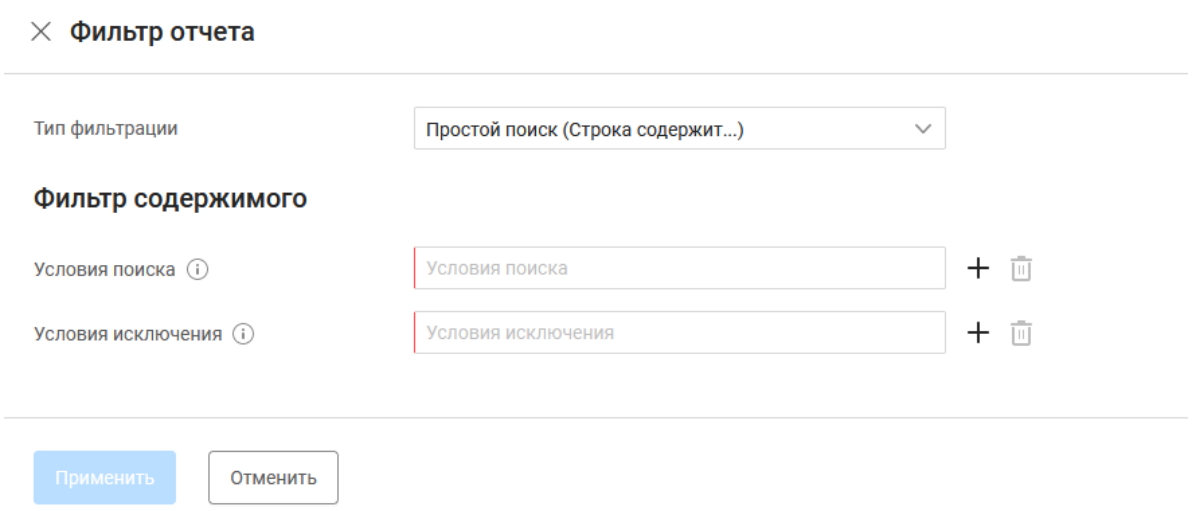


Рисунок 22 – Окно задания фильтров для текстового отчета «Фильтр»

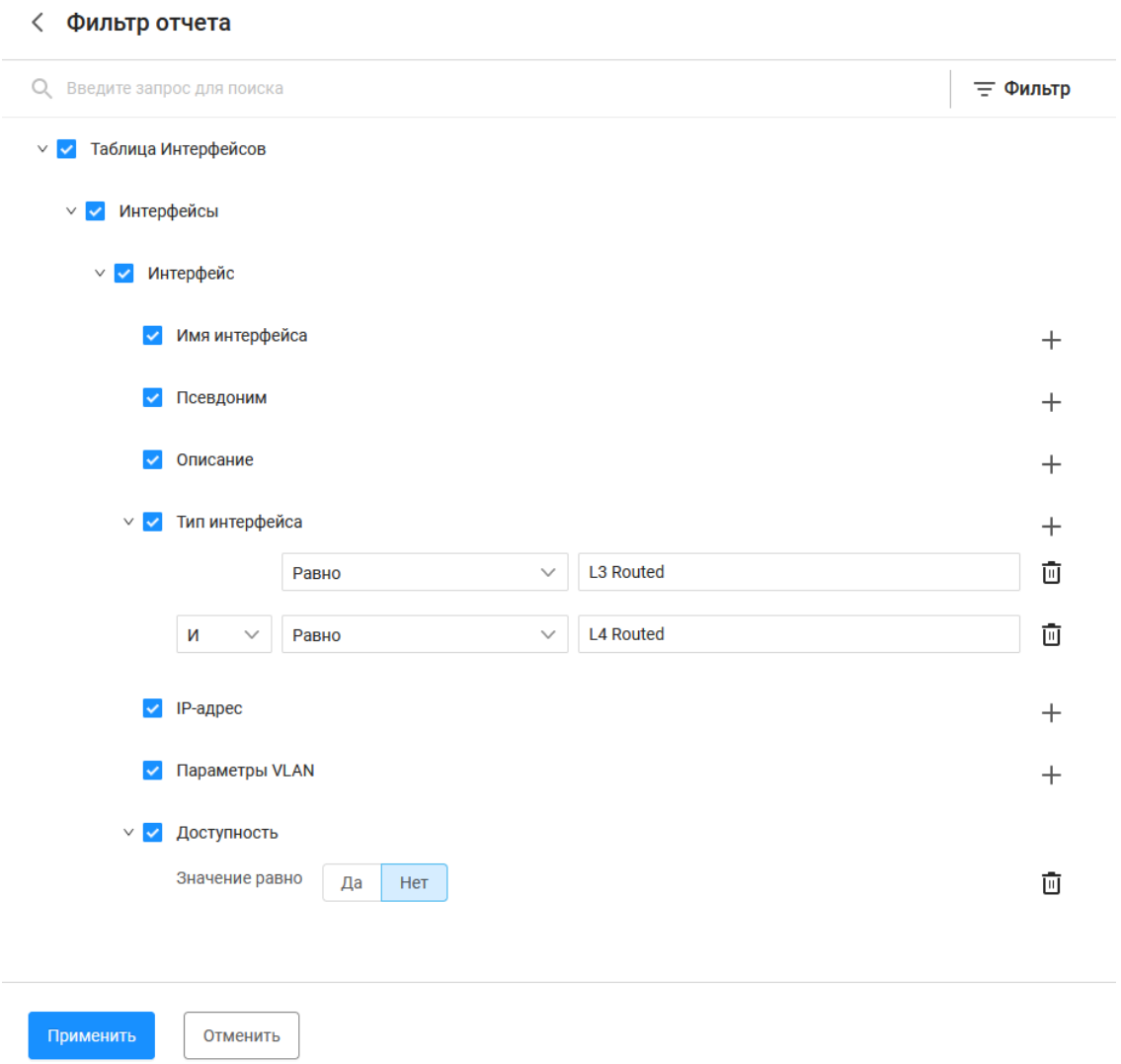


Рисунок 23 – Окно задания фильтров для структурированного отчета «Фильтр»

Таблица 5 – Состав и описание полей окна задания фильтров для отчета «Фильтр»

Поле	Описание
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.

Поле	Описание
	Описание регулярных выражений стандарта PCRE, допустимых к применению в ПК «Efros DO» при задании условий поиска для создания отчета «Фильтр», приведено в приложении Б
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; — «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; — «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

Поле	Описание
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	
Применить	При нажатии кнопки открывается форма просмотра сформированного в соответствии с заданными параметрами отчета
Отменить	При нажатии кнопки окно закрывается без применения введенных данных

3) Для текстового отчета:
— выбрать тип фильтрации;
— задать условия поиска и исключений в соответствии с выбранным типом фильтрации.
4) Для структурированного отчета:
— выбрать установкой флага параметры, включаемые в отчет;
— задать для выбранных параметров условия поиска.
5) Нажать кнопку «Применить». Откроется страница со сформированным отчетом рис. 24.

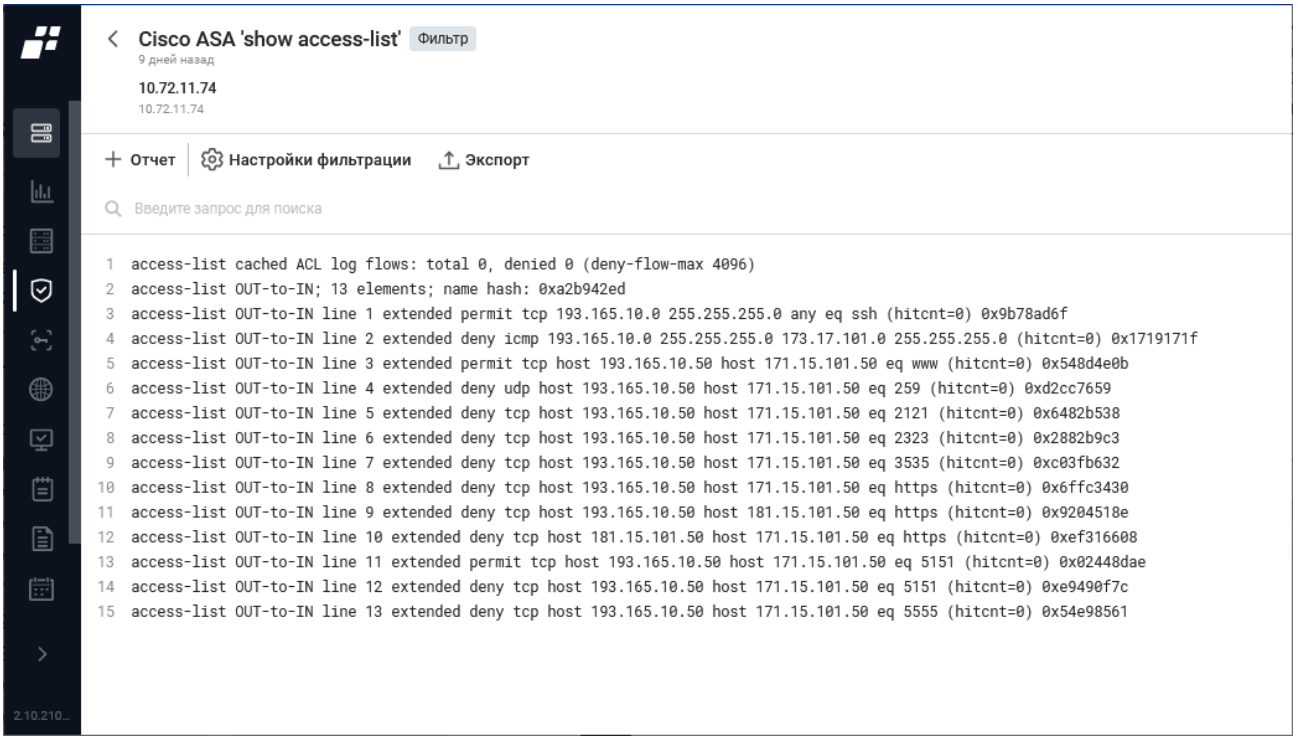


Рисунок 24 – Страница просмотра отчета «Фильтр»

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 созданного отчета «Фильтр», для чего:

— нажать кнопку «Отчет» (**Отчет**);
— в открывшемся окне (рис. 25) ввести имя нового отчета, задать настройки использования отчета:
  - на текущем устройстве или на всех устройствах соответствующего типа;
  - вариант использования (см. таблицу 4):
— 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 (подробнее про профили отчетов см. подраздел 2.4).

Новый отчет доступен для настройки (см. подпункт 2.1.4.3), далее для загрузки с указанных при настройке устройств и просмотра после загрузки на вкладках «Отчеты» и «Архив» в разделе «Устройства».

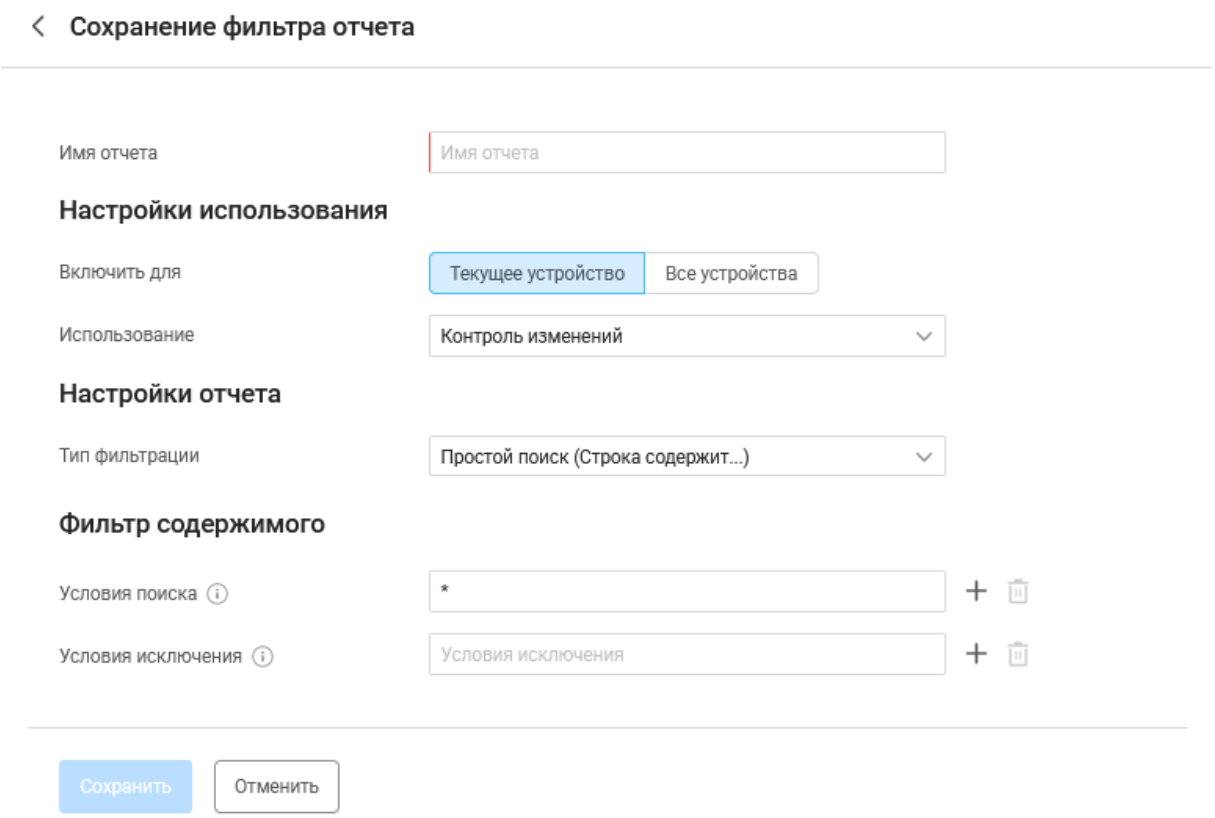


Рисунок 25 – Окно «Сохранение фильтра отчета»

2.1.4.3. Настройка отчета

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

1) Выбрать в дереве устройств требуемое устройство. Перейти на вкладку «Отчеты».
2) На вкладке «Отчеты» (см. рис. 18) выбрать необходимый отчет, установив курсор в строке отчета, нажать кнопку «Настройки» ( ).

В ПК «Efros DO» можно изменять только пользовательские отчеты. Нельзя изменить пользовательский отчет, предназначенный для контроля файлов на устройстве, в параметрах использования которого установлено «Контроль изменений», а последняя загруженная версия отличается от эталона – на вкладке «Статус» устройства есть сообщение о нарушении целостности такого отчета.

3) В открывшемся окне из раскрывающегося списка поля «Использование» выбрать необходимое значение (рис. 26, рис. 27), состав и описание значений полей окна приведены в таблице 6.

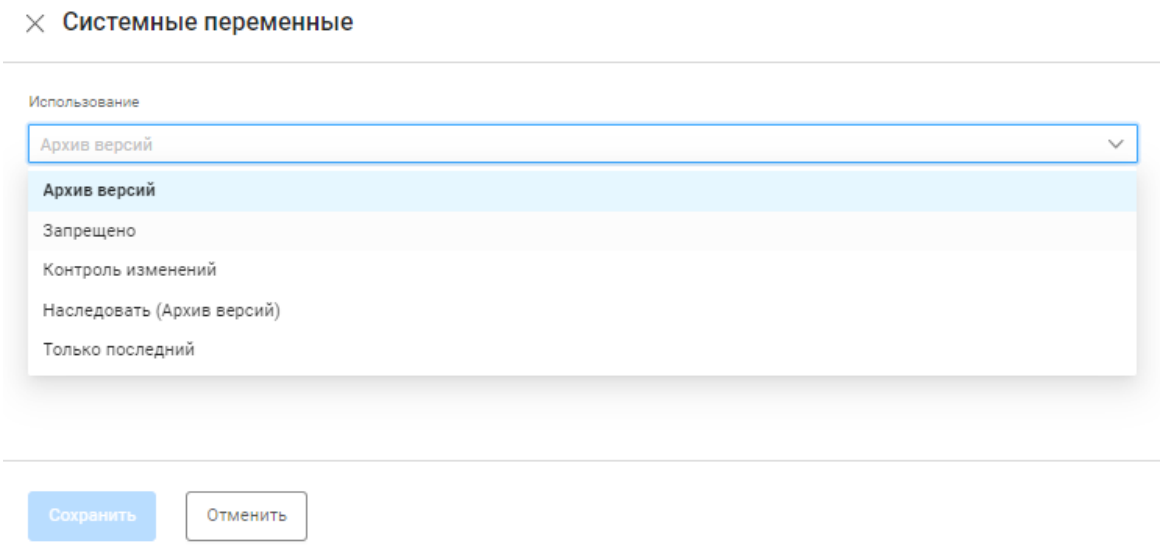


Рисунок 26 – Окно настройки отчета типа «Конфигурации»

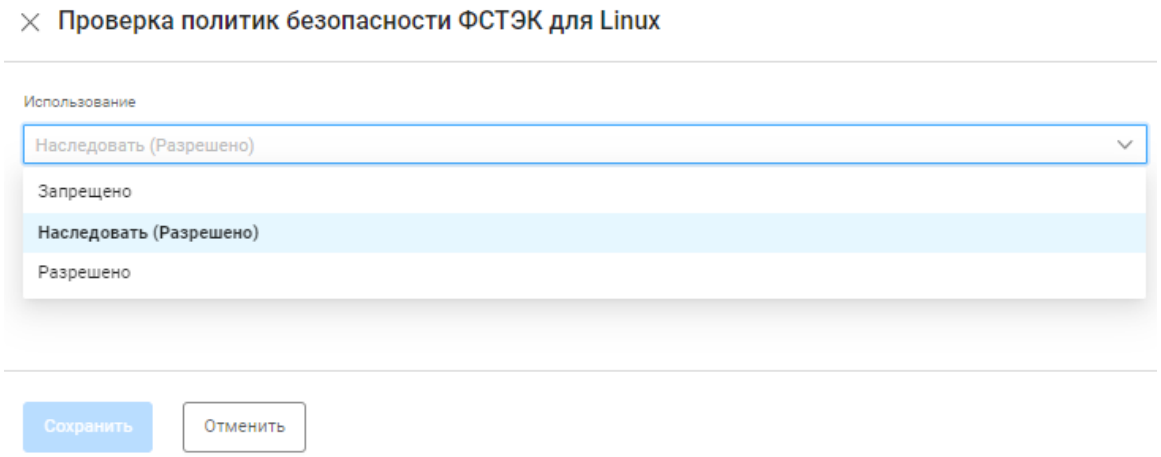


Рисунок 27 – Окно настройки отчета типа «Проверки»

Таблица 6 – Состав и описание полей окон настройки отчета для устройства

Поле	Описание
Поле «Использование» для отчетов типа «Конфигурации»	Выбор режима использования отчета из возможных значений: — «Архив версий» – в БД комплекса будут храниться все измененные версии отчета, загруженные с устройства; — «Запрещено» – загрузка отчета с устройств запрещена вне зависимости от настроек профиля отчетов. Отчет будет скрыт из вкладки «Отчеты»; — «Контроль изменений» – при загрузке отчета будет выполняться контроль целостности загружаемых версий и их сравнение с эталоном; — «Наследовать» – применить настройки профиля отчетов. В скобках отображается значение, установленное в профиле

Поле	Описание
	отчетов; — «Только последний» – в БД комплекса хранится только последняя измененная версия отчета, загруженного с устройства
Поле «Использование» для отчетов типа «Проверки»	Выбор режима использования отчета из возможных значений: — «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

4) Нажать кнопку «Сохранить». Окно настройки отчета закроется, внесенные изменения будут сохранены.

Для настройки всех отчетов одного устройства пользователю необходимо выполнить следующие действия:

1) Выбрать в дереве устройств требуемое устройство. Перейти на вкладку «Отчеты».
2) В заголовке вкладки «Отчеты» (см. рис. 18) нажать кнопку «Настройки отчетов» (Настройки отчетов).
3) Откроется окно настройки отчетов выбранного устройства (рис. 28), где в поле «Профиль устройства» расположен раскрывающийся список всех профилей устройства.
4) На вкладке «Конфигурации» в раскрывающемся списке поля «Использование» выбрать необходимое значение для каждого отчета. Состав и описание значений полей окна приведены в таблице 6.
5) На вкладке «Проверки» в раскрывающемся списке поля «Использование» выбрать требуемое значение варианта использования проверки для выбранного профиля. Состав и описание значений полей окна приведены в таблице 6.
6) В окне настройки отчетов нажать кнопку «Сохранить». Окно настройки отчетов устройства закроется, внесенные изменения будут сохранены.

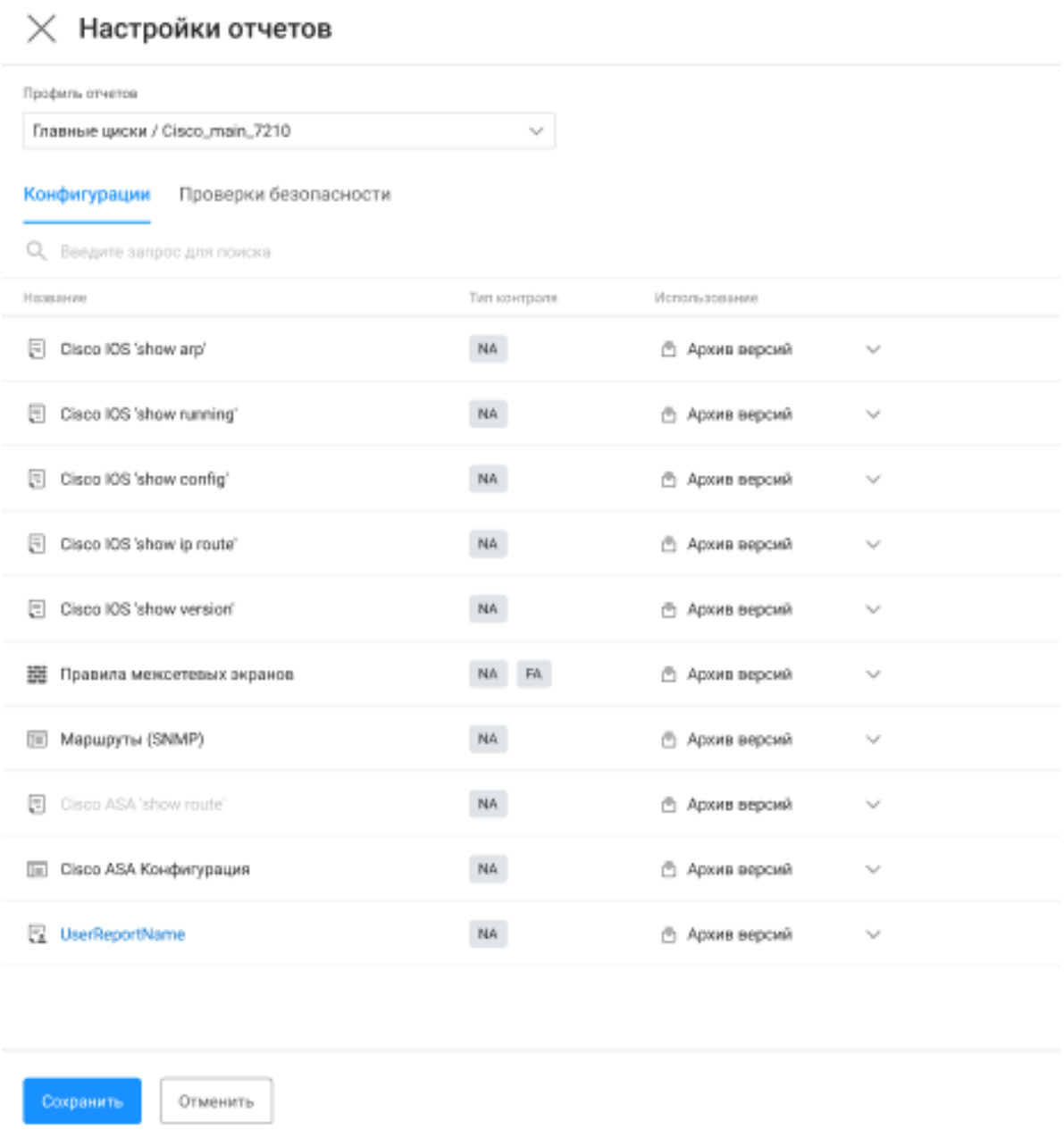


Рисунок 28 – Окно настройки отчетов выбранного устройства, вкладка «Конфигурации»

2.1.5. Вкладка «События»

Вкладка «События» содержит перечень всех событий, произошедших на устройстве/группе устройств (рис. 29).

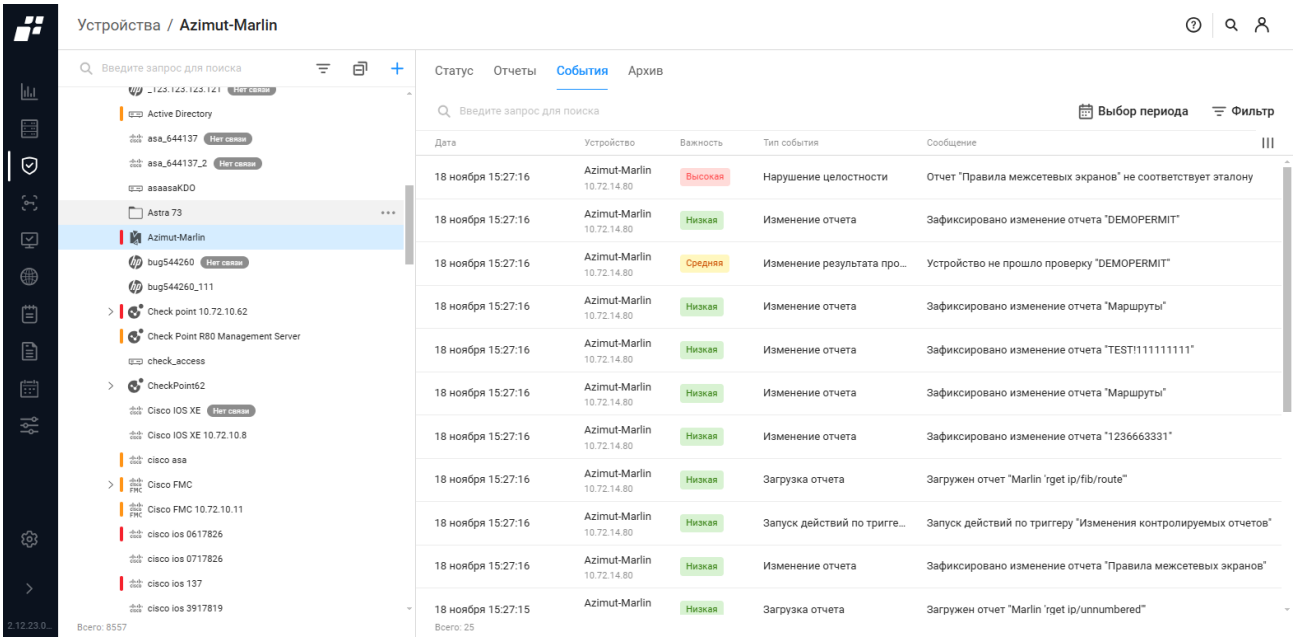


Рисунок 29 – Вкладка «События»

Перечень событий по умолчанию (до подключения внешних модулей), фиксируемых в комплексе:

- аудит;
- восстановление конфигурации;
- выполнение конфигурирования;
- выполнение операции;
- загрузка отчета;
- запуск действий по триггеру;
- запуск задания по расписанию;
- изменение доступности;
- изменение отчета.
- изменение результата проверки;
- контроль целостности компонентов;
- нарушение целостности;
- обновление словаря уязвимостей;
- переключение основного сервера;
- экспорт отчетов;
- ошибка сервера.

К ошибкам сервера могут относиться:

- ошибки выполнения реакций на события (отправка почты/syslog, экспорт

событий);
- ошибки запуска модулей (например, занят порт Syslog-сервера);
- критические ошибки при обработке результата загрузки отчёта или при выполнении операции;
- ошибки при выполнении связанных действий при commit/rollback транзакций;
- другие ошибки, которые могут быть важны пользователю, например, «Переполнение очереди syslog сообщений, часть сообщений пропущена».

На вкладке список событий реализован в виде таблицы. Для каждой записи списка отображаются следующие данные:
- дата – дата фиксации события в числовом формате;
- устройство – содержит название устройства/группы устройств и/или IP-адрес устройства;
- важность – уровень значимости зафиксированного события;
- тип события – тип зафиксированного события;
- сообщение – краткое описание события.

Для отображения на вкладке «События» событий дочерних устройств необходимо открыть окно фильтрации, нажав кнопку «Фильтр», установить флаг в поле «Загружать события дочерних устройств» и нажать кнопку «Применить».

Над списком событий располагаются:
- поле поиска (Введите запрос для поиска);
- кнопка «Выбор периода» (Выбор периода);
- кнопка «Фильтр» (Фильтр);
- кнопка «Колонки» ( ).

2.1.6. Вкладка «Архив»

Вкладка «Архив» содержит список всех загруженных в БД комплекса версий отчетов устройства, для которых установлен режим использования «Архив версий» или «Контроль изменений» (рис. 30).

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

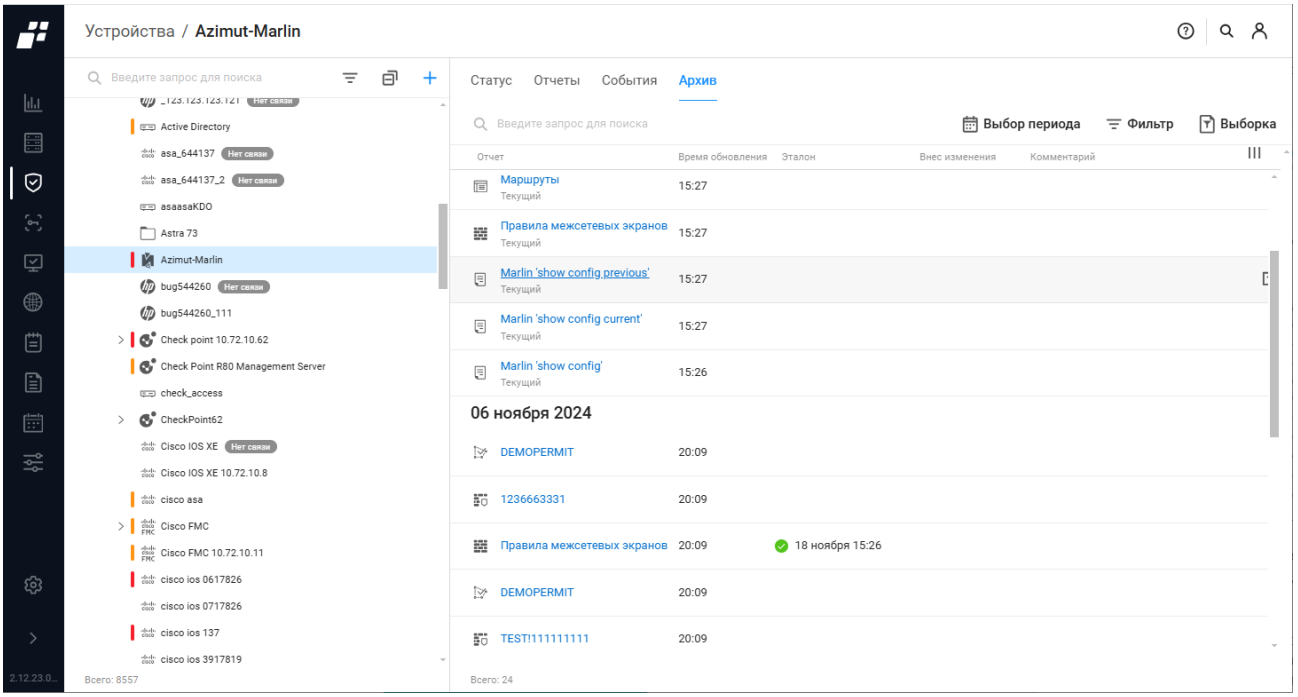


Рисунок 30 – Вкладка «Архив»

На вкладке список архивных отчетов реализован в виде таблицы. Для каждой записи списка отображаются следующие данные:

- отчет – содержит пиктограмму типа отчета и название отчета, название является ссылкой, при нажатии которой открывается окно просмотра отчета;
- время обновления – дата последнего обновления отчета в числовом формате;
- эталон – для эталонных версий отчетов содержит пиктограмму «», дату и время создания эталона, а также логин пользователя, создавшего эталон;
- внес изменения – логин пользователя, внесшего изменения в отчет;
- комментарий – пояснения по отчету.

При наведении курсора на строку любого архивного отчета, в ней отображается кнопка «Комментарий» () для добавления/редактирования комментария к отчету (выполняется аналогично добавлению/редактированию комментария при просмотре текущей версии отчета (подробнее см. п. 2.1.4.1))

Над списком отчетов располагаются:

- поле поиска (Введите запрос для поиска);
- кнопка «Выбор периода» (Выбор периода);
- кнопка «Фильтр» (Фильтр);
- кнопка «Выборка» (Выборка) для просмотра данных по выбранному типу отчёта за выбранный период (см. подпункт 2.1.6.2);
- кнопка «Колонки» ().

2.1.6.1. Просмотр архивной версии отчета

Для просмотра архивной версии отчета необходимо на вкладке «Архив» нажать на выбранный отчет. В результате откроется форма просмотра отчета.

Страница содержит следующие вкладки:

- «Отчет»;
- «История изменений».

На рис. 31 приведена страница просмотра структурированного отчета. На странице доступны:

- кнопка «Сравнить» (Сравнить) для сравнения ранее загруженных на сервер ПК «Efros DO» версий этого отчета;
- кнопка «Настройки» (Настройки) для настройки использование отчета;
- кнопка «Свернуть» (Свернуть) для сворачивания отчета в дерево. Кнопка отображается только для структурированных отчетов;
- кнопка «Раскрыть» (Раскрыть) для раскрытия отчета. Кнопка отображается только для структурированных отчетов;
- кнопка «Комментарий» (Комментарий) позволяет оставить комментарий к отчету (аналогично добавлению/редактированию комментария при просмотре текущей версии отчета (подробнее см. п. 2.1.4.1));
- переключатель «Только нарушения» позволяет включить отображение только нарушений. Кнопка отображается только для структурированных отчетов.

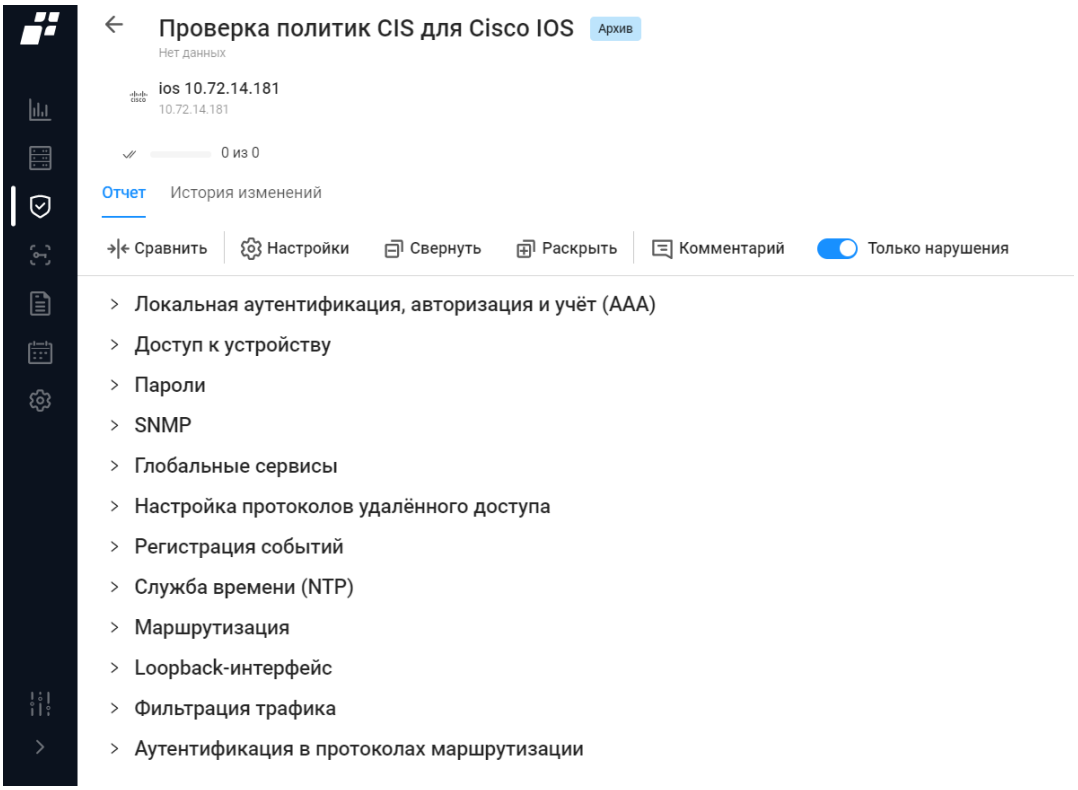


Рисунок 31 – Страница структурированного отчета, вкладка «Отчет»

На рис. 32 приведена страница текстового отчета. На странице доступны:

— кнопка «Сравнить» (Сравнить);
— кнопка «Настройки» (Настройки);
— кнопка «Экспорт» (Экспорт);
— кнопка «Комментарий» (Комментарий).

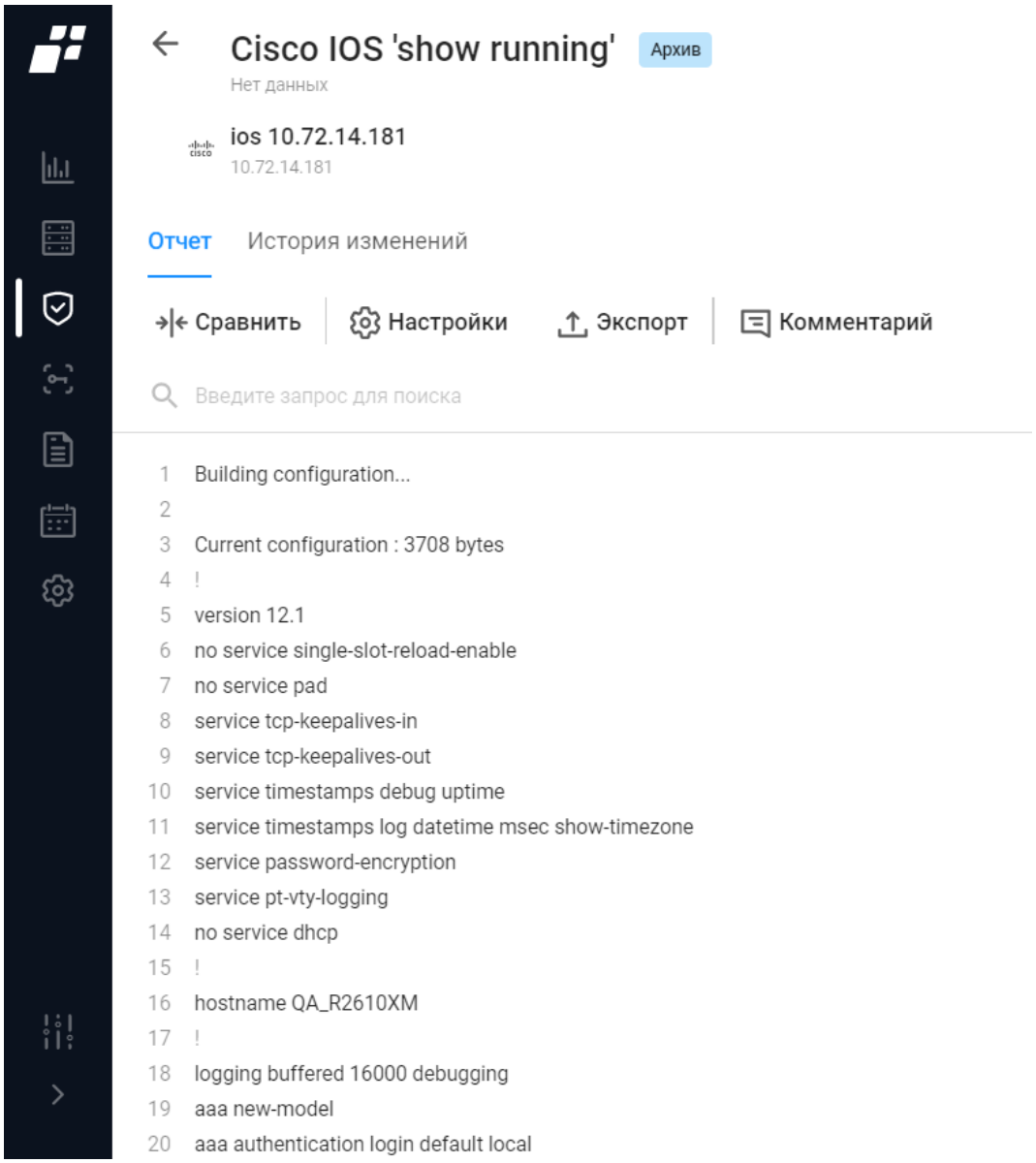


Рисунок 32 – Страница текстовой формы отчета, вкладка «Отчет»

Для просмотра истории изменений архивного отчета необходимо перейти на вкладку «История изменений». На рис. 33 показана вкладка «История изменений» для структурированной формы отчета, на рис. 34 – для текстовой формы отчета.

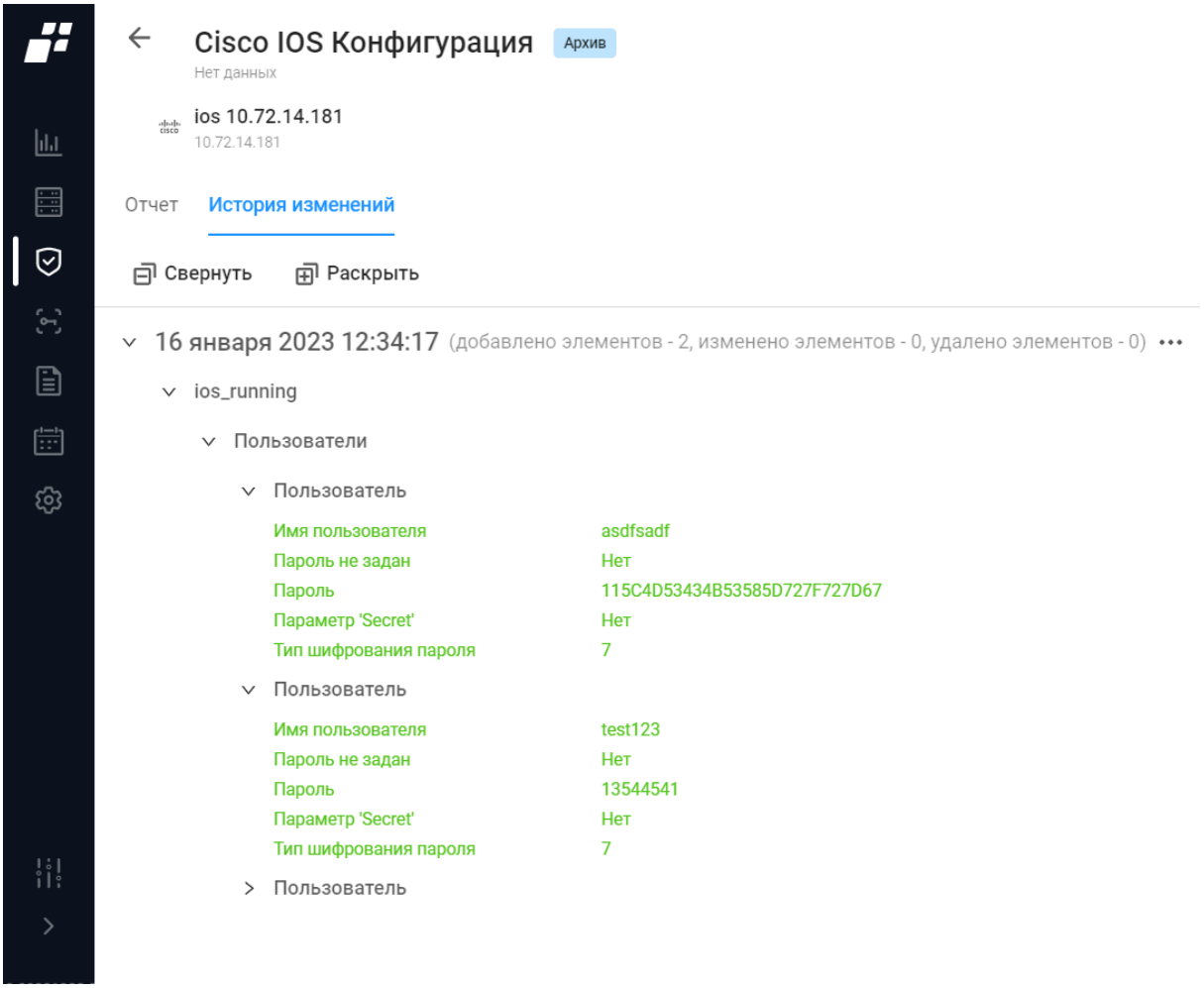


Рисунок 33 – Структурированная форма отчета, вкладка «История изменений»

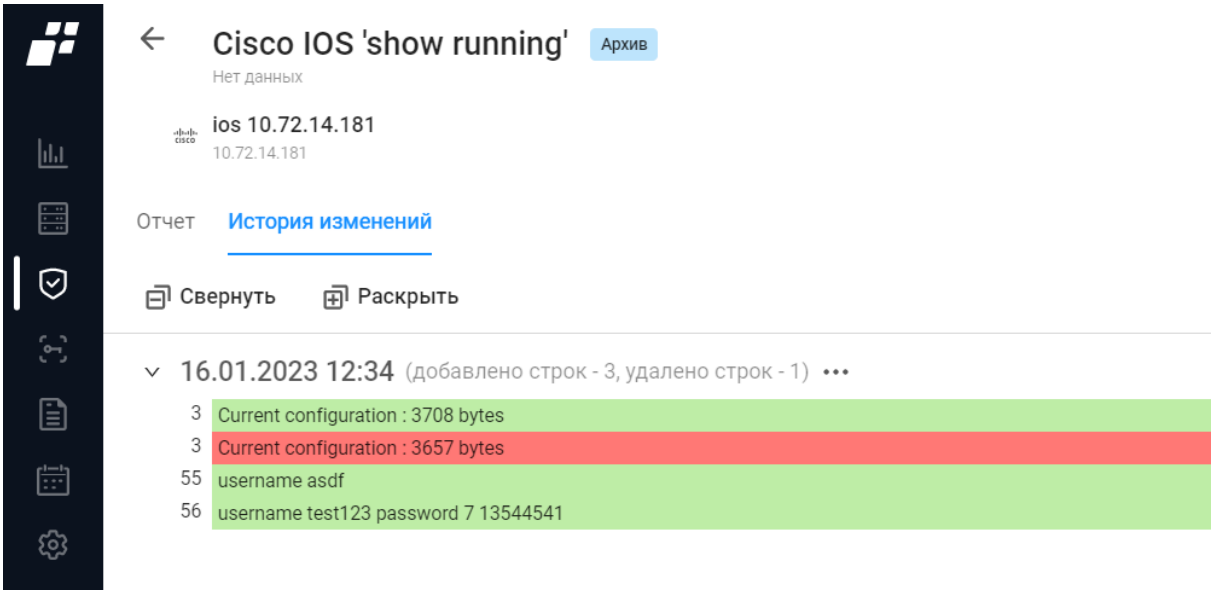


Рисунок 34 – Текстовая форма отчета, вкладка «История изменений»

2.1.6.2. Создание и просмотр выборки данных архивных отчетов

Для создания выборки данных архивных отчетов необходимо выполнить следующие шаги:

1) Нажать на кнопку «Выборка» (Выборка).
2) Откроется страница «Создание отчета (Выборка)», приведенная на рис. 35.

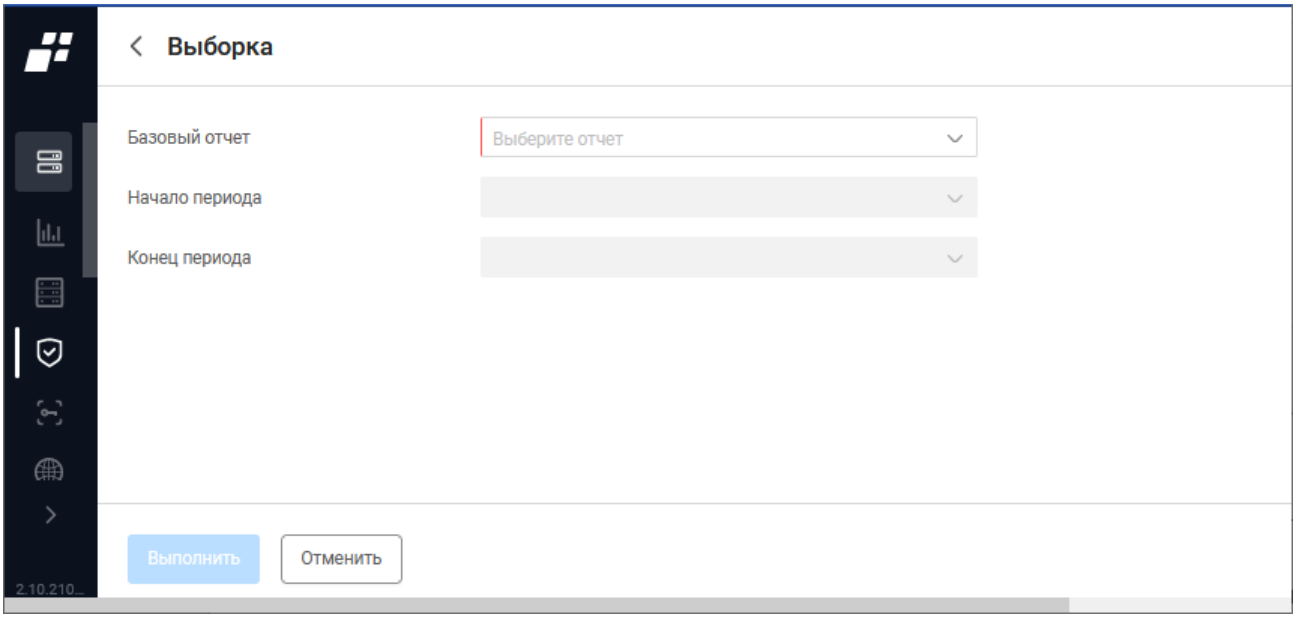
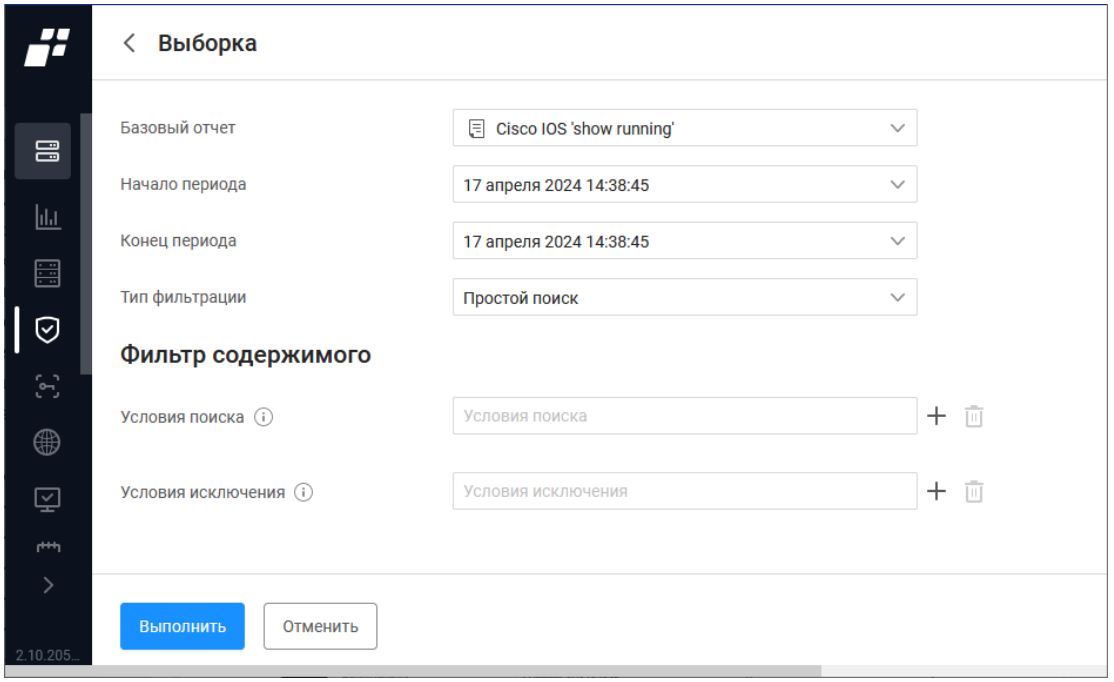


Рисунок 35 – Страница «Создание отчета (Выборка)»

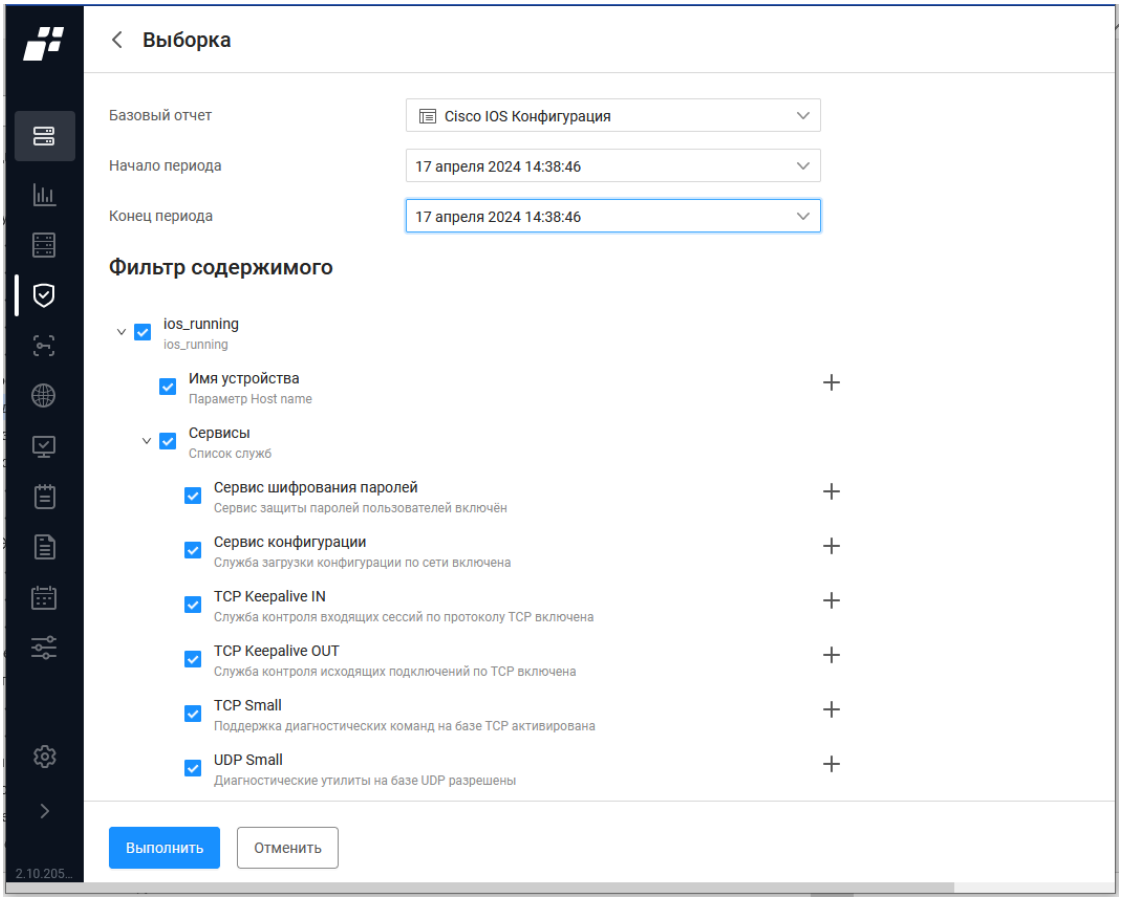
3) Выбрать базовый отчет, на основании которого будет формироваться выборка. В окне дополнительно отобразятся поля ввода параметров выборки (рис. 36). Состав полей окна и правила их заполнения приведены в таблице 7.
4) Заполнить поля страницы необходимыми параметрами и нажать кнопку «Выполнить». Откроется окно просмотра с данными загруженных версий выбранного типа отчета за указанный временной период с учетом установленных условий фильтра данных.

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.



а) для текстового отчета



б) для структурированного отчета

Рисунок 36 – Страница создания выборки с дополнительными полями

Таблица 7 – Состав и описание полей страницы создания выборки архивных отчетов

Поле	Описание
Поле «Базовый отчет»	Выбор варианта базового отчета, на основании которого будет формироваться 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» и Блок полей «Фильтр содержимого»	Правила заполнения полей аналогичны правилам, приведенным в таблице 5 для окна задания фильтров для отчета «Фильтр». Описание регулярных выражений стандарта PCRE, допустимых к применению в ПК «Efros DO» при задании условий поиска для создания отчета «Фильтр», приведено в приложении Б
Элементы управления	
Выполнить	При нажатии кнопки открывается форма просмотра сформированной в соответствии с заданными параметрами выборки
Отменить	При нажатии кнопки окно закрывается без применения введенных данных

2.2 Проверки безопасности

Отображаемые данные и доступная функциональность подраздела «Проверки безопасности» зависят от наличия хотя бы одной лицензии на функциональные модули «Efros NA», «Efros VC» или «Efros ICC».

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

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

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).

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

На рис. 37 приведена страница «Проверки безопасности».

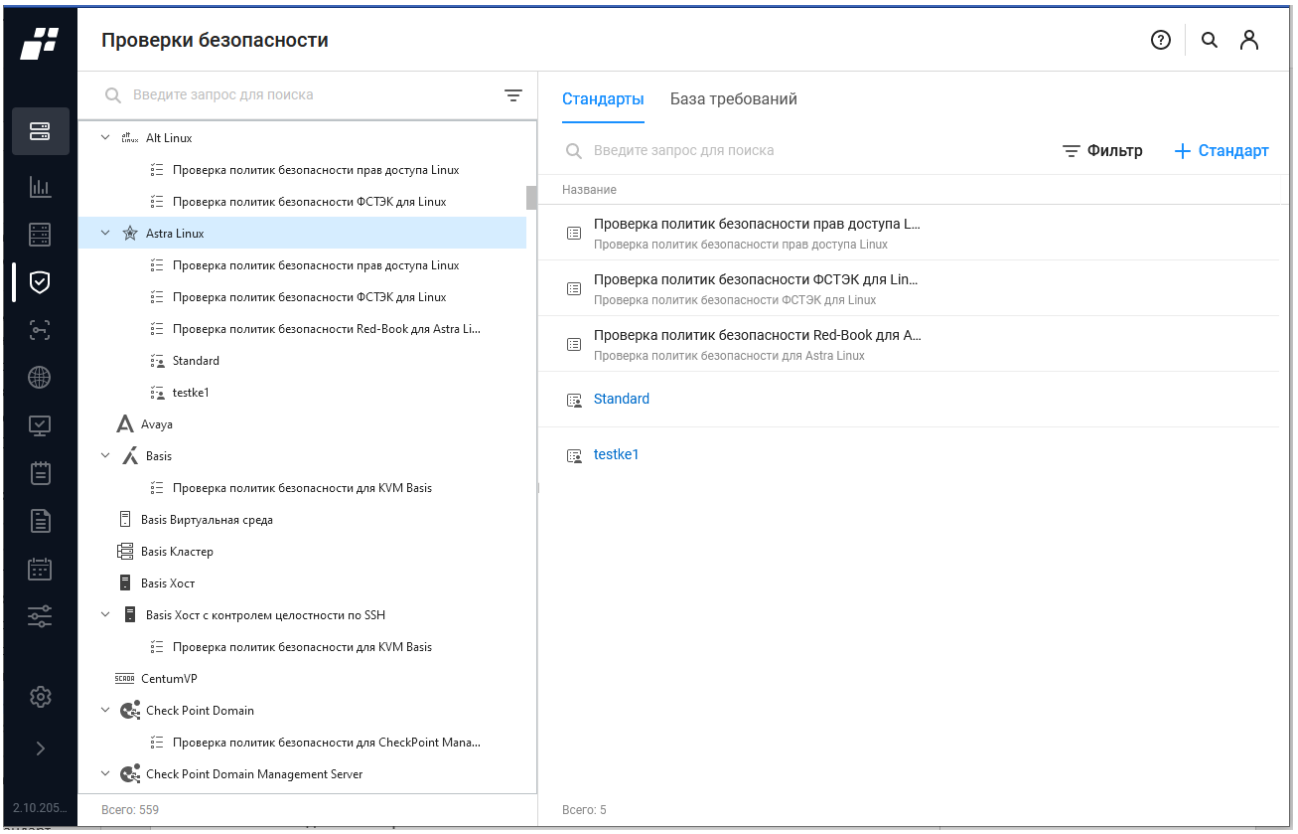


Рисунок 37 – Страница «Проверки безопасности»

Страница 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 (подробнее см. пункт 2.2.2);
  - «База требований» – содержит список требований безопасности для выделенного в дереве типа устройства, сгруппированный по категориям (подробнее см. пункт 2.2.3).

— 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 (на 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.

2.2.1. Дерево со списком стандартов

Иерархический список стандартов, сгруппированный по типам устройств.

При наведении курсора на строку:

1) Типа устройств – в строке отображается кнопка «Добавить» ( ) для перехода в окно создания нового стандарта проверки безопасности для соответствующего типа устройств.
2) Предустановленного стандарта – в строке отображается кнопка «Копировать» ( ) для перехода в окно создания нового пользовательского стандарта проверки безопасности путем копирования соответствующего предустановленного стандарта (с обязательным редактированием предустановленных параметров стандарта).
3) Пользовательского стандарта – в строке отображается кнопка «Меню» ( ), по нажатию которой открывается контекстное меню с пунктами:

— «Изменить» – для перехода в окно редактирования параметров стандарта;
— «Создать копию» – для перехода в окно создания нового пользовательского стандарта проверки безопасности путем копирования соответствующего пользовательского стандарта (с обязательным редактированием предустановленных параметров стандарта);
— «Удалить» – для удаления стандарта.

Над деревом доступны:

— поле поиска (Введите запрос для поиска);
— кнопка «Фильтр» ( ).

2.2.2. Вкладка «Стандарты»

Вкладка «Стандарты» содержит перечень стандартов проверок безопасности для соответствующего типа устройств (см. рис. 37). Для каждого стандарта отображаются:

— иконка типа стандарта:
  - « » – стандарт, созданный пользователем;
  - « » – предустановленный стандарт (появляется при установке модулей).
— название и описание стандарта.

Над списком стандартов располагаются:

— поле поиска (Введите запрос для поиска);

— кнопка «Фильтр» (Фильтр);

— кнопка «Стандарт» (+ Стандарт) для создания нового пользовательского стандарта (см. подпункт 2.2.2.1).

2.2.2.1. Создание пользовательского стандарта безопасности

Для создания пользовательского стандарта безопасности пользователю необходимо выполнить следующие действия:

1) В дереве стандартов выделить тип устройства и нажать в его строке кнопку «Добавить стандарт» (+) или нажать на вкладке «Стандарты» кнопку «Стандарт» (+ Стандарт).
2) На открывшейся странице «Создание стандарта безопасности» (рис. 38) заполнить поля страницы необходимыми параметрами. Состав и описание полей окна «Создание стандарта безопасности» приведены в таблице 8.
3) Нажать кнопку «Создать».

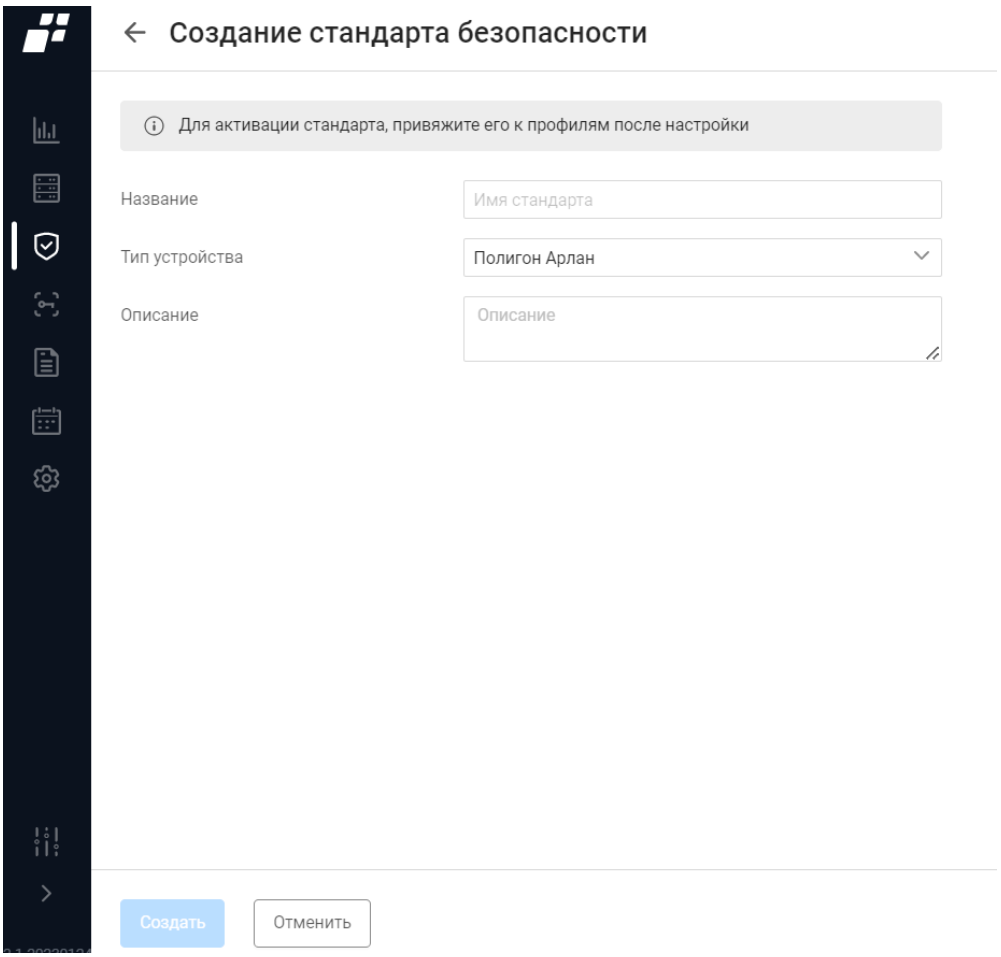


Рисунок 38 – Страница «Создание стандарта безопасности»

Таблица 8 – Состав и описание полей страницы «Создание стандарта безопасности»

Поле	Описание
Поле «Название»	Текстовое поле для ввода названия стандарта безопасности. Параметры ввода текста: от 1 до 250 любых символов
Поле «Тип устройства»	Тип устройства, для которого создается новый стандарт. Поле поддерживает возможность поиска
Поле «Описание»	Текстовое поле для ввода описания стандарта безопасности. Параметры ввода текста: от 1 до 4000 любых символов
Элементы управления	
Создать	При нажатии кнопки выполняется сохранение внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу без сохранения внесенных данных

Созданный стандарт проверки безопасности не содержит требований. Созданные пользовательские требования появятся в подразделе «Проверки безопасности» → вкладка «База требований».

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

Создать пользовательский стандарт можно также путем копирования имеющегося стандарта с помощью кнопки «Копировать» (). Кнопка появляется при наведении курсора на строку существующего стандарта. Далее откроется окно создания стандарта безопасности (см. рис. 38). Необходимо откорректировать требуемые поля и нажать кнопку «Сохранить».

2.2.2.2. Создание пользовательских требований проверок в пользовательском стандарте

Создание пользовательских требований в пользовательских стандартах возможно следующим путем:

- создание новых пользовательских требований;
- копирование имеющихся в пользовательском стандарте требований (с их последующим редактированием);
- выбор требований из базы требований определенного типа устройства;
- выбор требований из стандарта определенного типа устройств.

Для создания нового пользовательского требования необходимо:

1) В дереве выделить тип устройства, для которого был создан пользовательский

стандарт.

2) Выделить созданный пользовательский стандарт (рис. 39).

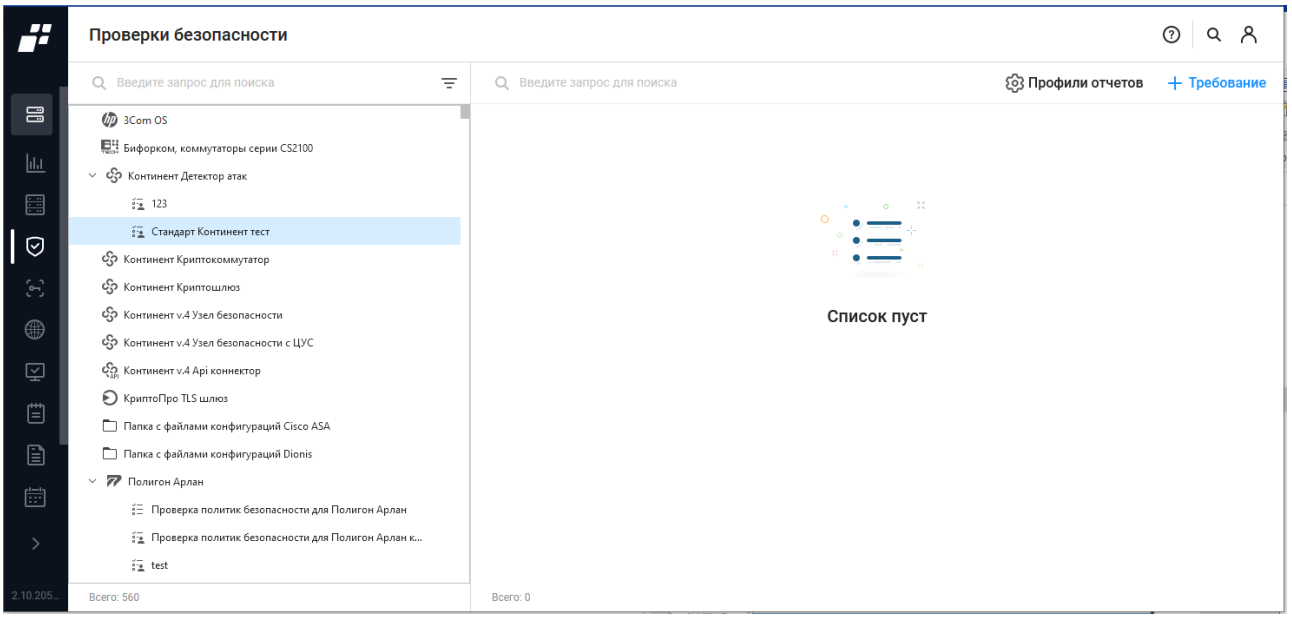


Рисунок 39 – Страница с пользовательским стандартом

3) Нажать кнопку «Требование» (+ Требование) и выбрать в контекстном меню пункт «Создать новое».
4) Откроется страница «Создание требования» (рис. 40). Заполнить поля страницы необходимыми параметрами. Состав и описание полей страницы «Создание требования» приведены в таблице 9.

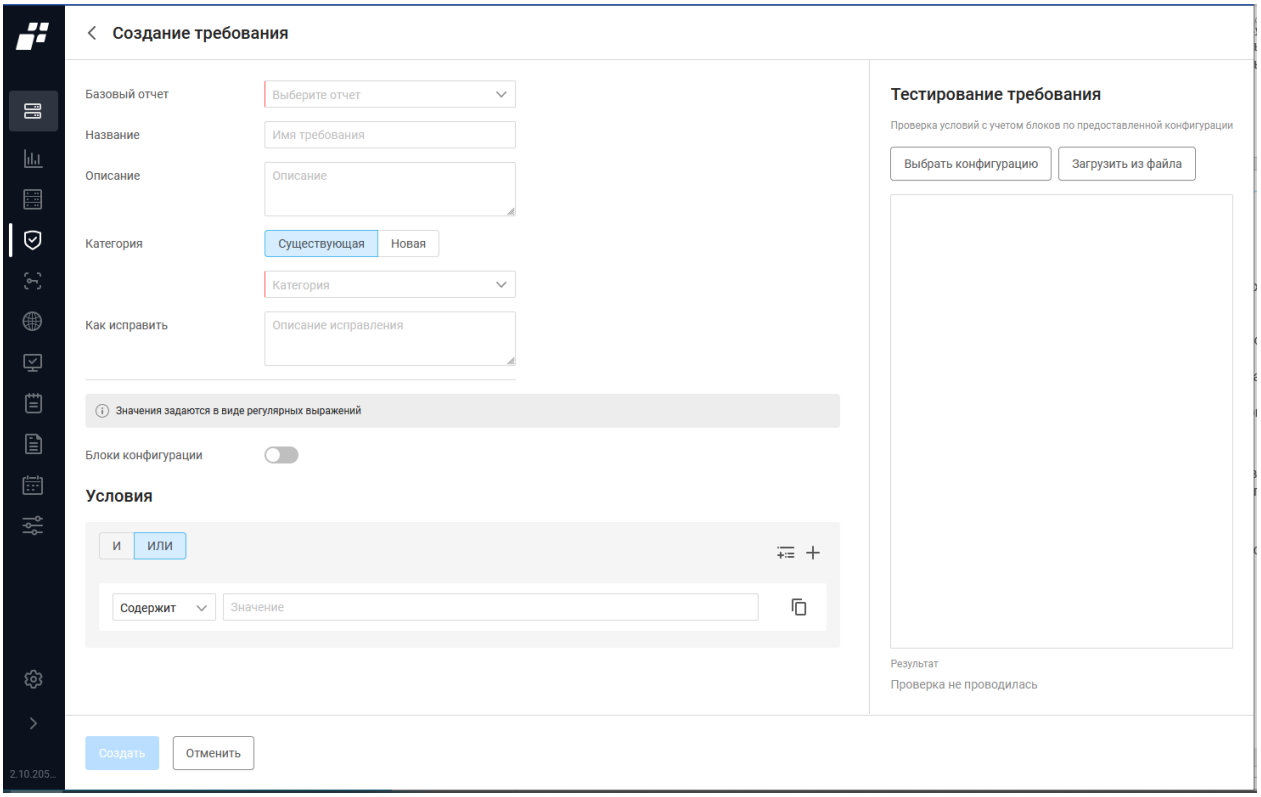


Рисунок 40 – Страница «Создание требования»

Таблица 9 – Состав и описание полей страницы «Создание требования»

Поле	Описание
Поле «Базовый отчет»	Поле с раскрывающимся списком базовых отчетов
Поле «Название»	Текстовое поле для ввода названия требования. Параметры ввода текста: от 1 до 250 любых символов
Поле «Описание»	Текстовое поле для ввода описания требования. Параметры ввода текста: от 1 до 4000 любых символов
Поле «Категория»	Переключатель: — «Существующая» – категория требования выбирается из списка существующих в базе требований для соответствующего производителя в поле со списком под переключателем; — «Новая» – категория отсутствует в базе требований для соответствующего производителя и должна быть добавлена в текстовом поле под переключателем
Поле «Как исправить»	Краткое описание как исправить ошибку при невыполнении требования
Поле «Блоки конфигурации»	Переключатель для включения/отключения блоков конфигурации. При включении переключателя появляются следующие поля: — «Начало блока»; — «Конец блока»;

Поле	Описание
	— «Поиск условий». Блоки конфигурации – это возможность выделить в конфигурации несколько одинаковых частей, в которых в дальнейшем можно контролировать наличие или отсутствие необходимого текста
Поле «Начало блока»	Регулярное выражение, определяющее начало блока конфигурации
Поле «Конец блока»	Регулярное выражение, определяющее конец блока конфигурации
Поле «Поиск условий»	Переключатель: — «В любом блоке» – совпадение хотя бы в одном блоке конфигурации; — «Во всех блоках» – совпадение во всех блоках конфигурации
Поле «Условия»	Поле для назначения/выбора 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» ()
Блок полей «Тестирование требования»	Предназначен для проверки выполнения требования с заданными условиями. Для проверки необходимо загрузить содержимое базового отчета проверки с использованием кнопок «Выбрать конфигурацию» (в открывшемся окне выбирается устройство из списка имеющихся в комплексе объектов защиты соответствующего типа) или «Загрузить из файла» (в открывшемся стандартном окне ОС выбирается файл с конфигурацией). В поле «Результат» отобразится результат выполнения проверки
Элементы управления	
Создать	При нажатии кнопки выполняется сохранение внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу без сохранения внесенных данных

5) Нажать кнопку «Создать».

Для добавления требований в пользовательский стандарт путем копирования имеющегося в стандарте пользовательского требования необходимо выполнить следующие действия:

1) Нажать в строке исходного требования кнопку «Копировать» ( ). Кнопка появляется при наведении курсора на строку требования.
2) Откроется страница «Создание требования» (см. рис. 39), поля которой будут

заполнены параметрами исходного требования. Состав и описание полей страницы приведены в таблице 7.

3) Внести в параметры требуемые изменения и нажать кнопку «Создать».

По умолчанию для созданного требования применяется использование «Запрещено». Для изменения использования необходимо перейти в настройки использования.

Для добавления требований в пользовательский стандарт из общей базы требований или из требований для выбранного типа устройств необходимо выполнить следующие действия:

1) Нажать кнопку «Требование» (+ Требование) и в контекстном меню выбрать пункт «Выбрать».
2) В открывшемся окне «Выбор требований» (рис. 41) выбрать установкой флага в соответствующих полях требования из общей базы требований или из требований для конкретного типа устройства. Состав и описание полей окна «Выбор требований» приведены в таблице 10.
3) Нажать кнопку «Добавить».

По умолчанию для созданного требования применяется использование «Запрещено». Для изменения использования необходимо перейти в настройки использования.

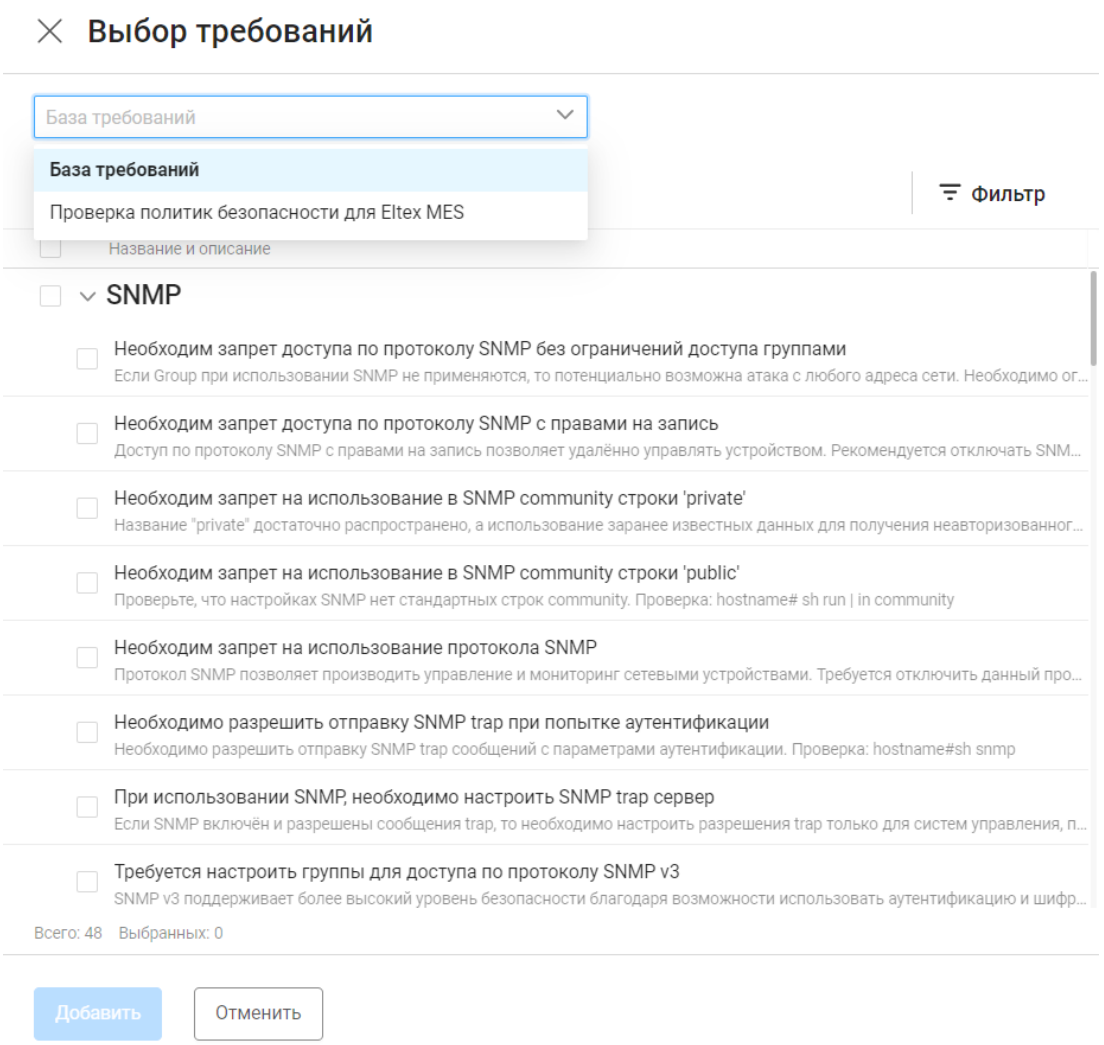


Рисунок 41 – Окно «Выбор требований»

Таблица 10 – Состав и описание полей окна «Выбор требований»

Поле	Описание
Поле «Источник требований»	Поле с выбором источника требования: — база требований; — список стандартов проверок безопасности для конкретного типа устройств
Поле «Список требований»	Список требований, зависящий от выбора в поле «Источник требований»
Элементы управления	
Добавить	При нажатии кнопки выбранные требования отображаются в стандарте
Отменить	При нажатии кнопки окно закрывается без применения введенных данных

2.2.2.3. Настройка использования стандарта проверок безопасности

Для настройки использования стандарта проверок безопасности пользователю необходимо выполнить следующие действия:

1) В дереве со списком стандартов выделить строку настраиваемого стандарта (предустановленного или пользовательского).
2) В заголовке открывшейся страницы стандарта нажать кнопку «Профили отчетов» (Профили отчетов).
3) В открывшемся окне настройки проверок установкой флагов выполнить настройку использования стандарта проверки для всех устройств, к которым он может быть применен – в области «Использование» в раскрывающемся списке выбрать значение «Разрешено».
4) Нажать кнопку «Сохранить».

2.2.2.4. Редактирование требований пользовательских проверок безопасности

Для редактирования требований пользовательских проверок безопасности необходимо выполнить следующие действия:

1) В дереве типов устройств выделить требуемый стандарт проверки безопасности.
2) Выбрать на вкладке «Стандарты» требование, которое необходимо откорректировать, и нажать на название требования. Появится окно для внесения изменений (рис. 42). Внести требуемые изменения в параметры требования. Состав и описание полей окна см. в таблице 11.
3) Нажать кнопку «Сохранить».

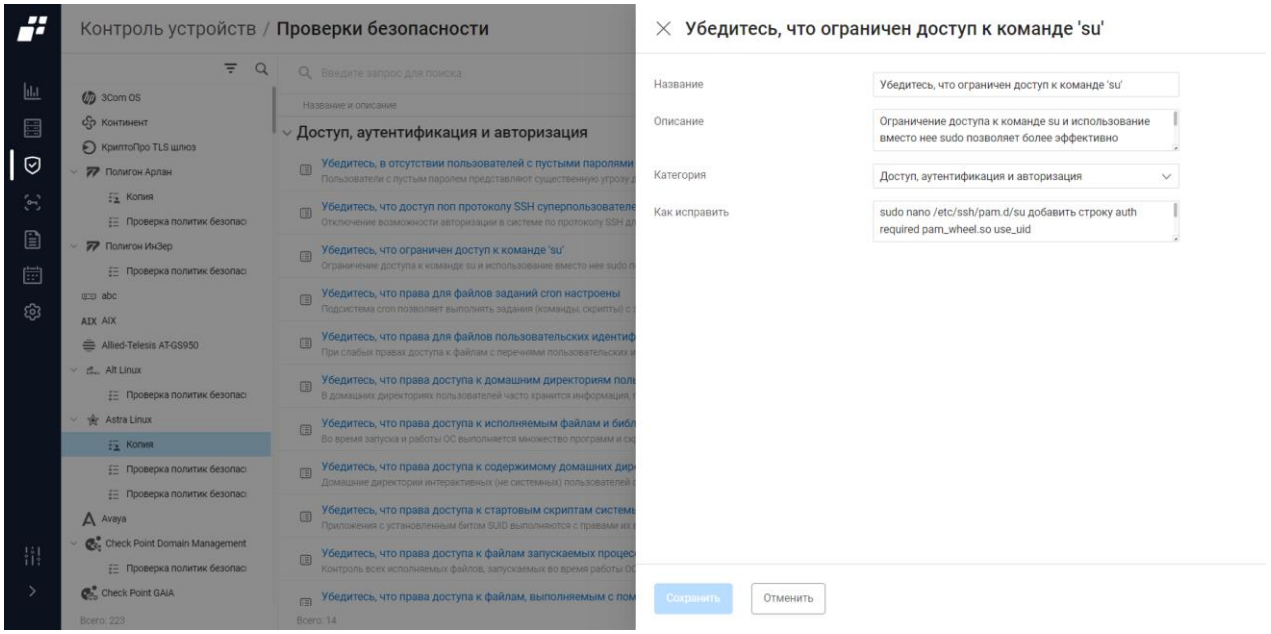


Рисунок 42 – Окно просмотра настроек требования в пользовательском стандарте

Таблица 11 – Состав и описание полей окна настроек требования в пользовательском стандарте

Поле	Описание
Поле «Название»	Текстовое поле. Название редактируемого пользовательского требования
Поле «Описание»	Текстовое поле. Краткое описание редактируемого пользовательского требования
Поле «Категория»	Раскрывающийся список категорий требований предустановленного внешнего модуля
Поле «Как исправить»	Текстовое поле с вариантом исправления невыполненного требования
Элементы управления	
Сохранить	По нажатию кнопки окно настройки закрывается, выполненные изменения применяются
Отменить	По нажатию кнопки окно настройки закрывается без применения введенных изменений

2.2.3. Вкладка «База требований»

Вкладка «База требований» содержит список требований безопасности для выделенного типа устройств в дереве типов устройств (рис. 43).
Над списком требований располагаются:

- поле поиска (Введите запрос для поиска);
- кнопка «Фильтр» (Фильтр);
- кнопка «Требование» (+ Требование) для создания нового требования пользовательского стандарта (см. подпункт 2.2.2.2).

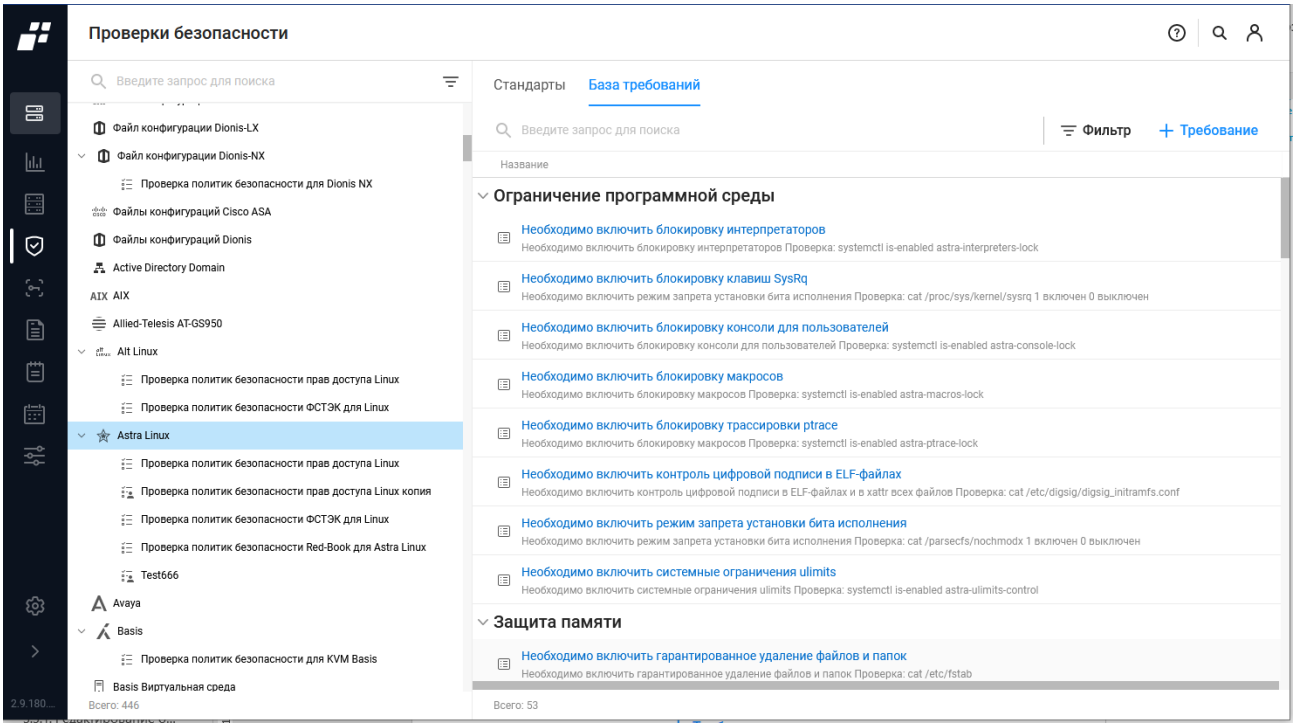


Рисунок 43 – Вкладка «База требований»

На вкладке список требований реализован в виде таблицы. Для каждой записи списка отображаются следующие данные:

- иконка требования («» – предустановленное требование, «» – пользовательское требование);
- название и описание требования.

Пользовательские требования доступны для копирования и удаления, при наведении курсора на строку отображаются кнопки «Копировать» () и «Удалить» ().

2.3 Проверки МЭ

Данный подраздел доступен при наличии лицензии на модуль «Efros FA».

В подразделе «Проверки МЭ» пользователь может добавлять стандарты проверок для анализа движения трафика по зонам (подсетям) и правил межсетевых экранов, а также осуществлять настройку требований проверок безопасности.

Подраздел «Проверки МЭ» состоит из следующих вкладок:

- «Стандарты безопасности» – для ведения списка стандартов безопасности МЭ, содержащих требования для контроля наличия/отсутствия правил МЭ;
- «Зонный анализ» – для ведения списка стандартов зонного анализа МЭ, содержащих требования запрета или разрешения прохождения трафика между зонами;

— «Зоны» – для ведения списка контролируемых сервером ПК зон сети.

2.3.1. Вкладка «Стандарты безопасности»

После установки ПК «Efros DO» список проверок МЭ пуст, на странице отображается сообщение «Список стандартов безопасности пуст. Вы можете создать новый стандарт при помощи кнопки ниже» и кнопка «Создать стандарт» для перехода на страницу создания стандарта безопасности.

Список стандартов безопасности на вкладке «Стандарты безопасности» (рис. 44) реализован в виде таблицы.

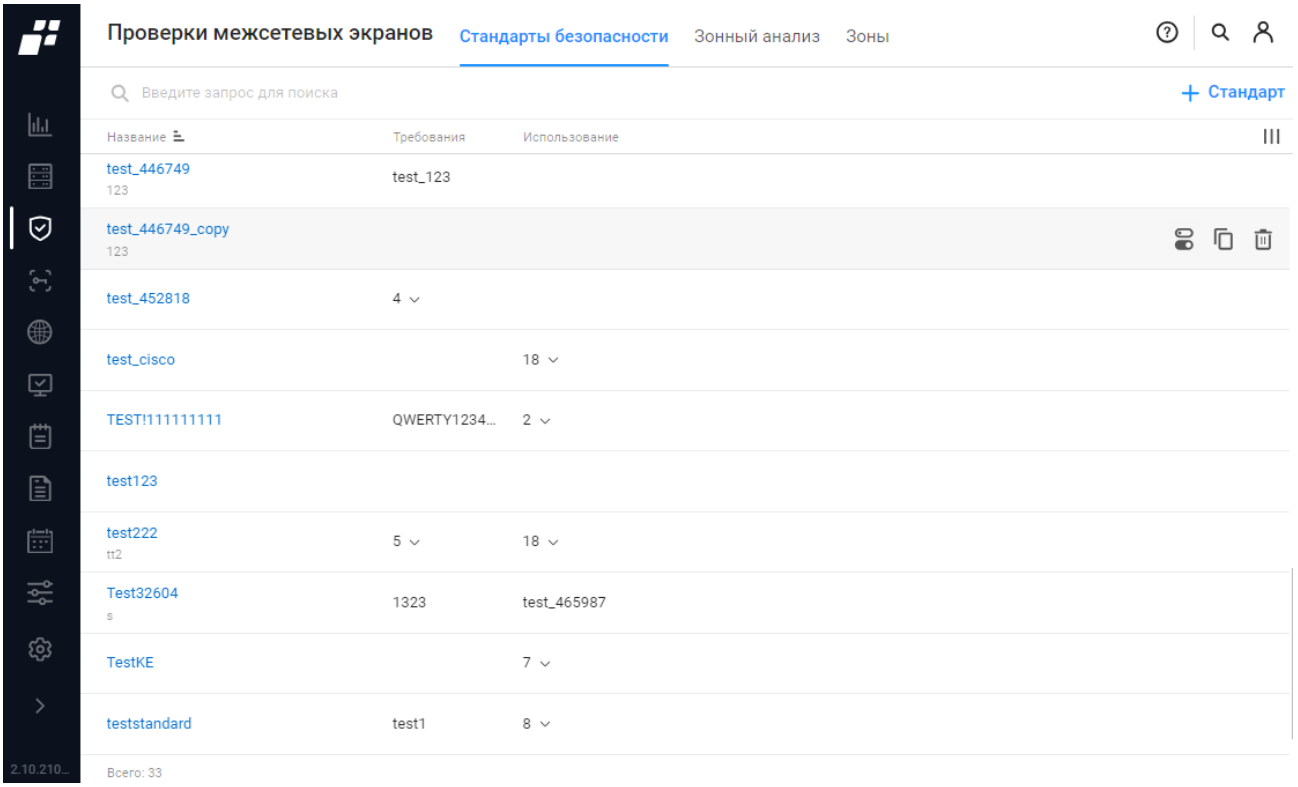


Рисунок 44 – Подраздел «Проверки МЭ», вкладка «Стандарты безопасности»

Для каждой записи списка отображаются следующие данные:

— название стандарта безопасности, является ссылкой, при нажатии которой открывается страница редактирования параметров стандарта;
— количество требований в стандарте или название требования;
— информация о том, в каких профилях отчетов используется стандарт безопасности (количество профилей отчетов или название профиля отчета).

При установке курсора в поле с указанием количества требований или профилей отчетов открывается окно со списком соответственно требований или профилей отчетов.

При наведении курсора на стандарт безопасности, в правой части экрана появляются

кнопки:

- «Использование» ( ) – для настройки использования стандарта;
- «Создать копию» ( ) – для создания нового стандарта на основе соответствующего стандарта;
- «Удалить» ( ).

Над списком стандартов безопасности располагаются:

- поле поиска (Введите запрос для поиска);
- кнопка «Стандарт» (+ Стандарт) – для создания нового стандарта безопасности;
- кнопка «Колонки» ( ).

2.3.1.1. Создание нового стандарта безопасности проверки МЭ

Для создания нового пользовательского стандарта безопасности проверки МЭ необходимо выполнить следующие действия:

1) На вкладке «Стандарты безопасности» нажать кнопку добавления стандарта (+ Стандарт) или кнопку «Создать стандарт», если стандарт создается впервые после установки комплекса.
2) Откроется страница «Создание стандарта безопасности» (рис. 45). Состав и описание полей окна приведены в таблице 12.
3) Заполнить поля страницы необходимыми параметрами.
4) Нажать кнопку «Создать».

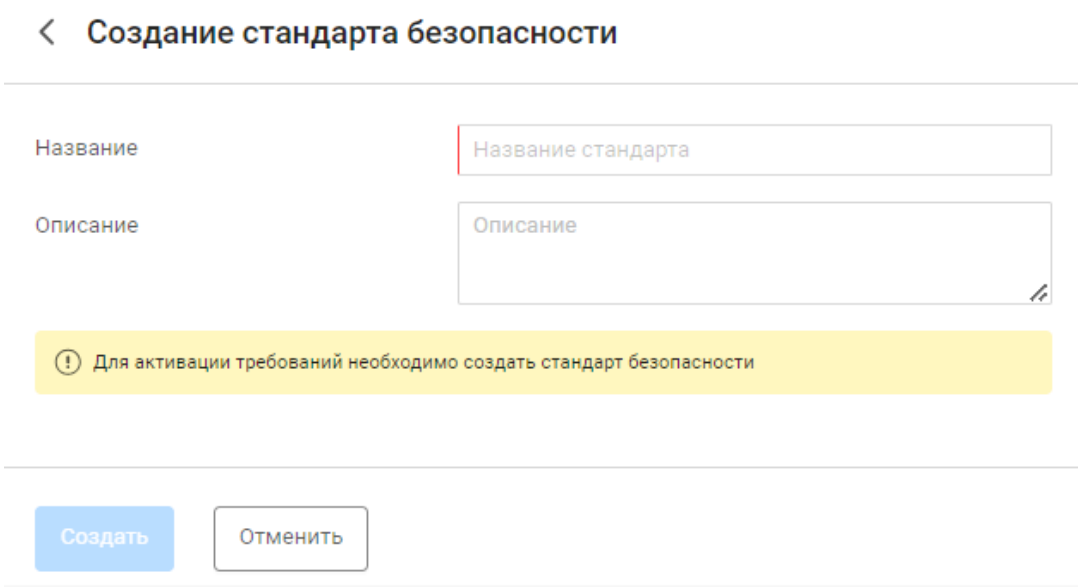


Рисунок 45 – Страница «Создание стандарта безопасности»

Таблица 12 – Состав и описание полей страницы «Создание стандарта безопасности»

Поле	Описание
Поле «Название»	Текстовое поле для ввода названия стандарта. Параметры ввода текста: от 1 до 250 любых символов
Поле «Описание»	Текстовое поле для ввода описания стандарта. Параметры ввода текста: от 1 до 4000 любых символов
Элементы управления	
Создать	При нажатии кнопки выполняется сохранение внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу без сохранения внесенных данных

Созданный стандарт безопасности не содержит требований. Необходимо добавить требования в созданный стандарт (см. подпункт 2.3.1.2) и задать параметры режима его использования в профилях отчетов (см. подпункт 2.3.1.3).

Имя стандарта должно быть обязательно изменено (не допускается наличие дубликатов стандартов безопасности МЭ/зонного анализа).

Создать пользовательский стандарт безопасности проверки МЭ можно также путем копирования имеющегося стандарта с помощью кнопки «Создать копию» (). Кнопка появляется при наведении курсора на строку существующего стандарта. Далее откроется окно создания стандарта безопасности (см. рис. 45). Необходимо откорректировать требуемые поля и нажать кнопку «Сохранить». Созданный путем клонирования стандарт будет содержать все требования исходного стандарта. После копирования можно отредактировать параметры созданного стандарта – добавить/удалить требования в стандарте (см. подпункт 2.3.1.2) и задать параметры режима его использования в профилях отчетов (см. подпункт 2.3.1.4).

2.3.1.2. Редактирование требований стандарта безопасности (вкладка «Требования»)

Для перехода на страницу редактирования стандарта безопасности необходимо нажать в списке стандартов ссылку-название стандарта. Откроется страница редактирования стандарта безопасности с активной вкладкой «Требования». На вкладке «Требования» можно создать новые требования стандарта и редактировать существующие (рис. 46).

Варианты добавления требований в стандарты безопасности:

- создание новых пользовательских требований;
- копирование требований текущего стандарта безопасности;

— копирование требований из других существующих стандартов безопасности.

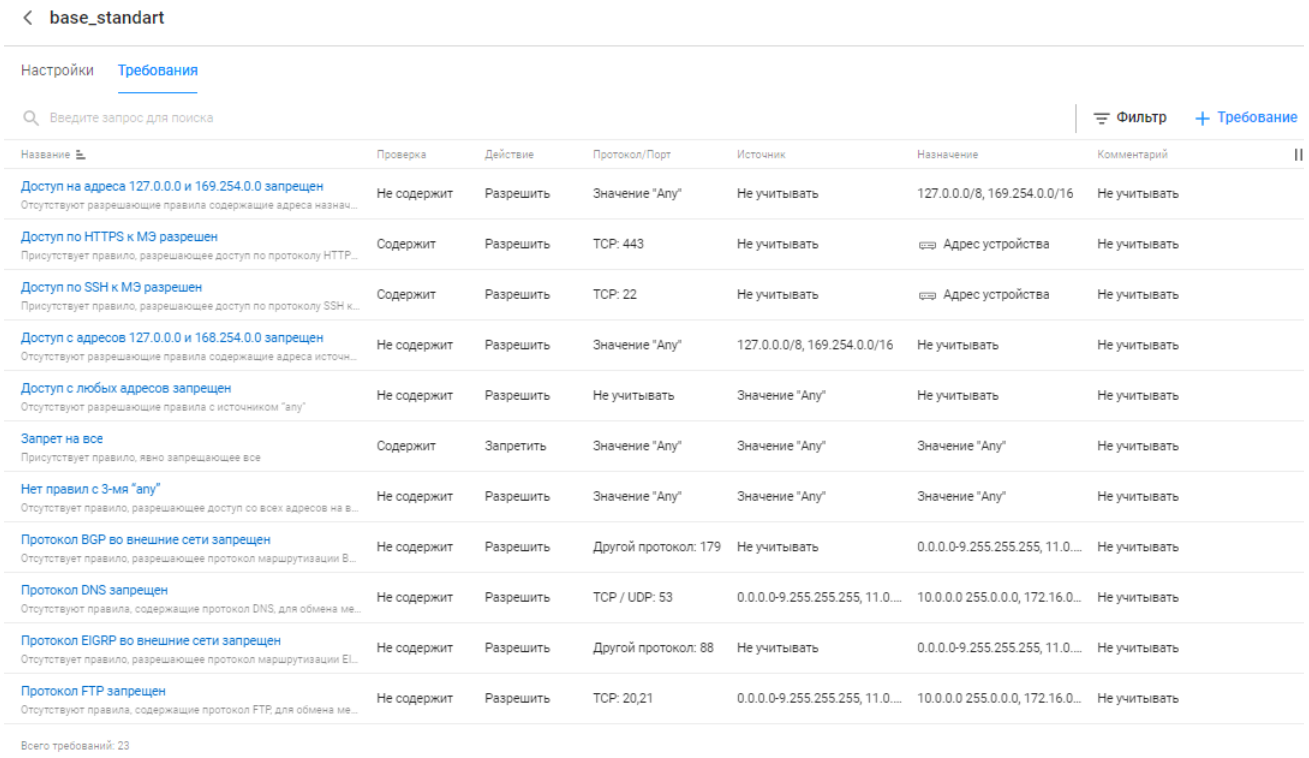


Рисунок 46 – Вкладка «Требования»

Для создания нового пользовательского требования необходимо:

1) Нажать кнопку «Требование» (+ Требование) и в контекстном меню выбрать пункт «Создать новое».
2) Откроется страница «Создание требования» (рис. 47). Заполнить поля страницы необходимыми параметрами. Состав и описание полей окна «Создание требования» приведены в таблице 13.
3) Выполнить при необходимости тестовый запуск отчета по сформированному требованию. Внести при необходимости корректировки в параметры требования по результатам тестирования.
4) Нажать кнопку «Создать».

Для добавления требований в стандарт безопасности МЭ путем копирования имеющегося в стандарте требования необходимо выполнить следующие действия:

1) Нажать в строке исходного требования кнопку «Копировать» ( ). Кнопка появляется при наведении курсора на строку требования.
2) Откроется страница «Создание требования» (см. рис. 47), поля которой будут заполнены параметрами исходного требования. Состав и описание полей страницы приведены в таблице 13.
3) Внести в параметры требуемые изменения и нажать кнопку «Создать».

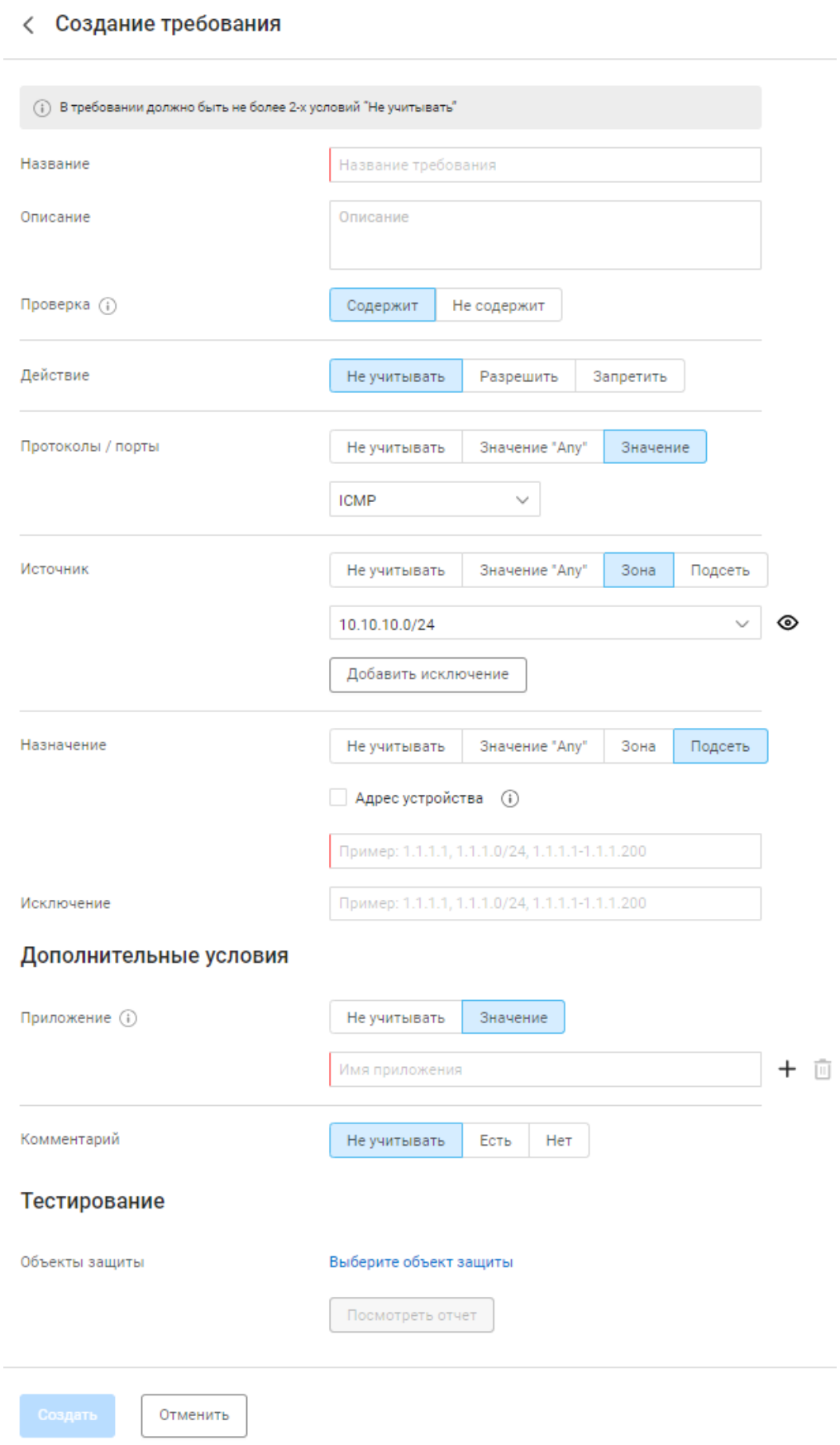


Рисунок 47 – Страница «Создание требования»

Таблица 13 – Состав и описание полей страницы создания нового требования

Поле	Описание
Поле «Название»	Текстовое поле для ввода названия требования. Параметры ввода текста: от 1 до 250 любых символов
Поле «Описание»	Текстовое поле для ввода названия требования. Параметры ввода текста: от 1 до 4000 любых символов
Поле «Проверка»	Поле с двумя переключателями: — «Содержит» – стандарт содержит проверки на наличие правил, соответствующих заданным параметрам требования; — «Не содержит» – стандарт не содержит проверки
Поле «Действие»	Поле с переключателями: — «Не учитывать»; — «Разрешить»; — «Запретить»
Поле «Протоколы/ Порты»	Поле с переключателями: — «Не учитывать»; — «Значение ‘Any’»; — «Значение». При выборе варианта «Значение» появляется раскрывающийся список для выбора протокола (значение по умолчанию: ICMP)
Поле «Источник»*	Поле с переключателем: — «Не учитывать»; — «Значение ‘Any’»; — «Зона»; — «Подсеть». При выборе варианта «Зона» появляется раскрывающийся список IP-адресов зон и возможность исключить IP-адреса из зоны в поле «Исключение»*. При выборе варианта «Подсеть» появляется поле для ввода IP-адресов подсетей и возможность исключить IP-адреса из подсети в поле «Исключение». При установке флага в поле «Адрес устройства» в условии будут использоваться адреса интерфейсов устройства, с которыми связаны политики ACL
Поле «Назначение»*	Поле с переключателем: — «Не учитывать»; — «Значение ‘Any’»; — «Зона»; — «Подсеть».

Поле	Описание
	При выборе варианта «Зона» появляется раскрывающийся список IP-адресов зон и возможность исключить IP-адреса из зон в поле «Исключение»*. При выборе варианта «Подсеть» появляется поле для ввода IP-адресов подсетей и возможность исключить IP-адреса из подсети в поле «Исключение». При установке флага в поле «Адрес устройства» в условии будут использоваться адреса интерфейсов устройства, с которыми связаны политики ACL
Поле «Приложение»	Поле с переключателями: — «Не учитывать»; — «Значение» При выборе варианта «Значение» появляется поле добавления поля приложения для фильтрации уровня приложений правил МЭ
Поле «Комментарий»	Поле с переключателями: — «Не учитывать»; — «Есть»; — «Нет»
Тестирование	
Поле «Объекты защиты»	Поле со ссылкой на существующие устройства в БД комплекса для выбора устройства, на котором будет выполнен тестовый запуск отчета
Кнопка «Посмотреть отчет»	При нажатии кнопки выполняется запуск формирования тестового отчета. Отчет содержит перечень правил для указанного устройства, удовлетворяющих заданным параметрам требования
Элементы управления	
Создать	При нажатии кнопки выполняется сохранение внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу без сохранения внесенных данных
* Поле поддерживает возможность поиска	

Для добавления требований в стандарт безопасности МЭ путем копирования требований из других существующих стандартов безопасности, необходимо выполнить следующие действия:

1) Нажать кнопку «Требование» (+ Требование) и из раскрывающегося списка выбрать «Копировать из стандарта». Откроется окно «Выбор требований»

(рис. 48).

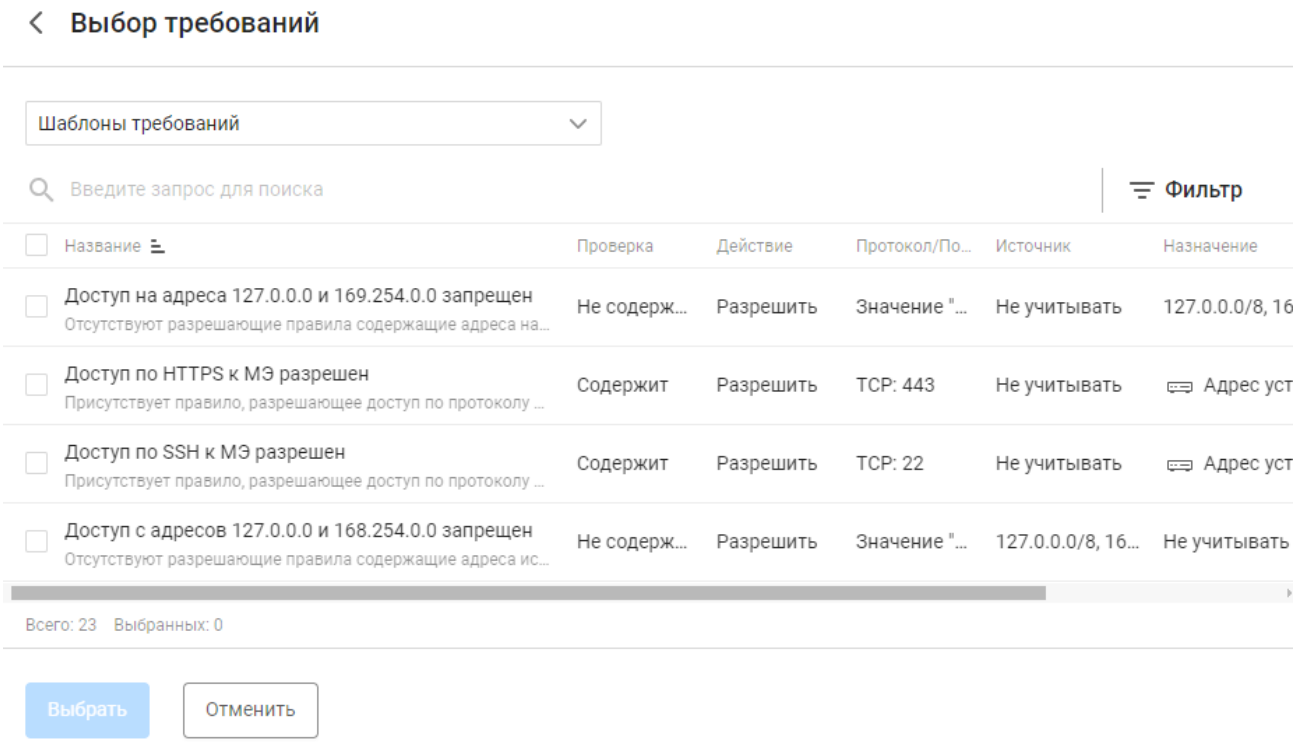


Рисунок 48 – Окно «Выбор требований»

2) В поле выбора стандартов выбрать стандарт безопасности и отметить необходимые требования проверок для их переноса в текущий стандарт. При необходимости воспользоваться фильтром.
3) Нажать кнопку «Выбрать».

По умолчанию для созданного требования применяется использование «Запрещено». Для изменения использования необходимо перейти в настройки использования.

Для редактирования требования необходимо нажать ссылку-наименование требования в списке требований стандарта, внести в поля открывшейся страницы редактирования (аналогична странице создания требования (см. рис. 47, таблицу 13)) требуемые изменения и нажать кнопку «Сохранить».

2.3.1.3. Редактирование параметров стандарта безопасности (вкладка «Настройки»)

Для редактирования параметров стандарта безопасности необходимо нажать в списке стандартов ссылку-название стандарта и на открывшейся странице редактирования стандарта безопасности с активной вкладкой «Требования» перейти на вкладку «Настройки» (рис. 49).

На вкладке «Настройки» можно редактировать наименование, описание и

использование стандарта в профилях отчетов (подробнее см. подпункт 2.3.1.4).

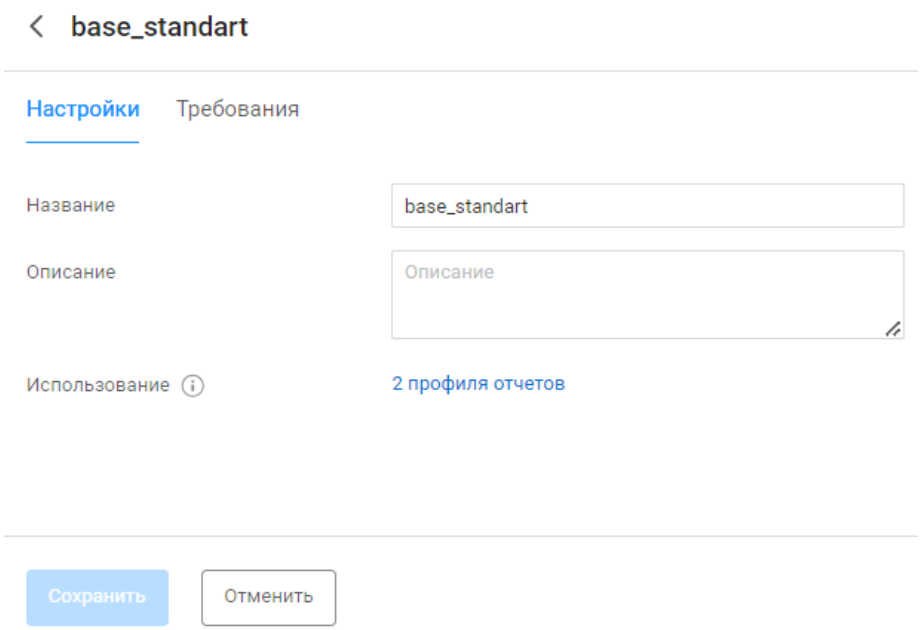


Рисунок 49 – Страница стандарта безопасности. Вкладка «Настройки»

2.3.1.4. Настройка использования стандарта безопасности

Для настройки использования стандарта безопасности МЭ необходимо выполнить следующие действия:

1) В списке стандартов в строке настраиваемого стандарта нажать кнопку «Использование» ( ).или при редактировании параметров стандарта на вкладке «Настройки» (см. подпункт 2.3.1.3) нажать на ссылку поля «Использование».
2) В открывшемся окне выполнить настройку использования стандарта безопасности для профилей отчетов устройств, к которым он может быть применен. Для этого в области «Использование» в раскрывающемся списке выбрать значение «Разрешено» (рис. 50).
3) Нажать кнопку «Сохранить».

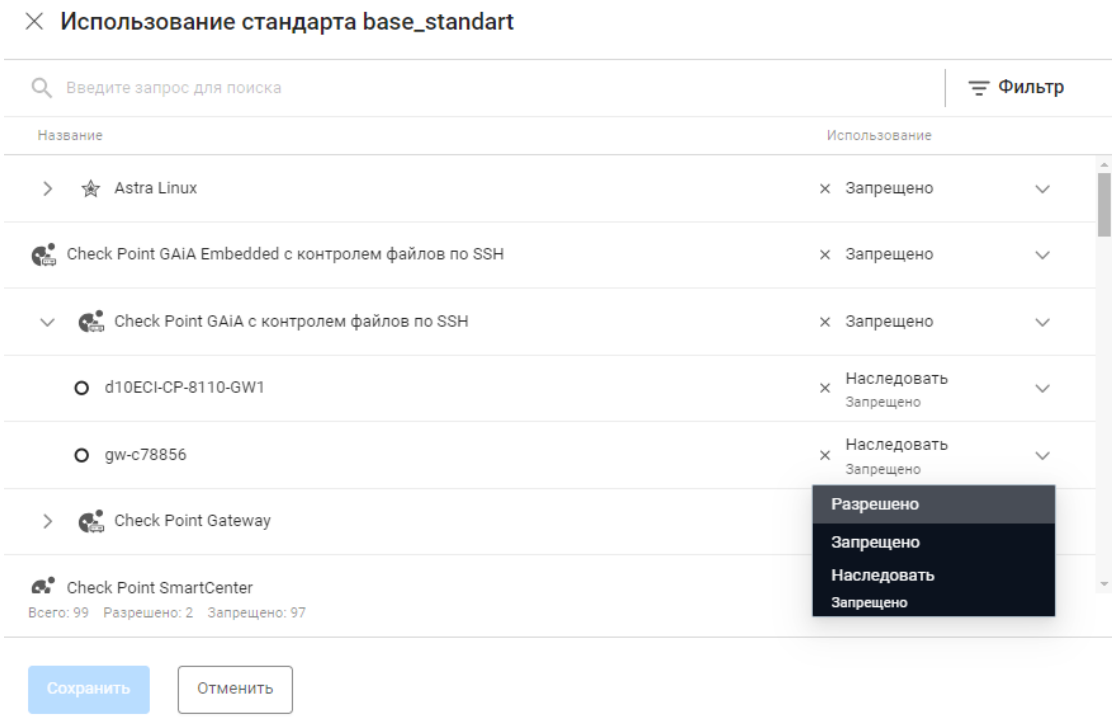


Рисунок 50 – Окно настройки профилей для выбранного стандарта безопасности

В разделе «Устройства» на вкладке «Отчеты» устройства, связанного с профилем отчетов, для которого разрешено использование стандарта безопасности МЭ, станет доступен новый отчет типа «Проверки» с наименованием, соответствующим разрешенному стандарту. На вкладке «Отчет» будет содержаться перечень требований стандарта безопасности, для каждого требования будет приведен список правил МЭ, удовлетворяющих заданным параметрам требования, на вкладке «История изменений» – перечень версий отчета с зафиксированными изменениями в соответствующем стандарте безопасности МЭ.

2.3.2. Вкладка «Зонный анализ»

После установки ПК «Efros DO» список стандартов зонного анализа пуст, на странице отображается сообщение «Список пуст. Вы можете создать стандарт при помощи кнопки ниже» и кнопка «Создать стандарт».

Список стандартов зонного анализа на вкладке «Зонный анализ» (рис. 51) реализован в виде таблицы. Для каждой записи списка отображаются следующие данные:

- название стандарта зонного анализа, является ссылкой, при нажатии которой открывается страница редактирования параметров стандарта;
- количество зон, которые стандарт контролирует;
- информация о том, в каких профилях отчетов используется стандарт зонного анализа (количество профилей отчетов или название профиля отчета).

При установке курсора в поле с указанием количества зон или профилей отчетов открывается окно со списком соответственно зон сети или профилей отчетов.

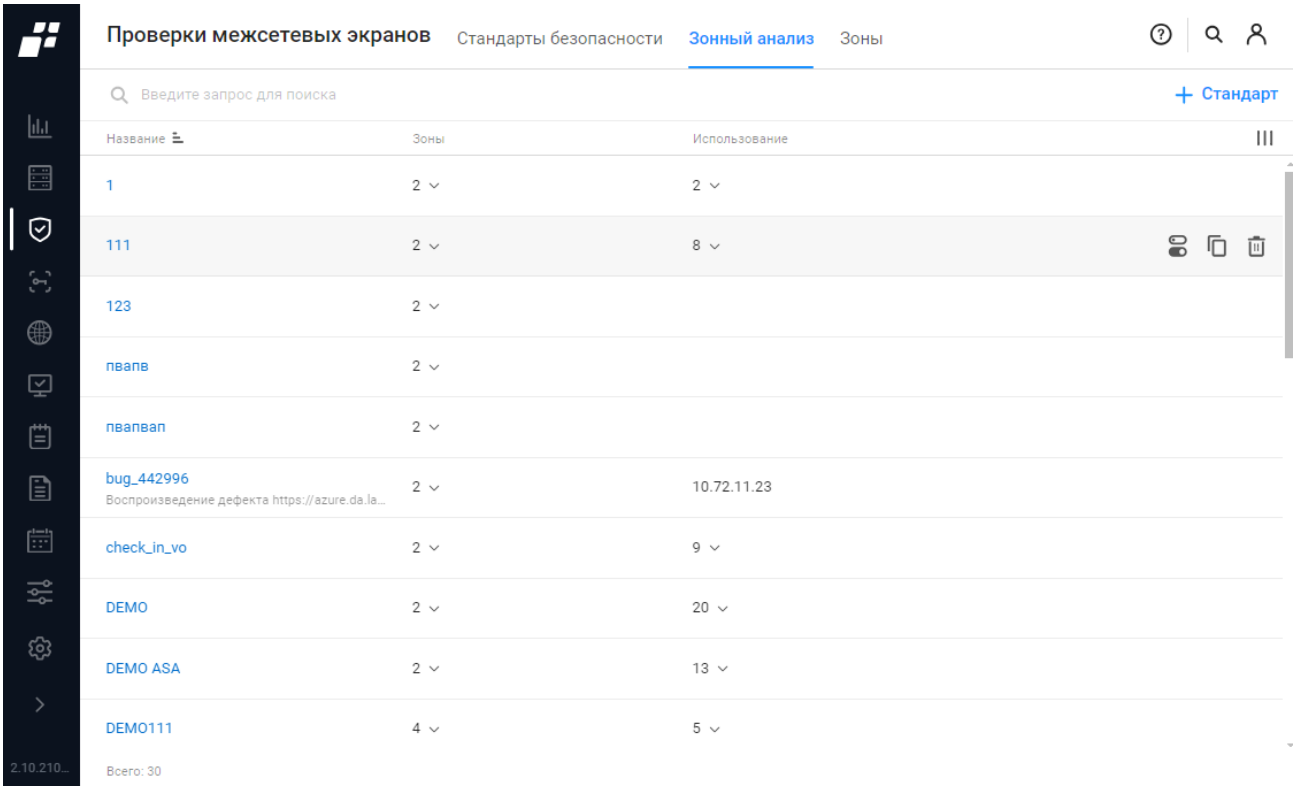


Рисунок 51 – Вкладка «Зонный анализ»

Над списком стандартов располагаются:

- поле поиска (Введите запрос для поиска);
- кнопка «Стандарт» (Стандарт);
- кнопка «Колонки» ( ).

При наведении курсора на строку со стандартом, в правой части строки появятся кнопки:

- «Использование» ( ) – для настройки использования стандарта;
- «Создать копию» ( ) – для создания нового стандарта на основе соответствующего стандарта;
- «Удалить» ( ).

2.3.2.1. Создание нового стандарта зонного анализа

Для создания нового стандарта зонного анализа необходимо выполнить следующие действия:

1) На вкладке «Зонный анализ» нажать кнопку добавления стандарта (Стандарт).

2) Откроется страница «Создание стандарта зонного анализа» (рис. 52). Состав и описание полей окна приведены в таблице 14.
3) Заполнить поля страницы необходимыми параметрами, настроить при этом матрицу требований запрета и/или разрешения трафика между зонами в соответствии с подпунктом 2.3.2.2.
4) Нажать кнопку «Создать».

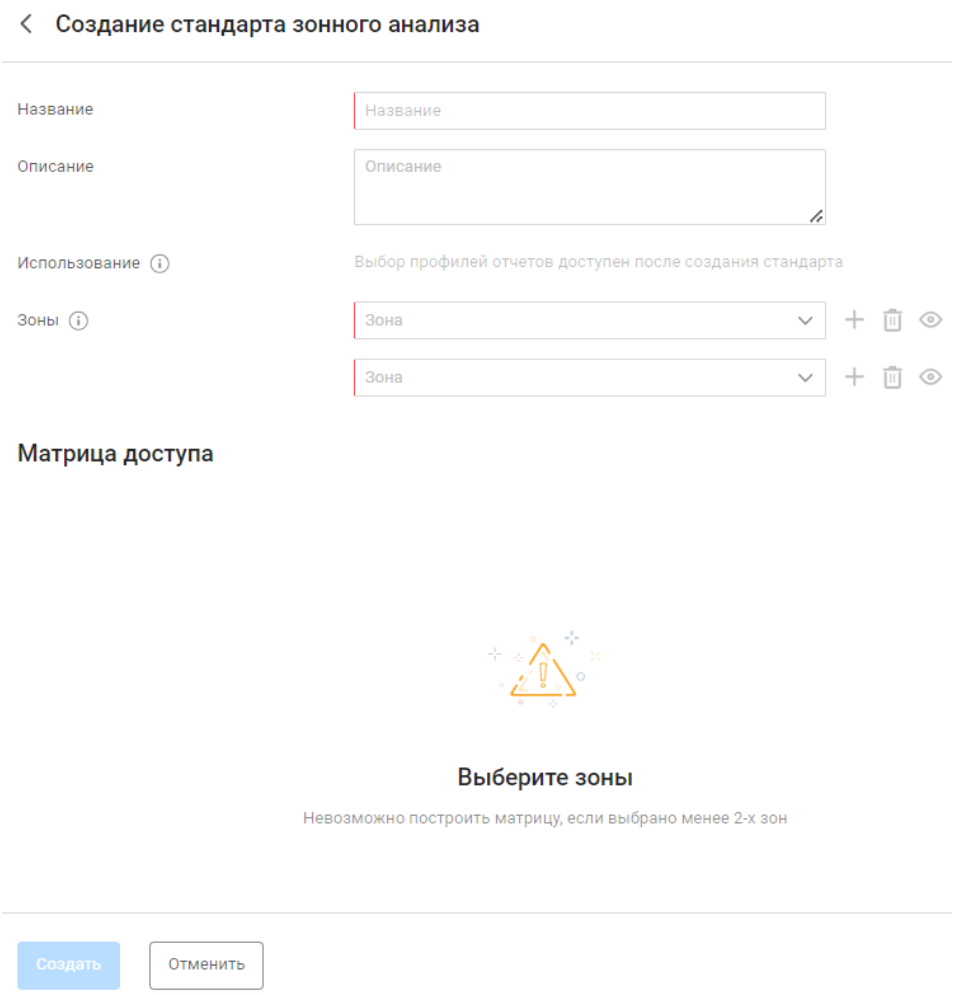


Рисунок 52 – Страница «Создание стандарта зонного анализа»

Таблица 14 – Состав и описание полей страницы «Создание стандарта зонного анализа»

Поле	Описание
Поле «Название»	Текстовое поле для ввода названия стандарта. Параметры ввода текста: от 1 до 250 любых символов
Поле «Описание»	Текстовое поле для ввода описания стандарта. Параметры ввода текста: от 1 до 4000 любых символов
Поле «Использование»	Поле для выбора профиля отчета, на основании которого стандарт будет привязан к устройству

Поле	Описание
Поле «Зона»	Список полей с раскрывающимся списком зон для формирования матрицы доступа. В поле доступен поиск зон по мере ввода символов из названия зоны. В правой части любой строки доступны кнопки: — «Добавить» (+) – для добавления строки; — «Удалить» (🗑) – для удаления строки» — «Просмотреть» (👁) – для просмотра состава выбранной зоны (IP-адрес/ IP-адрес с маской/ диапазон) Слева от каждой строки отображается символ «⠿». Перетаскиванием символа изменяется положение строки в списке и положение зоны в матрице доступа (см. ниже)
Поле «Матрица доступа»	Позволяет настроить требования запрета и/или разрешения трафика между зонами. ⓘ Матрица доступа автоматически заполняется после выбора зон в поле «Зоны». При добавлении в поле «Зона» новой строки в матрице добавляются строка и столбец с наименованием новой зоны, в полях на пересечении с другими зонами доступна ссылка «Не учитывать». По нажатию ссылки открывается окно настройки требования запрета и/или разрешения трафика между зонами, указанными в соответствующих столбце и строке (подробнее см. подпункт 2.3.2.2). После задания параметров требования, в ячейке матрицы отобразятся данные – выбранный тип доступа (полный или частичный запрет или разрешение), для частичного разрешения/запрета протоколы и порты, параметры остальных взаимодействий (при наличии), исключения. Если требованию назначен уровень критичности, то в левой части ячейки будет отображаться полоса соответствующего уровню цвета (см. таблицу 15)
Элементы управления	
Создать	При нажатии на кнопку введенные данные сохраняются
Отменить	При нажатии на кнопку введенные данные не сохраняются

ⓘ Добавленный стандарт зонного анализа не содержит требований. Необходимо добавить требования (см. подпункт 2.3.2.2) и при необходимости изменить параметры режима его использования в профилях отчетов (выполняется аналогично настройке использования стандартов безопасности МЭ в соответствии

с подпунктом 2.3.1.4).

Создать стандарт зонного анализа можно также путем копирования имеющегося стандарта с помощью кнопки «Создать копию» ( ). Кнопка появляется при наведении курсора на строку существующего стандарта. Далее откроется страница создания стандарта зонного анализа (см. рис. 52). Необходимо откорректировать требуемые поля и нажать кнопку «Сохранить». Созданный путем клонирования стандарт будет содержать все требования исходного стандарта. После копирования можно отредактировать параметры созданного стандарта – добавить/удалить требования в стандарте (см. подпункт 2.3.2.2) и задать параметры режима его использования в профилях отчетов (см. подпункт 2.3.1.4).

2.3.2.2. Создание нового требования для стандарта зонного анализа

Для создания нового требования для стандарта зонного анализа необходимо:

1) В матрице доступа выбрать поле для настройки трафика между зонами и нажать в нем ссылку «Не учитывать» (на рис. 53).

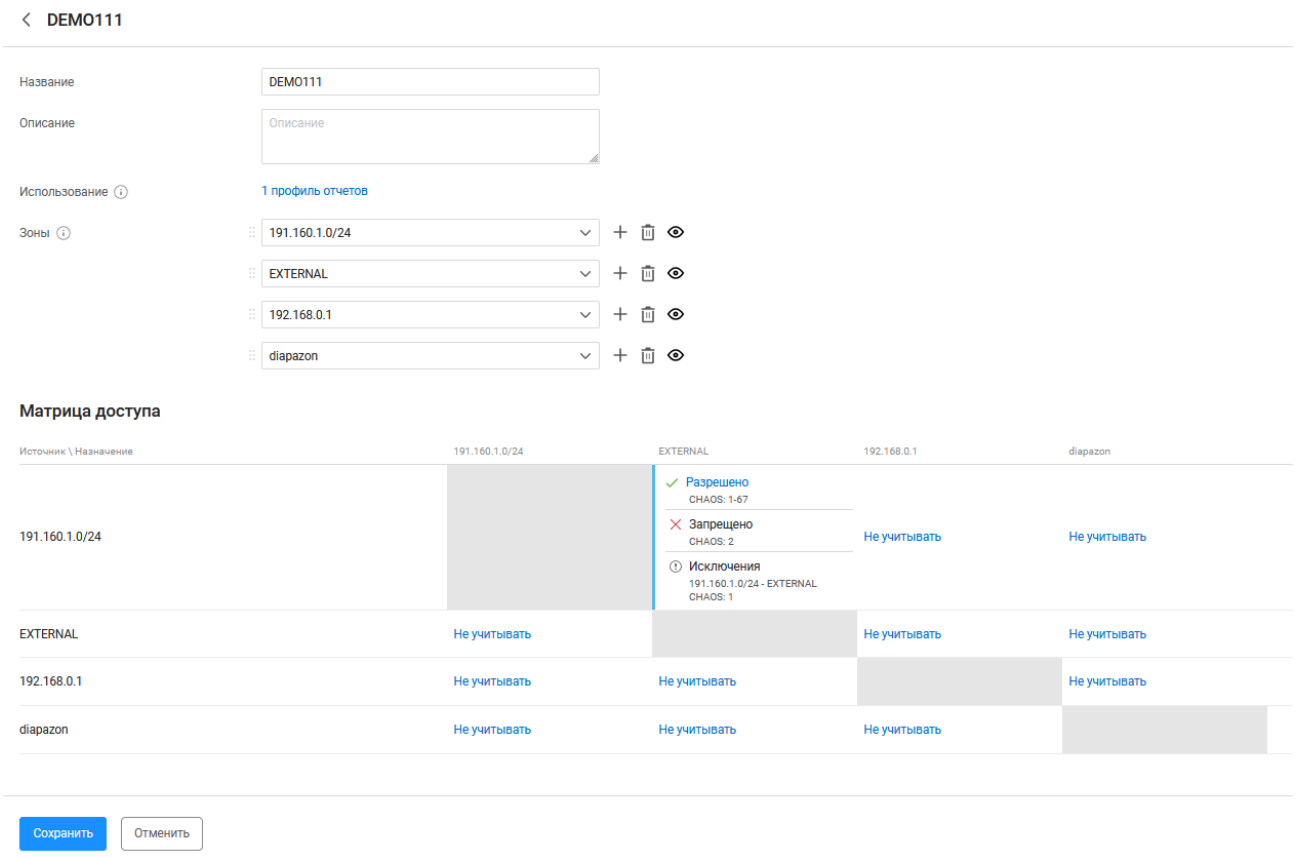


Рисунок 53 – Страница «Создание стандарта зонного анализа»

2) Откроется окно создания нового требования (рис. 54). Состав и описание полей окна приведены в таблице 15.
3) Заполнить поля окна необходимыми параметрами и нажать кнопку «Изменить». Окно создания нового требования закроется, в поле настройки трафика между

зонами, выбранном в перечислении 1 отобразятся краткие характеристики требования – тип доступа, заданные ограничения и исключения с указанными в настройках требования портами/протоколами.

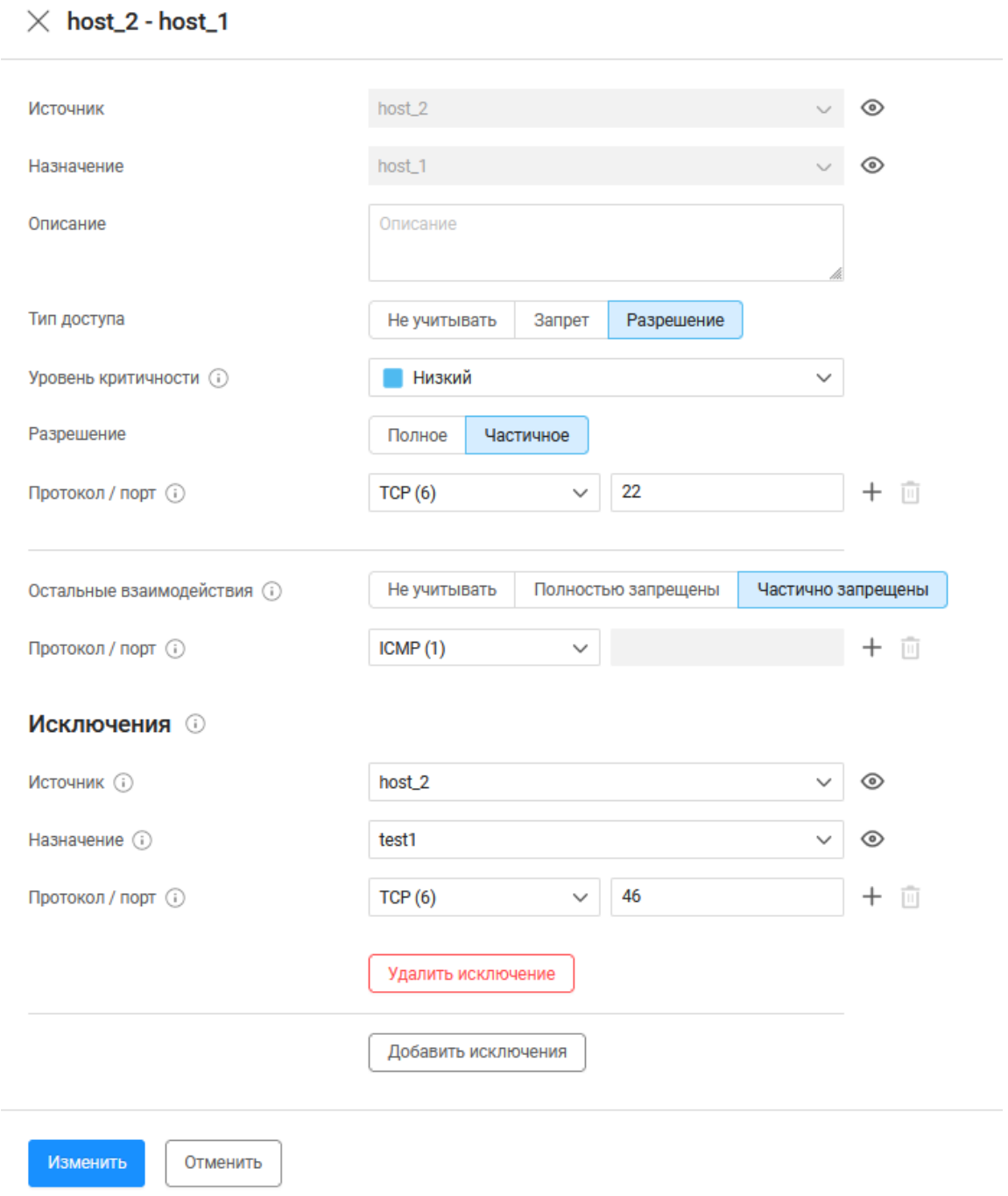


Рисунок 54 – Окно создания нового требования

Таблица 15 – Состав и описание полей окна создания нового требования

Поле	Описание
Поле «Источник»	Отправитель трафика. Определяется автоматически. Недоступен для корректировки

Поле	Описание
Поле «Назначение»	Получатель трафика. Определяется автоматически. Недоступен для корректировки
Поле «Описание»	Текстовое поле для ввода описания требования. Параметры ввода текста: от 1 до 4000 любых символов
Поле «Тип доступа»	Переключатель: — «Не учитывать» – требование не настроено и не применяется; — «Запрет» – для настройки параметров требования, запрещающих трафик между указанными источником и получателем; — «Разрешение» – для настройки параметров требования, разрешающих трафик между указанными источником и получателем
Поле «Уровень критичности»	Поле со списком для выбора уровня критичности требования. Выбранный уровень будет отображаться в соответствующей ячейке матрицы доступа, при просмотре в подразделе «Устройства» отчетов зонного анализа (с пиктограммой «  ») на уровне правила «зона-зона», а также при просмотре в разделе «Центр задач» карточки заявки типа «Запрос доступа» на вкладках «Соответствие» и «Проверка». Каждому уровню соответствует цвет его отображения – «Низкий» (■), «Средний» (■), «Высокий» (■) или «Критичный» (■)
Поле «Запрет»	Появляется при выборе в поле «Тип доступа» положения переключателя «Запрет». Переключатель: — «Полный» – полный запрет трафика. Далее при необходимости добавить исключения требования по кнопке «Добавить исключения» (см. ниже); — «Частичный» – частичный запрет трафика. Далее необходимо указать запрещаемые протоколы и порты (см. ниже описание поля «Протокол/порт»), а также указать параметры взаимодействия по другим протоколам/портам (см. ниже описание поля «Остальные взаимодействия») и, при необходимости, добавить для них исключения по кнопке «Добавить исключения» (см. ниже)
Поле «Разрешение»	Появляется при выборе в поле «Тип доступа» положения переключателя «Разрешение».

Поле	Описание
	Переключатель: — «Полное» – полное разрешение трафика. Далее при необходимости добавить исключения требования по кнопке «Добавить исключения» (см. ниже); — «Частичное» – частичное разрешение трафика. Далее необходимо указать разрешенные протоколы и порты (см. ниже описание поля «Протокол/порт»), а также указать параметры взаимодействия по другим протоколам/портам (см. ниже описание поля «Остальные взаимодействия») и, при необходимости, добавить для них исключения по кнопке «Добавить исключения» (см. ниже)
Кнопка «Добавить исключения»	После нажатия кнопки на странице дополнительно отображается блок полей для добавления исключения требования: — «Источник» – для выбора источника трафика; — «Назначение» – для выбора получателя трафика; — «Протокол/порт» – для выбора протокола обмена из списка значений и указания исключаемых из проверки портов (подробнее см. ниже). Блок может быть удален по нажатию кнопки «Удалить исключение». Для добавления нового блока полей для добавления исключения требования – нажать повторно кнопку «Добавить исключение»
Поле «Протокол/порт»	Содержит раскрывающийся список используемых протоколов и значение «Любой» для выбора исключаемого из проверки протокола. Для некоторых протоколов (например, TCP, UDP, TCP/UDP) доступен ввод номеров портов, исключаемых из проверки. Порты указываются через «,», допустимо указывать диапазон, например, 22,23,45-47. Поле может содержать несколько строк с различными выбранными протоколами/портами. Добавление строк выполняется по нажатию кнопки «Добавить» (+), удаление – по нажатию кнопки «Удалить» (🗑) в правой части любой строки
Поле «Остальные взаимодействия»	Позволяет настроить требования обратного действия. Переключатель: — «Не учитывать»;

Поле	Описание
	— «Полностью запрещены»; — «Частично запрещены». При выборе положения «Частично разрешены» необходимо указать разрешенные протоколы/порты обмена данными (см. выше описание поля «Протокол/порт») и, при необходимости, добавить для них исключения по кнопке «Добавить исключения» (см. выше)
Элементы управления	
Создать	При нажатии на кнопку введенные данные сохраняются
Отменить	При нажатии на кнопку введенные данные не сохраняются

Для просмотра и редактирования параметров требования стандарта зонного анализа необходимо в матрице доступа выбрать требуемое поле для настройки трафика между зонами и нажать в нем ссылку-тип доступа, выбранный ранее в требовании. Откроется окно редактирования параметров требования, аналогичное окну создания требования (см. рис. 54). Далее необходимо просмотреть заданные ранее параметры требования, внести требуемые изменения в соответствии с таблицей 15 и нажать кнопку «Сохранить».

2.3.3. Вкладка «Зоны»

После установки ПК «Efros DO» на странице отображаются разделы «Внутренние адреса» и «Глобальные адреса». Разделы не содержат ни одной зоны.

Вкладка «Зоны» (рис. 55) предназначена для создания необходимых зон для выполнения зонного анализа. На странице список зон реализован в виде списка.

Для каждой записи списка отображаются:

- название зоны, является ссылкой, при выборе которой открывается страница редактирования параметров зоны сети;
- состав зоны (IP-адрес/ IP-адрес с маской/ диапазон);
- информация о том, с какими стандартами безопасности связана зона (название стандарта безопасности или количество стандартов безопасности, при выборе которого открывается список названий стандартов);
- информация о том, с какими стандартами зонного анализа связана зона (название стандарта зонного анализа или количество стандартов зонного анализа, при выборе которого открывается список названий стандартов);
- дата, время внесения последних изменений в запись списка и логин пользователя, внесшего изменения.

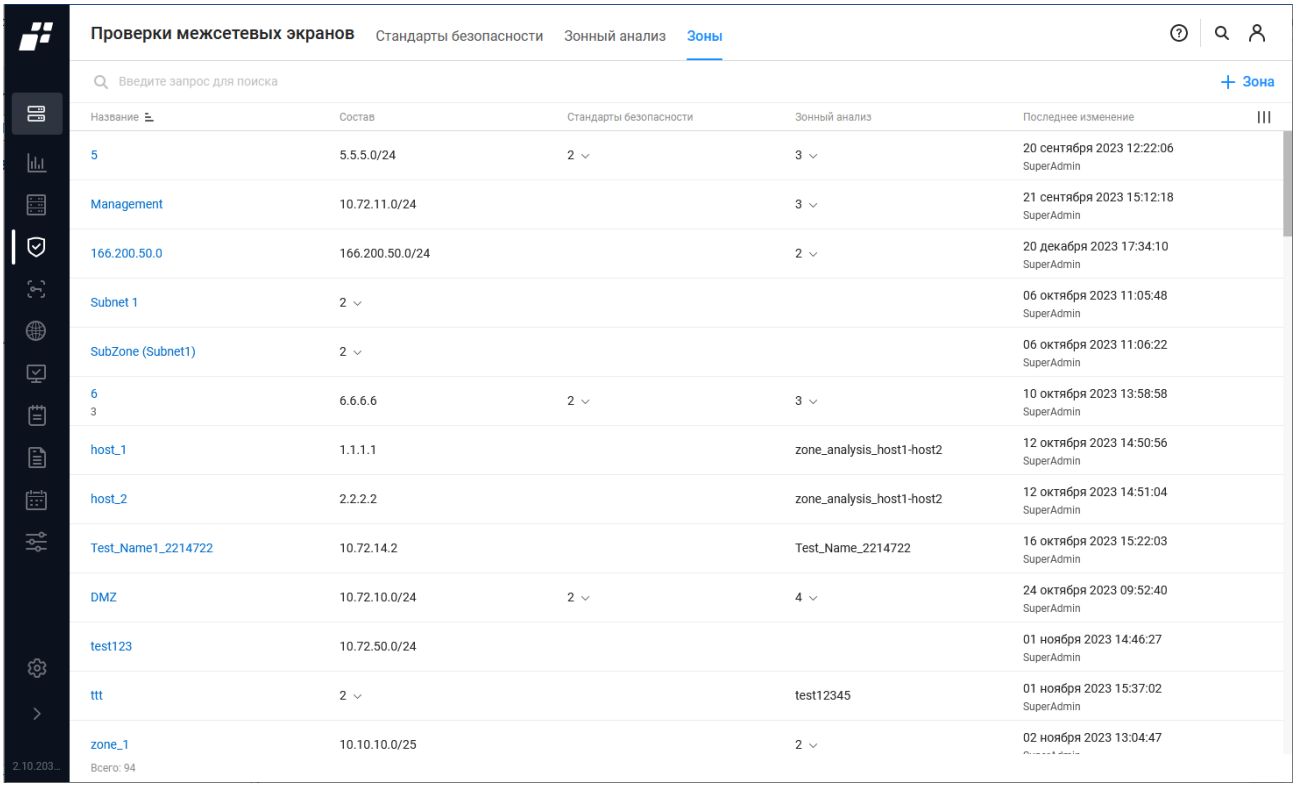


Рисунок 55 – Вкладка «Зоны»

Над списком зон доступны:

- поле поиска (Введите запрос для поиска);
- кнопка «Зона» (+ Зона);
- кнопка «Колонки» ( ).

При наведении курсора на строку с зоной, в правой части строки появятся кнопки:

- «Создать копию» ( );
- «Удалить» ( ).

2.3.3.1. Создание новой зоны

Для добавления новой зоны необходимо выполнить следующие действия:

1) Нажать кнопку «Зона» (+ Зона).
2) Откроется страница «Создание зоны» (рис. 56). Заполнить поля страницы необходимыми параметрами. Состав и описание полей страницы приведены в таблице 16.

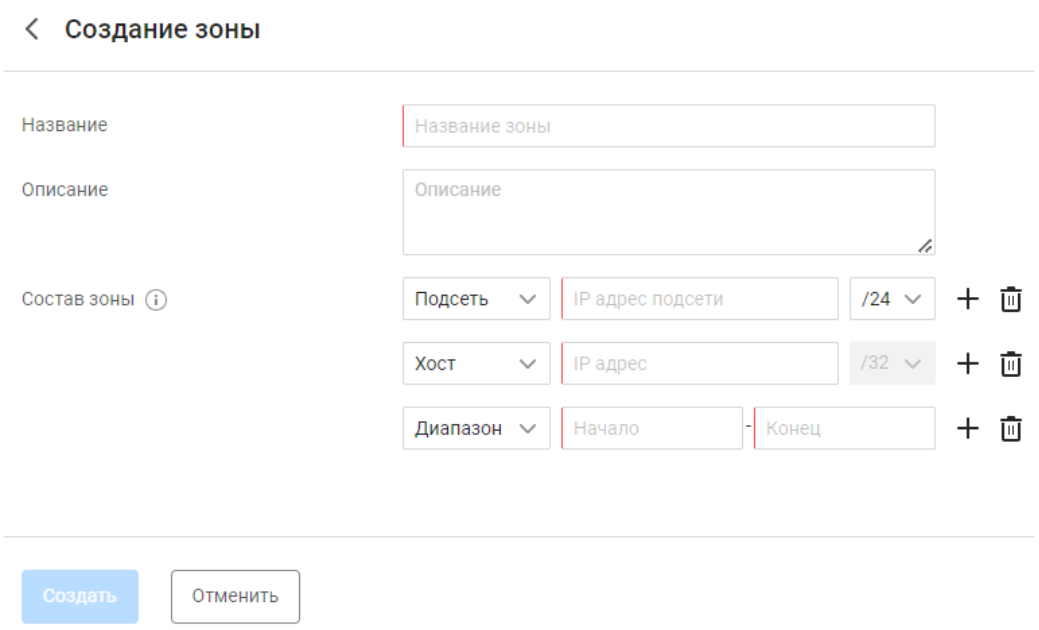


Рисунок 56 – Страница «Создание зоны»

Таблица 16 – Состав и описание полей страницы «Создание зоны»

Поле	Описание
Поле «Название»	Текстовое поле для ввода названия зоны. Параметры ввода текста: от 1 до 250 любых символов
Поле «Описание»	Текстовое поле для ввода описания зоны. Параметры ввода текста: от 1 до 4000 любых символов
Поле «Состав зоны»	Содержит блоки полей для добавления объектов одного из трех типов: — «Подсеть»; — «Хост»; — «Диапазон». Блоки добавляются по нажатию кнопки «Добавить» (+), удаляются – по нажатию кнопки «Удалить» (🗑)
Элементы управления	
Создать	При нажатии на кнопку введенные данные сохраняются
Отменить	При нажатии на кнопку введенные данные не сохраняются

При сохранении данных зоны выполняется проверка на пересечение или выход основных диапазонов на наличие зависимостей в требованиях. Если зона пересекается в стандарте зонного анализа, то отображается сообщение об ошибке.

2.3.3.2. Редактирование зоны

Для перехода на страницу редактирования зоны сети необходимо нажать в списке зон ссылку-название зоны.

На вкладке «Настройки» страницы можно редактировать наименование, описание и состав зоны (рис. 57), на вкладке «Зависимости» – просмотреть список стандартов безопасности и стандартов зонного анализа, где используется редактируемая зона. Название каждого стандарта является ссылкой, при выборе которой открывается страница соответствующего стандарта.

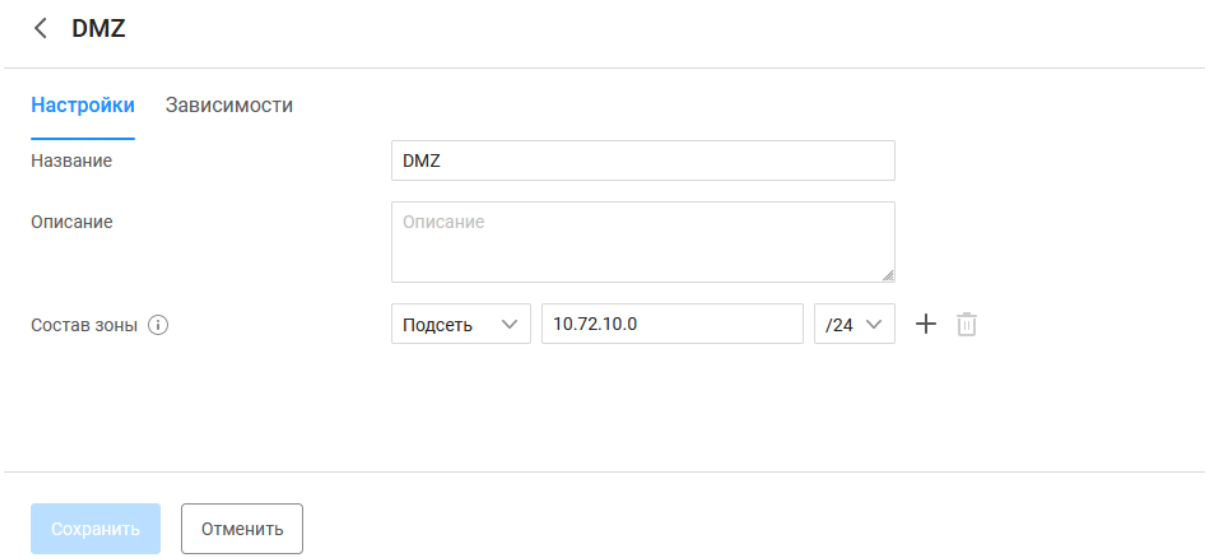


Рисунок 57 – Страница зоны DMZ. Вкладка «Настройки»

При редактировании данных зоны выполняется проверка на пересечение или выход основных диапазонов на наличие зависимостей в требованиях. Если зона:

- участвует в стандартах (стандарты безопасности и/или зонного анализа) в качестве исключений, то изменения сохраняются, правила исключений в стандарте не учитываются;
- пересекается в стандарте зонного анализа, то отображается сообщение об ошибке.

2.4 Профили отчетов

Отображаемые данные и доступная функциональность подраздела «Профили отчетов» зависят от наличия хотя бы одной лицензии на функциональные модули «Efros NA», «Efros FA», «Efros VC» или «Efros ICC».

Подраздел «Профили отчетов» (рис. 58) позволяет пользователю управлять настройками параметров контроля устройств.

Профили отчетов, добавленные в комплекс в результате подключения внешних модулей, доступны только для внесения изменений в части использования отчетов и проверок.

Рабочая область подраздела состоит из следующих элементов:

- дерево профилей отчетов;
- вкладка «Конфигурации»;
- вкладка «Проверки безопасности».

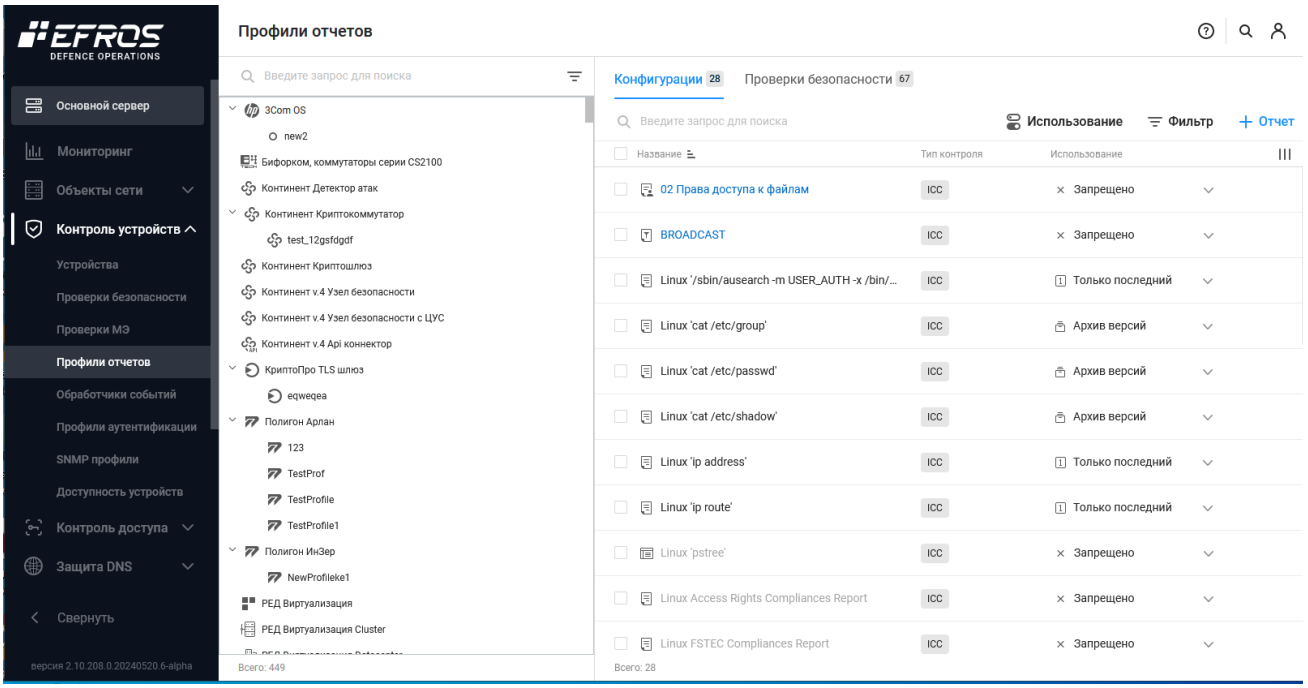


Рисунок 58 – Подраздел «Профили отчетов»

2.4.1. Дерево профилей отчетов

Дерево со списком профилей отчетов сгруппировано по типам устройств. Список профилей отчетов в дереве соответствует внешним модулям, добавленным в комплекс (более подробно о модулях написано в документе «Руководство пользователя. Часть 1. Настройка и администрирование»).

Над деревом доступны следующие элементы:

- поле поиска (Введите запрос для поиска);
- кнопка «Фильтр» ( ).

При наведении курсора на профиль отчетов в его строке отобразится кнопка «Создание профиля отчетов» ( ), которая позволяет создать пользовательский профиль отчетов для выбранного типа устройства.

При наведении курсора на созданный пользовательский профиль отчетов в его строке отобразится 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. При наведении курсора в дереве на строку профиля в строке отобразится кнопка «Удалить» (🗑), на вкладках «Конфигурации» и «Проверки безопасности» такого профиля отчетов не активны кнопки «Использование» (Использование) и «Отчет» (+ Отчет).

2.4.1.1. Создание пользовательского профиля отчетов

Для создания пользовательского профиля отчетов устройства необходимо выполнить следующие действия:

1) Навести курсор на базовый профиль отчетов и нажать на кнопку «Создание профиля отчета» (+).
2) Откроется страница «Создание профиля отчетов» (рис. 59). Заполнить поля страницы необходимыми параметрами. Состав и описание полей страницы приведены в таблице 17.
3) Нажать кнопку «Создать».

Созданный профиль содержит отчеты и проверки родительского профиля. При необходимости можно отредактировать использование отчетов и проверок в колонке «Использование».

На вкладке «Конфигурации» можно добавлять пользовательские отчеты (более подробно о добавлении пользовательских отчетов описано в подпункте 2.4.2.1). На вкладке «Проверки безопасности» добавление пользовательских отчетов типа «Проверки» не доступно, автоматически отображаются проверки из подразделов «Проверки безопасности» и «Проверки МЭ».

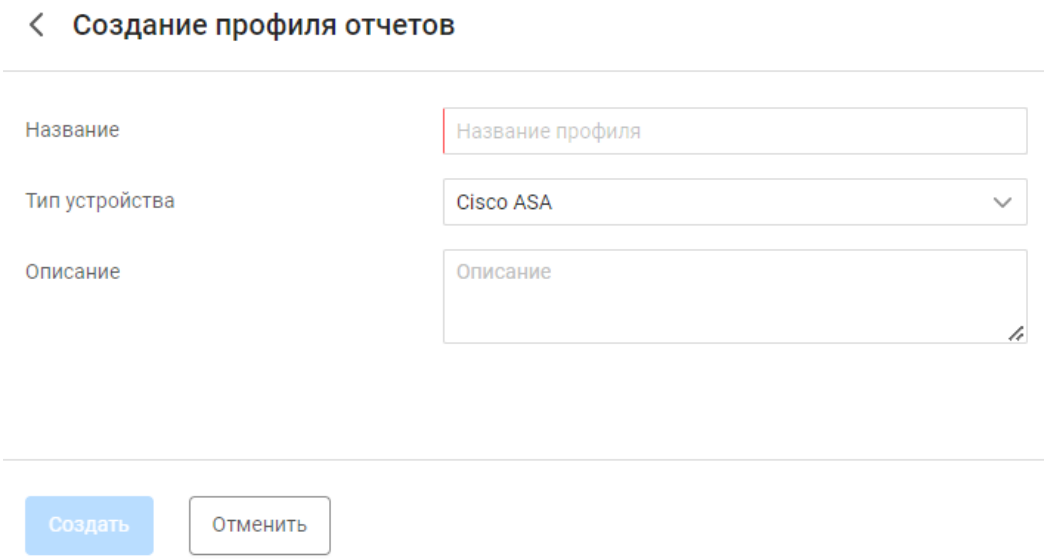


Рисунок 59 – Страница «Создание профиля отчетов»

Таблица 17 – Состав и описание полей страницы «Создание профиля отчетов»

Поле	Описание
Поле «Название»	Текстовое поле для ввода названия профиля отчетов. Параметры ввода текста: от 1 до 250 любых символов
Поле «Тип устройства»	Поле с раскрывающимся списком профилей отчетов
Поле «Описание»	Текстовое поле для ввода описания профиля отчетов. Параметры ввода текста: от 1 до 4000 любых символов
Элементы управления	
Создать	При нажатии на кнопку введенные данные сохраняются
Отменить	При нажатии на кнопку введенные данные не сохраняются

2.4.2. Вкладка «Конфигурации»

Вкладка «Конфигурации» содержит перечень отчетов для выделенного в дереве профиля отчета (базового или созданного пользователем).

Над списком отчетов располагаются:

- поле поиска (Введите запрос для поиска);
- кнопка «Использование» (Использование) для настройки использования профиля отчетов (подробнее см. пункт 2.4.4);
- кнопка «Фильтр» (Фильтр);
- кнопка «Отчет» (+ Отчет).

На вкладке для каждого отчета отображается следующая информация:

- иконка формы отчета:

- «» – 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;
- «» – отчет по объектам МЭ;

— название отчета, для пользовательских отчетов является ссылкой, при нажатии которой открывается страница редактирования параметров отчета;
— тип контроля (тип лицензии, отвечающий за данный отчет);
— тип использования отчета, поле со списком для выбора типа использования отчета (перечень доступных типов использования с их описанием см. в пункте 2.4.4).

При наведении курсора на пользовательский отчет в его строке отобразятся кнопки:

— «Создать копию» () – для создания нового пользовательского на основе соответствующего отчета;
— «Удалить» ().

При наведении курсора на пользовательский отчет типа «Фильтр» в его строке доступна только кнопка «Удалить» ().

Нельзя удалить отчет, предназначенный для контроля файлов на устройстве, в параметрах использования которого установлено «Контроль изменений», а последняя загруженная версия отличается от эталона – на вкладке «Статус» устройства есть сообщение о нарушении целостности такого отчета.

Каждому отчету также соответствует поля для флага. При выборе нескольких отчетов над списком отчетов вкладки отображается поле «Использование» (рис. 60) для групповой настройки использования выбранных отчетов (подробнее см. пункт 2.4.4).

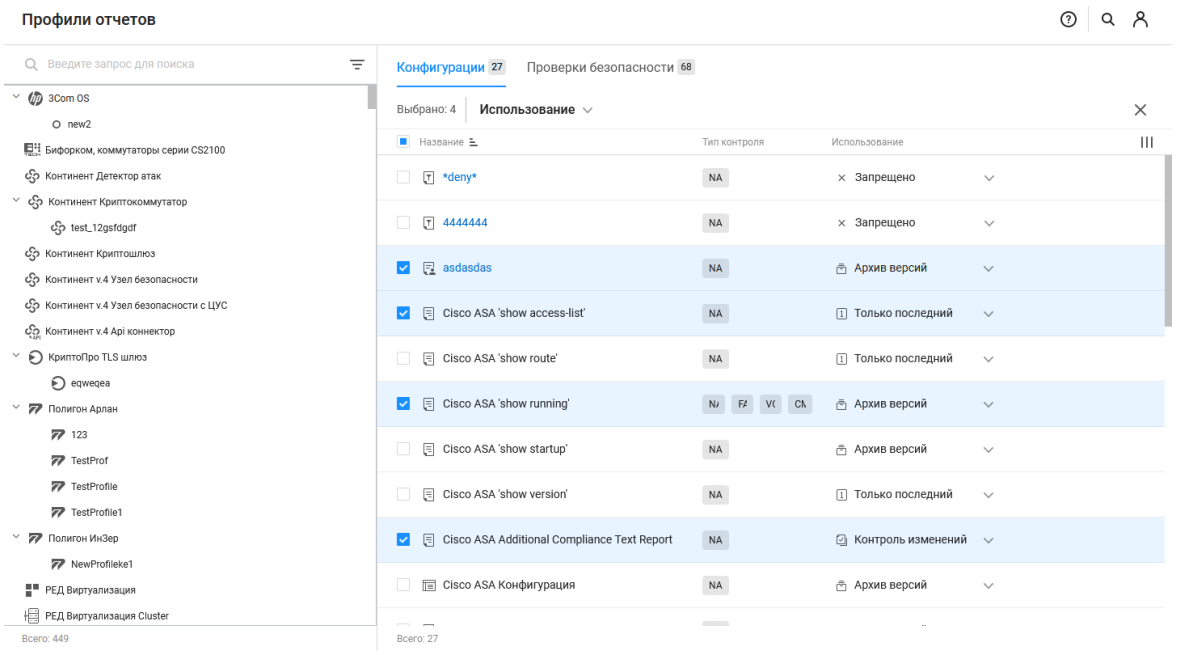


Рисунок 60 – Поле «Использование» в заголовке списка отчетов вкладки «Конфигурации»

2.4.2.1. Создание пользовательского отчета типа «Конфигурации»

Для создания нового (пользовательского) отчета типа «Конфигурации» необходимо выполнить следующие действия:

1) В дереве профилей отчетов выделить необходимый профиль отчета.
2) На вкладке «Конфигурации» в правом верхнем углу нажать кнопку «Отчет» (+ Отчет).
3) Заполнить поля открывшейся страницы «Создание отчета» (рис. 61) необходимыми параметрами в зависимости от вида добавляемого отчета. Состав и описание полей страницы «Создание отчета» приведены в таблице 18.
4) Проверить, при необходимости, корректность введенных параметров нового отчета, для чего:
   - нажать в поле «Тестирование» кнопку «Выбор устройства»;
   - в открывшемся окне установкой курсора в строке списка устройств указать устройство, с которого будет выполняться загрузка нового отчета;
   - нажать кнопку «Сохранить». Начнется процесс загрузки нового отчета с выбранного устройства, на странице добавится поле «Результат» со ссылкой в окно просмотра результата выполнения тестовой загрузки отчета.
5) Нажать кнопку «Создать». Откроется страница подраздела «Профили отчетов», отчет будет добавлен в список отчетов типа «Конфигурации» профиля.

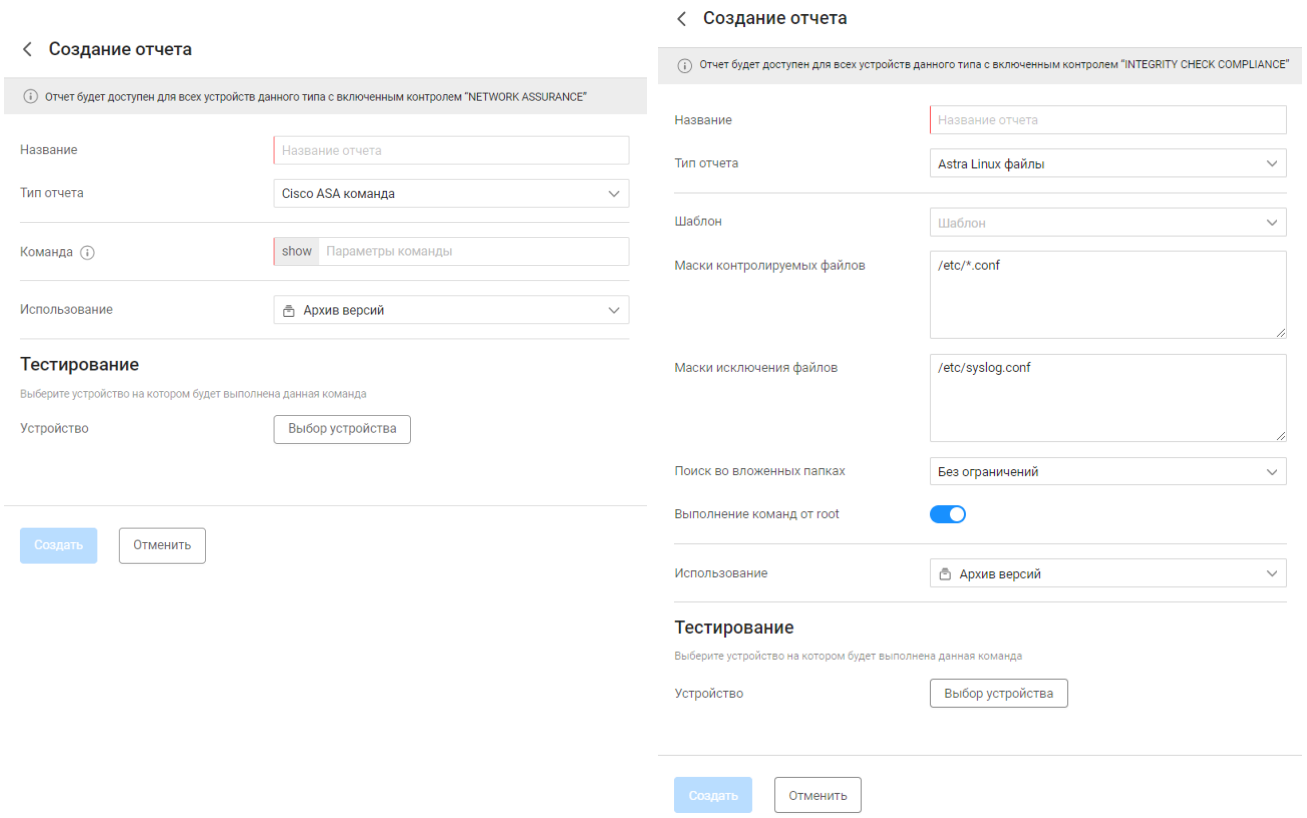


Рисунок 61 – Страница «Создание отчета» для разных типов отчета

Таблица 18 – Состав и описание полей страницы «Создание отчета»

Поле	Описание
Поле «Название»	Текстовое поле для ввода названия отчета. Параметры ввода текста: от 1 до 250 любых символов
Поле «Тип отчета»	Раскрывающийся список с типами профилей
Дополнительные поля	Состав дополнительных полей зависит от выбранного типа отчета. Например: — при создании отчета по контролю целостности (КЦ) для ОС пользователь имеет возможность указать маски для выбора контролируемых файлов и для исключения файлов; — для некоторых типов устройств (ОС, СУБД и др.) в поле «Шаблон» страницы доступны для выбора предустановленные шаблоны со списками файлов, которые необходимо поставить на КЦ; — поле «Команда» содержит поле со списком доступных в зависимости от типа отчета команд и поле для ввода параметра команды. Справа в поле расположена кнопка «Информация» (ⓘ), при нажатии которой открывается подсказка с перечнем доступных команд;

Поле	Описание
	— при включении переключателя «Выполнение команды от root» необходимо использовать для выполнения команд sudo/pfexec
Поле «Использование»	Поле со списком для выбора режима использования отчета (подробнее см. пункт 2.4.4)
Поле «Тестирование»	Позволяет выбрать устройство, на котором будет протестировано выполнение заданной команды. После выбора устройства запускается процесс тестирования, ниже отображается поле «Результат» со ссылкой «Лог операции». При выборе ссылки открывается окно просмотра сообщений в ходе выполнения и результата выполнения тестирования после его завершения
Элементы управления	
Создать	При нажатии на кнопку введенные данные сохраняются
Отменить	При нажатии на кнопку введенные данные не сохраняются

Созданный отчет доступен для:

- редактирования – страница редактирования параметров отчета открывается при нажатии ссылки-наименования отчета в списке отчетов профиля на вкладке «Конфигурации»;
- настройки его использования – выбором требуемого значения в поле колонки «Использование» в списке отчетов профиля на вкладке «Конфигурации» (подробнее см. пункт 2.4.4);
- создания на его основе другого отчета – по нажатию кнопки «Создать копию» ( ) в строке отчета (отображается при наведении курсора на строку отчета);
- удаления – выполняется по нажатию кнопки «Удалить» ( ) в строке отчета (отображается при наведении курсора на строку отчета).

2.4.3. Вкладка «Проверки безопасности»

Вкладка «Проверки безопасности» содержит список проверок, которые связаны с профилем устройства, выбранным в дереве профилей (рис. 62).

Над списком проверок располагаются:

- поле поиска (Введите запрос для поиска);
- кнопка «Использование» (Использование) для настройки использования профиля отчетов (подробнее см. пункт 2.4.4);
- кнопка «Фильтр» (Фильтр).

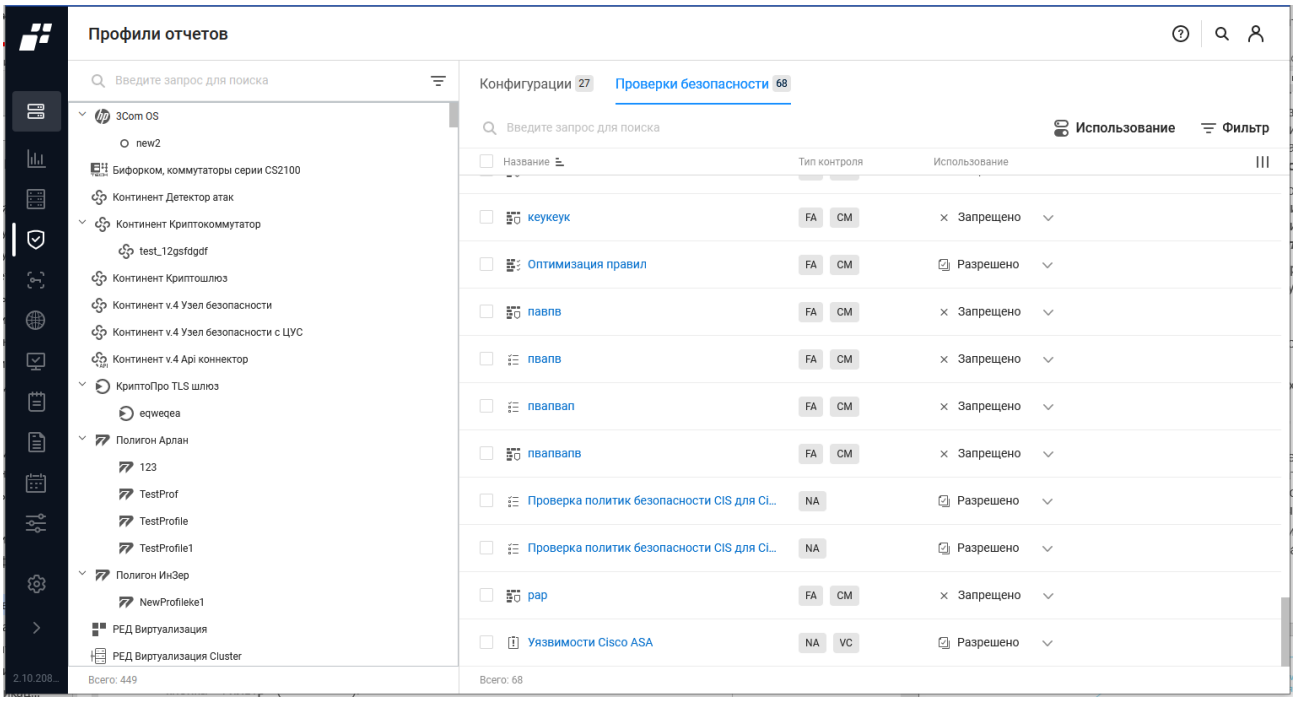


Рисунок 62 – Вкладка «Проверки безопасности»

На вкладке для каждого отчета отображается следующие данные:

- иконка проверки:
  - «» – стандартная проверка;
  - «» – проверка по межсетевым экранам (МЭ);
  - «» – проверка типа «Оптимизация правил»;
  - «» – проверка на уязвимости;
- название проверки, является ссылкой, при нажатии которой открывается страница настройки использования отчета;
- тип контроля (тип лицензии, отвечающий за данный отчет);
- тип использования проверки, поле со списком для выбора типа использования отчета (перечень доступных типов использования с их описанием см. в пункте 2.4.4).

Каждому отчету также соответствует поля для флага. При выборе нескольких отчетов над списком отчетов вкладки отображается поле «Использование» для групповой настройки использования выбранных отчетов (подробнее см. пункт 2.4.4).

Редактирование параметров проверок на вкладке «Проверки безопасности» (кроме типа «Использование») осуществляется в подразделах «Проверки безопасности» (подраздел 2.2) и «Проверки МЭ» (подраздел 2.3).

2.4.4. Настройка использования отчетов для устройств

Для изменения использования одного отчета в профиле отчетов необходимо выполнить следующие действия:

1) В дереве профилей отчетов выделить необходимый профиль отчета и перейти на требуемую вкладку «Конфигурации» или «Проверки безопасности».
2) В строке отчета в поле «Использование» выбрать необходимое значение (на рис. 63 приведен пример настройки для отчета типа «Конфигурации»).

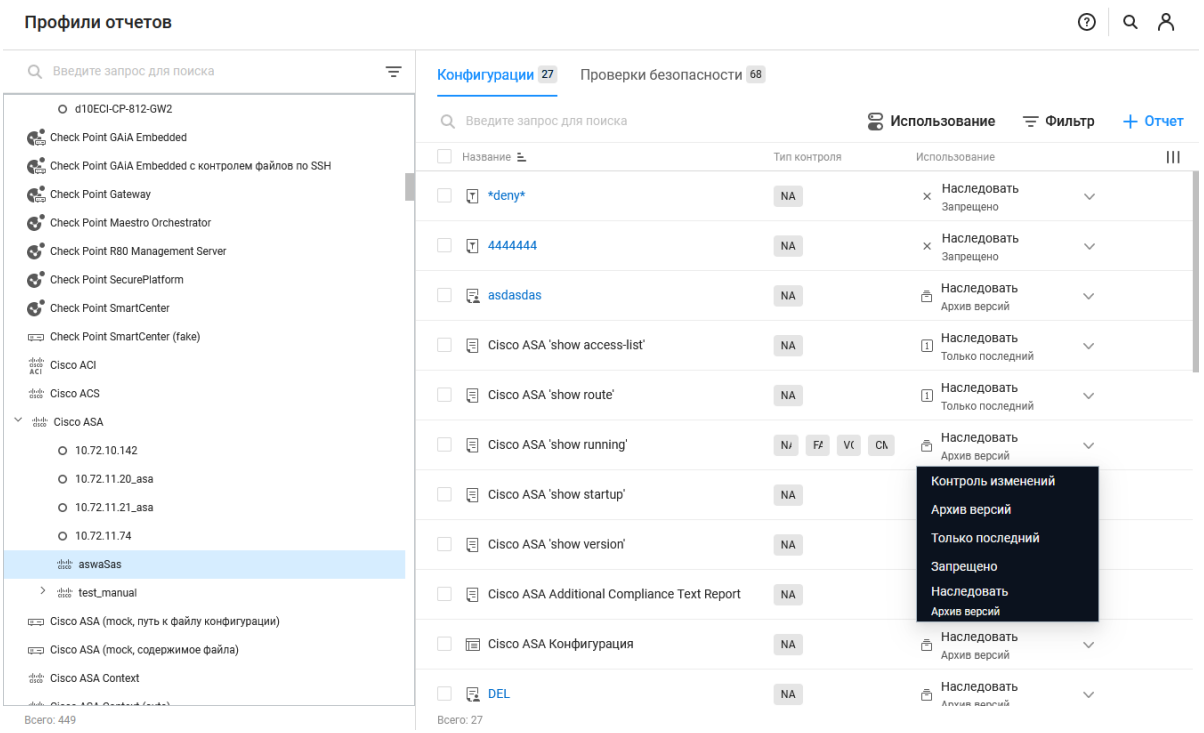


Рисунок 63 – Настройка использования отчета типа «Конфигурации»

3) В колонке «Использование» поменять значение на нужный вариант (перечень возможных значений использования для отчетов типа «Конфигурации» и «Проверки безопасности» приведен в таблице 19). Изменение будет сохранено, отобразится соответствующее сообщение.

Таблица 19 – Перечень возможных значений использования для отчетов типа «Конфигурации» и «Проверки безопасности»

Тип отчета	Возможные значения режима использования отчета
«Конфигурации»	— «Контроль изменений» – вне зависимости от настроек базового профиля будет выполняться контроль целостности загруженного с устройства отчета; — «Архив версий» – в базе данных комплекса будут храниться все измененные версии отчета, загруженного с устройства; — «Только последний» – в базе данных комплекса хранится

Тип отчета	Возможные значения режима использования отчета
	только последняя измененная версия отчета, загруженного с устройства; — «Запрещено» – загрузка отчета с устройств запрещена вне зависимости от настроек базового профиля; — «Наследовать (XXXXXX)» – применить настройки базового профиля. В скобках отображается значение, установленное для отчета в базовом профиле (отображается для пользовательских отчетов)
«Проверки безопасности»	— «Разрешено» – разрешить проверку вне зависимости от настроек базового профиля; — «Запрещено» – запретить проверку вне зависимости от настроек базового профиля

Для внесения изменений в настройки режима использования группы отчетов профиля типа «Конфигурации» или «Проверки безопасности» пользователю необходимо выполнить следующие действия:

1) В дереве профилей отчетов выделить необходимый профиль отчета и перейти на требуемую вкладку «Конфигурации» или «Проверки безопасности».
2) В полях для флага строк требуемых отчетов установить флаг. Для включения в группу всех отчетов вкладки – установить флаг в поле «Название» в заголовке таблицы списка.
3) В отобразившемся над списком отчетов поле «Использование» (на рис. 64 приведен пример настройки использования для группы отчетов типа «Проверки безопасности») выбрать необходимое значение (см. таблицу 19). Изменение будет сохранено, отобразится соответствующее сообщение.

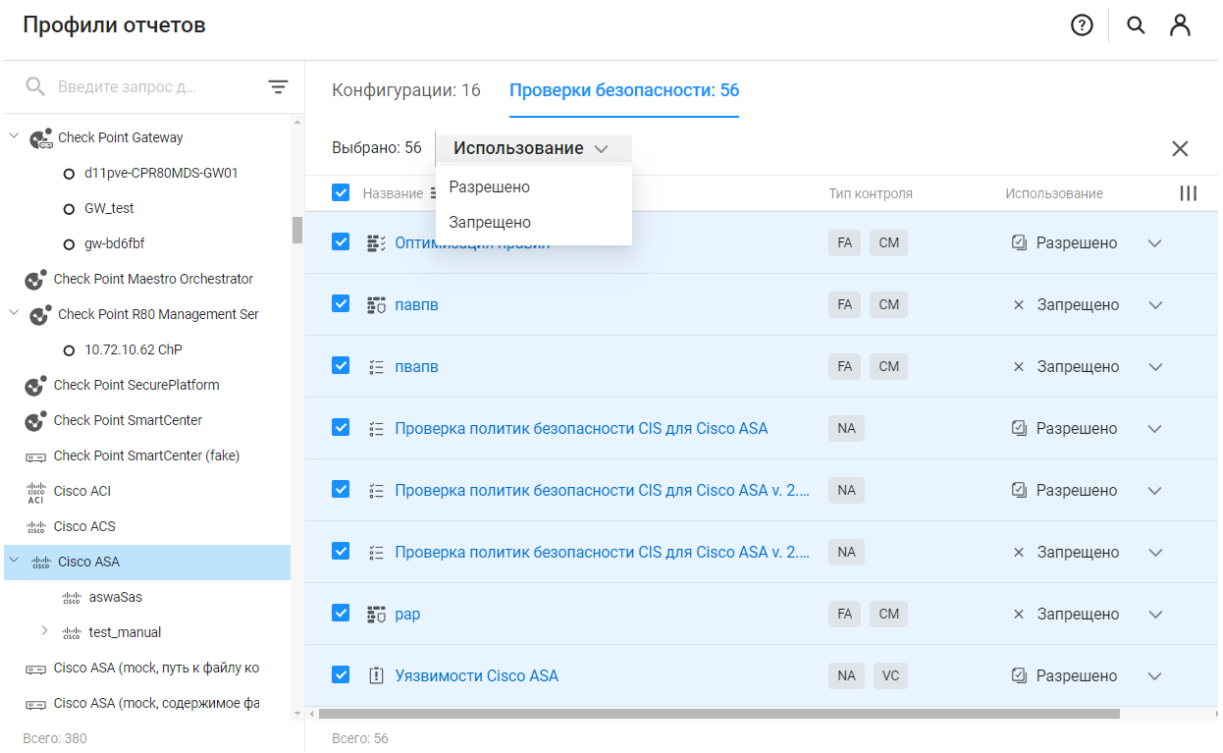


Рисунок 64 – Страница «Профили отчетов» в режиме настройки использования группы отчетов

Для настройки использования профилей отчетов для всех устройств комплекса пользователю необходимо выполнить следующие действия:

1) В дереве профилей отчетов выделить необходимый профиль отчета.
2) На вкладке «Конфигурации» или «Проверки безопасности» нажать над списком отчетов кнопку «Использование» (Использование).
3) В открывшемся окне (рис. 65):

— для настройки каждого устройства отдельно – выбрать в списке поля «Профиль» назначаемый устройству профиль отчетов;

— для настройки группы устройств – выбрать в окне установкой флагов требуемые устройства и выбрать в отобразившемся над списком отчетов поле «Профиль отчетов» назначаемый устройствам профиль отчетов (см. таблицу 19).

Для включения в группу всех устройств – установить флаг в поле «Объект защиты» в заголовке таблицы списка.

4) Нажать кнопку «Сохранить». Окно закроется, внесенные изменения будут сохранены.

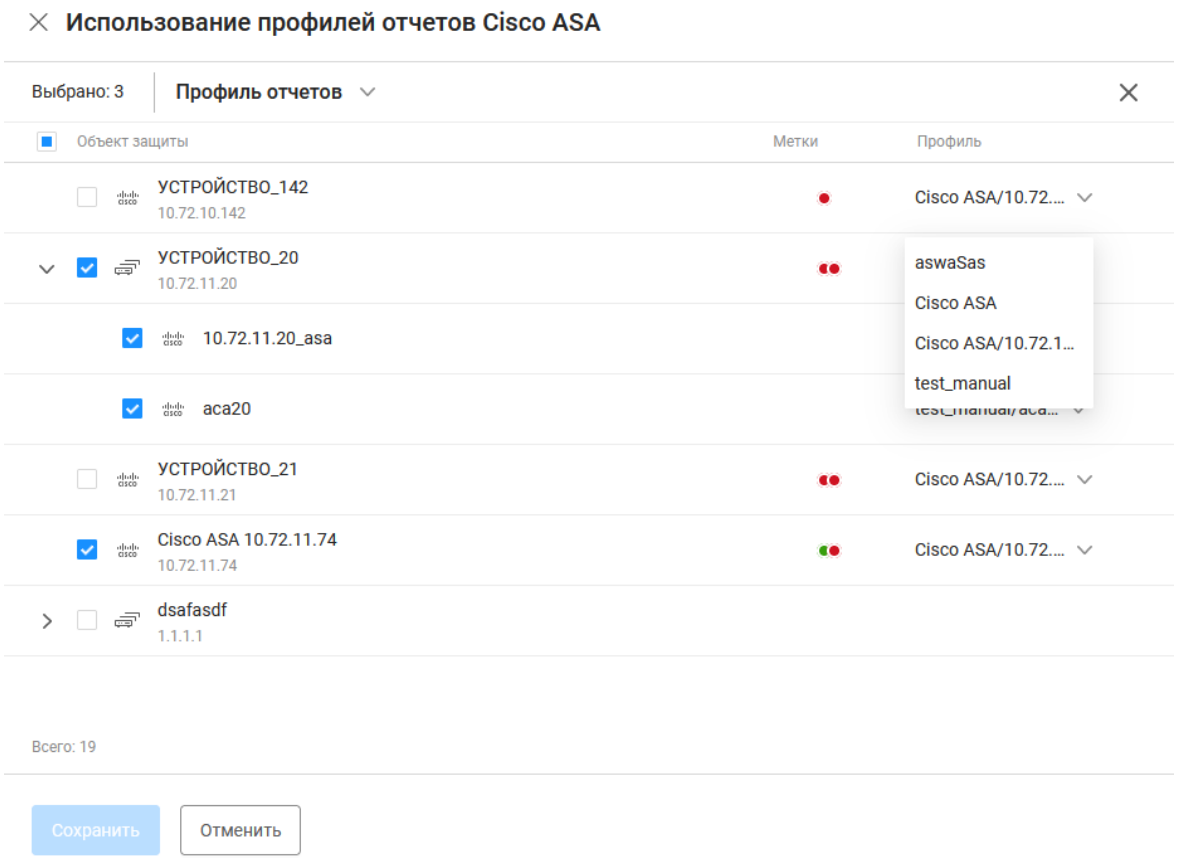


Рисунок 65 – Окно настройки использования профилей отчетов для всех устройств

2.5 Обработчики событий

Отображаемые данные и доступная функциональность подраздела «Обработчики событий» зависят от наличия хотя бы одной лицензии на функциональные модули «Efros NA», «Efros FA», «Efros VC» или «Efros ICC».

Подраздел «Обработчики событий» (рис. 66) позволяет пользователю задать триггеры (условия) для реакции комплекса на события, которые произошли на устройствах или в самом комплексе.

Для каждой записи списка отображаются следующие данные:

- название – наименование и описание обработчика событий. Наименование является ссылкой, при переходе по которой открывается окно для редактирования данных обработчика событий;
- статус – переключатель:
  - « » – обработчик событий активен;
  - « » – обработчик событий неактивен.

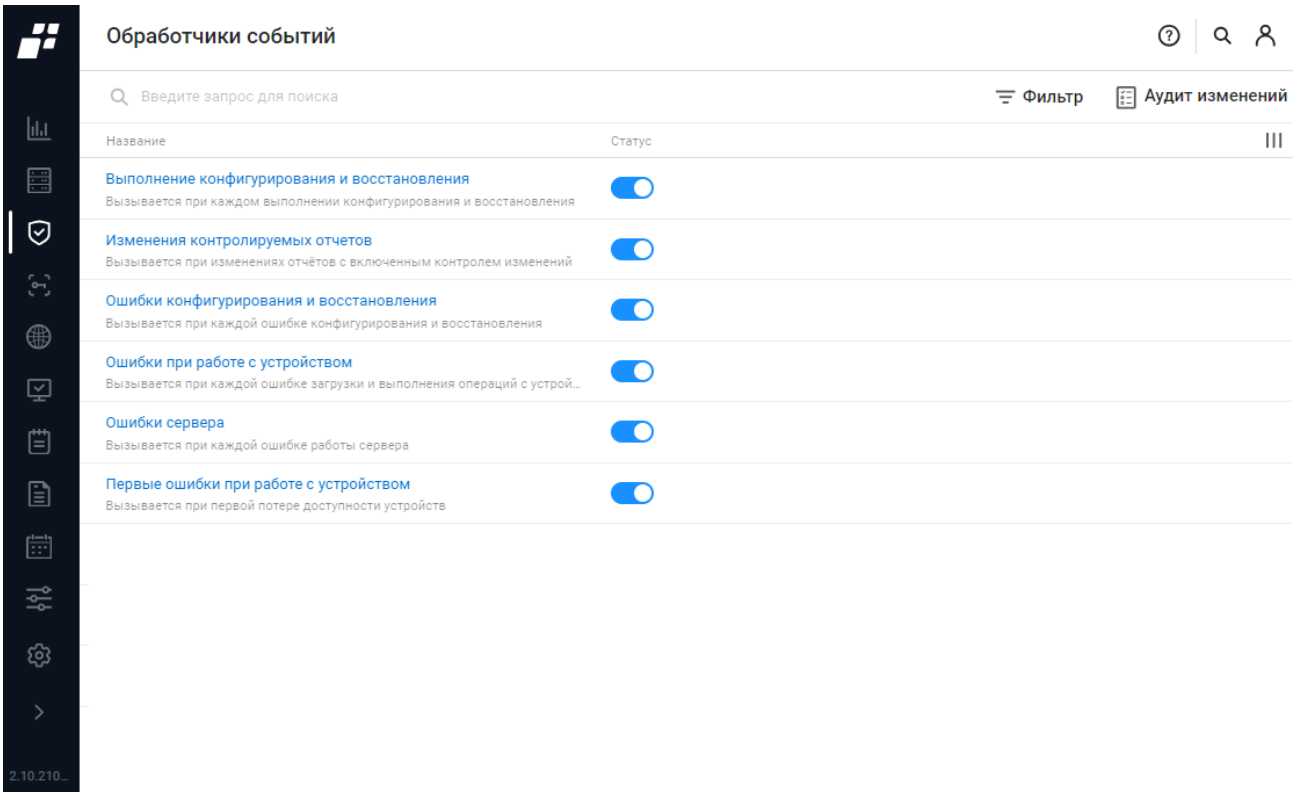


Рисунок 66 – Подраздел «Обработчики событий»

Список обработчиков событий:

- «Выполнение конфигурирования и восстановления»;
- «Изменения контролируемых отчетов»;
- «Ошибки конфигурирования и восстановления»;
- «Ошибки при работе с устройством»;
- «Ошибки сервера»;
- «Первые ошибки при работе с устройством».

Над списком располагаются:

- поле поиска (Введите запрос для поиска);
- кнопка «Фильтр» (Фильтр);
- кнопка «Аудит изменений» (Аудит изменений) для перехода в окно включения/выключения загрузки отчетов при получении событий об изменении конфигурации устройства.

Удаление встроенных обработчиков событий невозможно, но пользователь может редактировать и отключать их. Отключенные обработчики событий отображаются затененными.

2.5.1. Редактирование обработчика событий

Для редактирования обработчика событий необходимо выполнить следующие действия:

1) Выбрать обработчик событий, который требуется отредактировать. Нажать на имя обработчика. Откроется страница редактирования обработчика (рис. 67). Состав и описание полей страницы приведены в таблице 20.

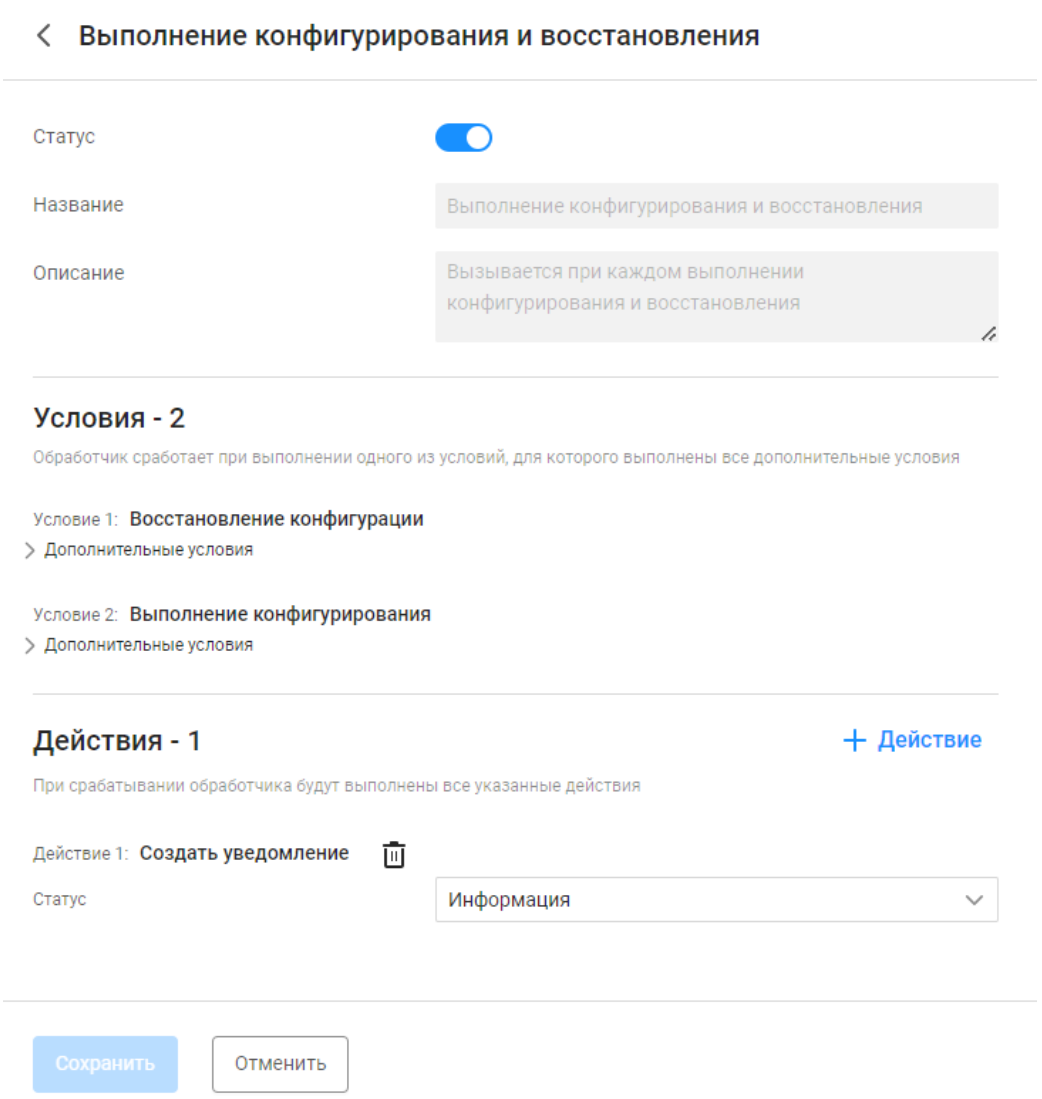


Рисунок 67 – Страница редактирования обработчика

Таблица 20 – Состав и описание страницы редактирования обработчика

Поле	Описание
Поле «Статус»	При включенном переключателе осуществляется обработка событий, при выключенном – триггер выключен
*Поле «Название»	Название обработчика
*Поле «Описание»	Описание обработчика

Поле	Описание
*Поле «Условия»	Условия выполнения правил обработки событий. Доступны только для просмотра
Поле «Действия»	Выбор типа выполняемого действия через кнопку «Действие» (+ Действие). Перечень действий для обработчиков событий зависит от состава включенных модулей комплекса, может содержать, например, действия: — «Выполнить операцию ‘Проверить соединение‘«; — «Загрузить отчеты»; — «Отправить Syslog сообщение»; — «Отправить сообщение через Exchange»; — «Создать уведомление»
Элементы управления	
Создать	При нажатии на кнопку введенные данные сохраняются
Отменить	При нажатии на кнопку введенные данные не сохраняются
*поля недоступны для редактирования	

2) Для включения или выключения обработчика включить/выключить переключатель «Статус».
3) Просмотреть заданные условия выполнения правил обработки событий.
4) Добавить новые действия в области «Действия». Для добавления одного действия:

— нажать кнопку «Действие» (+ Действие);
— из раскрывающегося списка выбрать тип действия, которое будет выполнено в комплексе в ответ на произошедшее событие (рис. 68);
— задать для него дополнительные параметры (см. ниже).

5) Удалить неактуальные действия. Для удаления одного действия нажать соответствующую ему кнопку «Удалить» ( ).
6) Нажать кнопку «Сохранить». Произойдет возврат в форму настройки обработки событий, внесенные изменения будут сохранены.

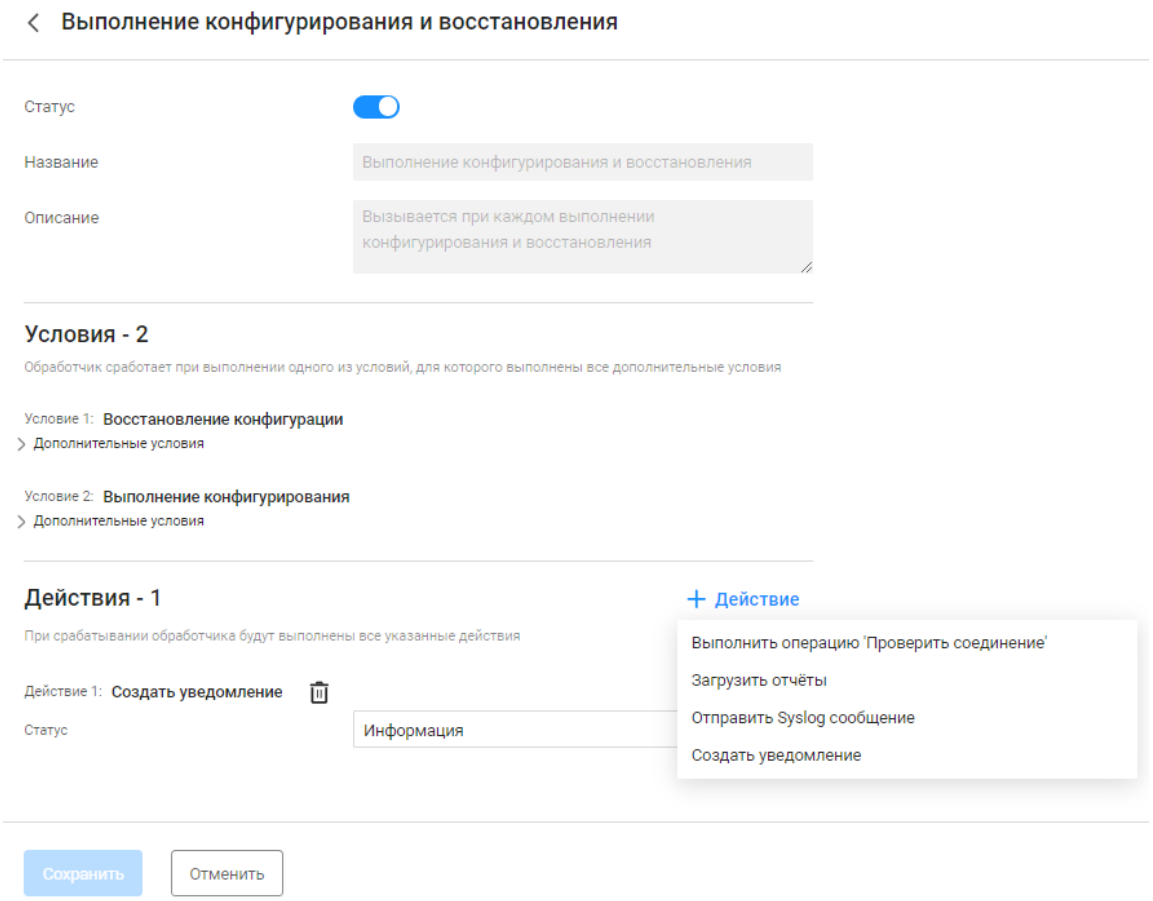


Рисунок 68 – Добавление действий для обработчика событий

Для настройки выполнения действия необходимо после выбора в перечислении 4 соответствующего действия:

— «Проверить соединение» или «Загрузить отчеты» – проставить флаг в строке требуемого типа действия «на источнике события» или «на устройствах». При выборе типа выполнения действия «на устройствах», установить курсор в поле «Выберите устройства» и выбрать установкой флагов в раскрывшемся списке устройств комплекса требуемые устройства/группы устройств (рис. 69);

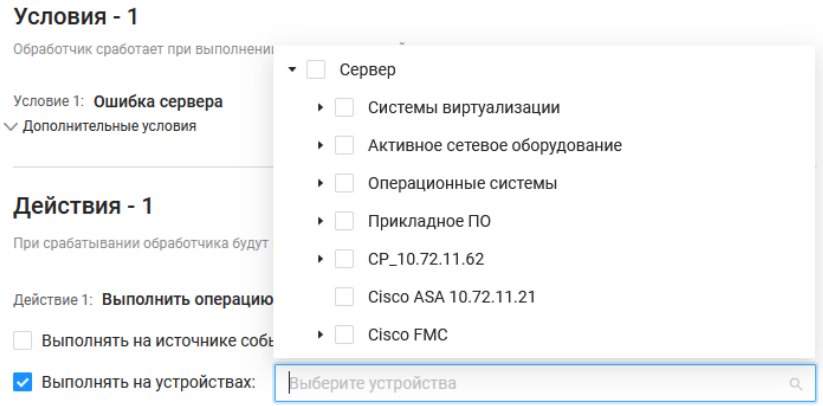


Рисунок 69 – Параметры выполнения операции «Проверить соединение»

— «Отправить Syslog сообщение» – ввести данные Syslog сервера, выбрать в поле «Важность» категорию сообщения и, при необходимости, включить переключатель «Добавить в сообщение IP-адрес и имя устройства» (рис. 70);

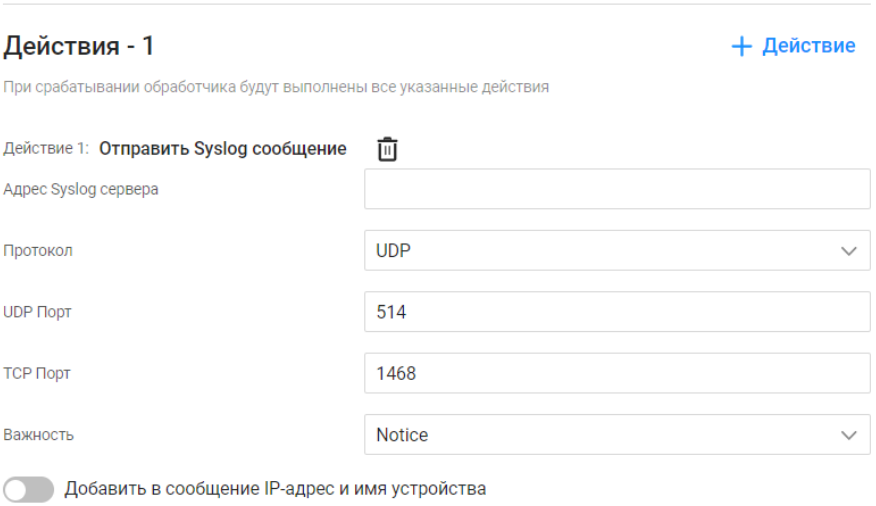


Рисунок 70 – Параметры отправки Syslog сообщения

— «Отправить сообщение через Exchange» – ввести в поле «Получатели» список электронных адресов получателей сообщения (рис. 71);

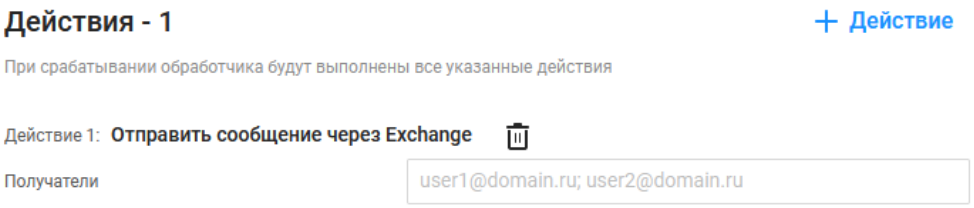


Рисунок 71 – Параметры отправки сообщения через Exchange

— «Создать уведомление» – выбрать в поле «Статус» статус уведомления (рис. 72).

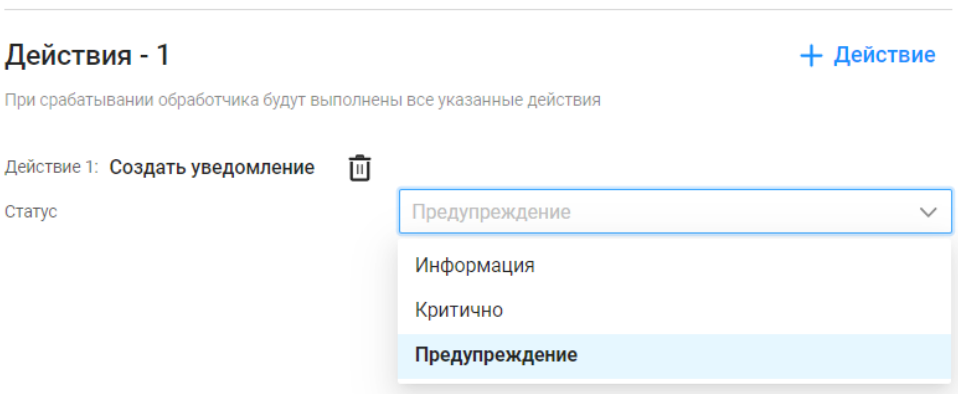


Рисунок 72 – Параметры создания уведомления

2.6 Профили аутентификации

Отображаемые данные и доступная функциональность подраздела «Профили аутентификации» зависят от наличия хотя бы одной лицензии на функциональные модули »Efros NA», «Efros FA», «Efros VC» или «Efros ICC».

Подраздел «Профили аутентификации» (рис. 73) позволяет настроить параметры аутентификации пользователей на оборудовании.

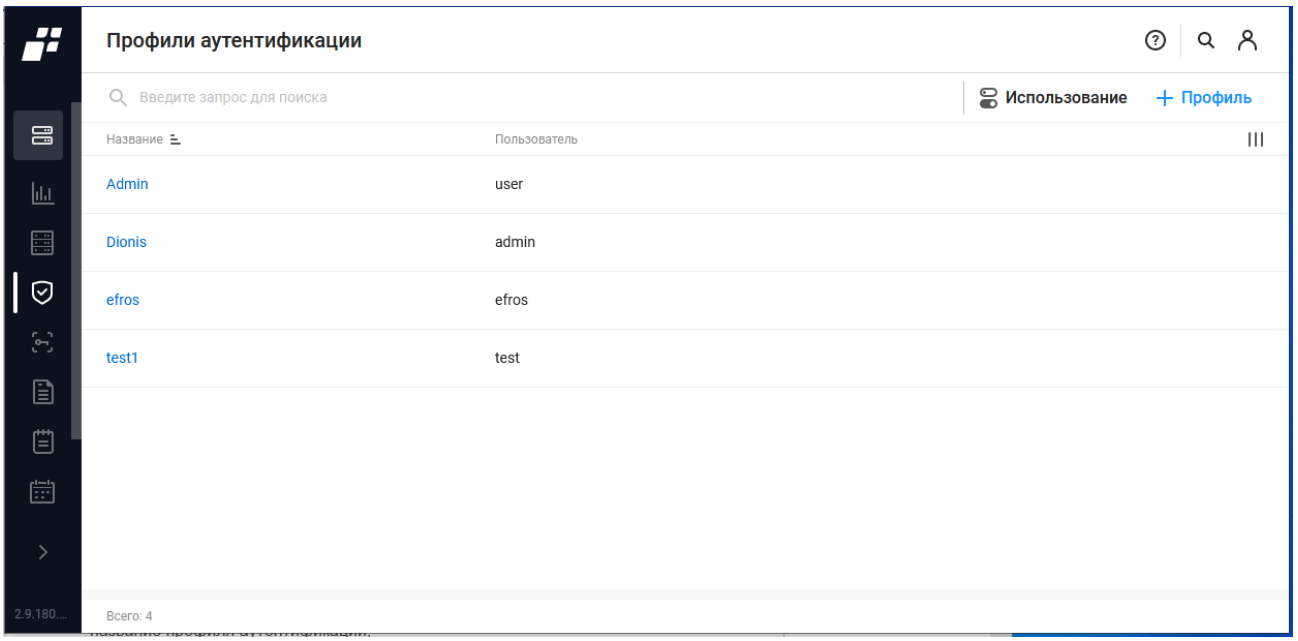


Рисунок 73 – Подраздел «Профили аутентификации»

Над списком профилей располагаются:

- поле поиска (Введите запрос для поиска);
- кнопка «Использование» (Использование) для перехода в окно просмотра и настройки использования профиля аутентификации (см. пункт 2.6.2);
- кнопка «Профиль» (+ Профиль) для перехода на страницу создания нового профиля аутентификации (см. пункт 2.6.1).

Для каждой записи списка отображаются следующие данные:

- название профиля аутентификации, является ссылкой, при нажатии которой открывается страница редактирования параметров профиля аутентификации;
- пользователь – логин, под которым происходит подключение пользователя к устройству для внесения изменений в настройки устройства.

При наведении курсора на профиль аутентификации, появляется кнопка «Удалить» ( ) для удаления профиля аутентификации.

2.6.1. Создание профиля аутентификации

Для создания нового профиля аутентификации необходимо выполнить следующие действия:

1) Нажать кнопку «Профиль» (+ Профиль).
2) На открывшейся странице «Создание профиля аутентификации» (рис. 74) заполнить поля страницы необходимыми параметрами. Состав и описание полей страницы приведены в таблице 21.
3) Нажать кнопку «Создать».

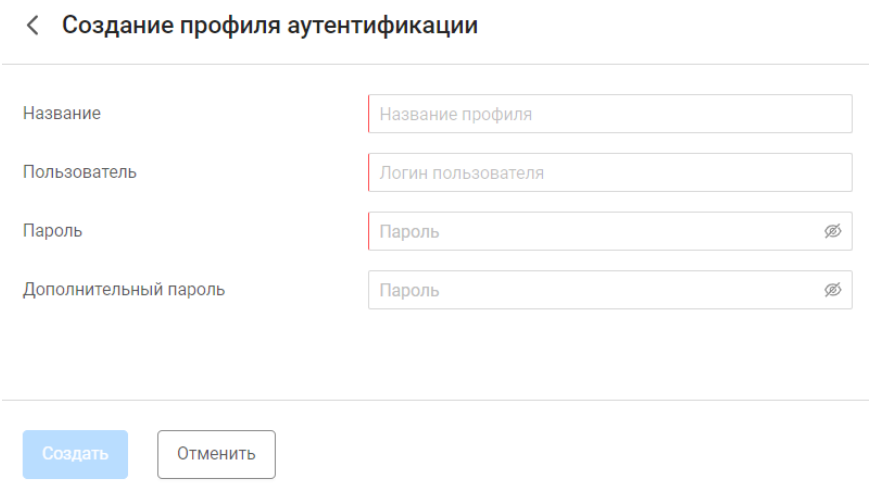


Рисунок 74 – Страница «Создание профиля аутентификации»

Таблица 21 – Состав и описание полей страницы «Создание профиля аутентификации»

Поле	Описание
Поле «Название»	Текстовое поле для ввода названия профиля аутентификации. Параметры ввода текста: от 1 до 250 любых символов
Поле «Пользователь»	Указать пользователя, от имени которого будет происходить авторизация на контролируемых комплексом устройствах. Форматы ввода: — логин; — домен\логин; логин@домен (в формате UPN)
Поле «Пароль»	Указать пароль, под которым будет происходить авторизация на контролируемых комплексом устройствах. Для просмотра введенного пароля – воспользоваться кнопкой «⌀» в правой части поля
Поле «Дополнительный пароль»	Ввести дополнительный пароль для привилегированного режима. Для просмотра введенного пароля – воспользоваться кнопкой «⌀» в правой части поля

Поле	Описание
Элементы управления	
Создать	При нажатии на кнопку введенные данные сохраняются
Отменить	При нажатии на кнопку введенные данные не сохраняются

2.6.2. Настройки использования профиля аутентификации

Для настройки использования профиля аутентификации необходимо выполнить следующие действия:

1) Нажать на странице со списком профилей кнопку «Использование» (Использование). Откроется окно «Использование “Профили аутентификации”» (рис. 75, таблица 22).

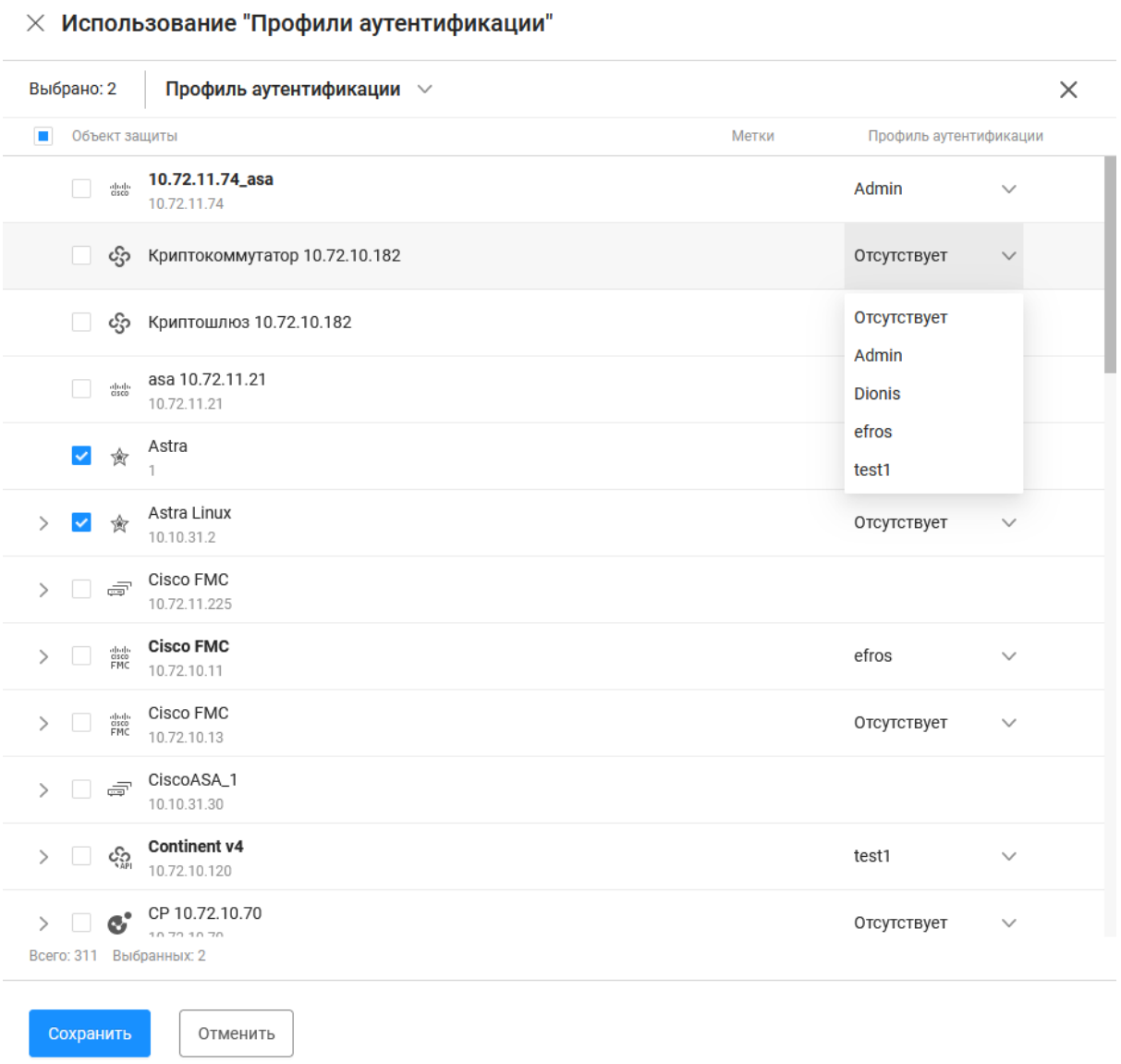


Рисунок 75 – Окно «Использование “Профили аутентификации”»

Таблица 22 – Состав и описание полей окна «Использование «Профили аутентификации»

Поле	Описание
Поле для флага	Для выбора устройства
Поле «Объект защиты»	Список доступных устройств в комплексе. Для выбора устройства необходимо поставить флаг в поле для флага
Поле «Метки»	Особые метки пользователей комплекса
Поле «Профиль аутентификации»	Раскрывающийся список существующих профилей аутентификации. Изначально профиль не назначен, в поле отображается значение «Отсутствует»
Элементы управления	
Поле поиска	Для ввода последовательности символов из искомой записи
Кнопка «Фильтр»	Для фильтрации списка профилей аутентификации
Сохранить	При нажатии кнопки выполняется сохранение настроек
Отменить	При нажатии кнопки выполняется переход на страницу списка профилей аутентификации

2) В окне «Использование «Профили аутентификации»:
— для настройки каждого устройства отдельно – выбрать в списке поля «Профиль аутентификации» назначаемый устройству профиль аутентификации;
— для настройки группы устройств – выбрать в окне установкой флагов требуемые устройства и выбрать в отобразившемся над списком устройств поле «Профиль аутентификации» назначаемый устройствам профиль аутентификации.

Для включения в группу всех устройств – установить флаг в поле «Объект защиты» в заголовке таблицы списка.

3) Нажать кнопку «Сохранить». Окно закроется, внесенные изменения будут сохранены.

2.7 Доступность устройств

Отображаемые данные и доступная функциональность подраздела «Доступность устройств» зависят от наличия хотя бы одной лицензии на модули »Efros NA», «Efros FA», «Efros VC» или «Efros ICC».

Подраздел «Доступность устройств» (рис. 76) позволяет пользователю включать (отключать) функции проверки доступности устройств с указанием интервала в минутах.

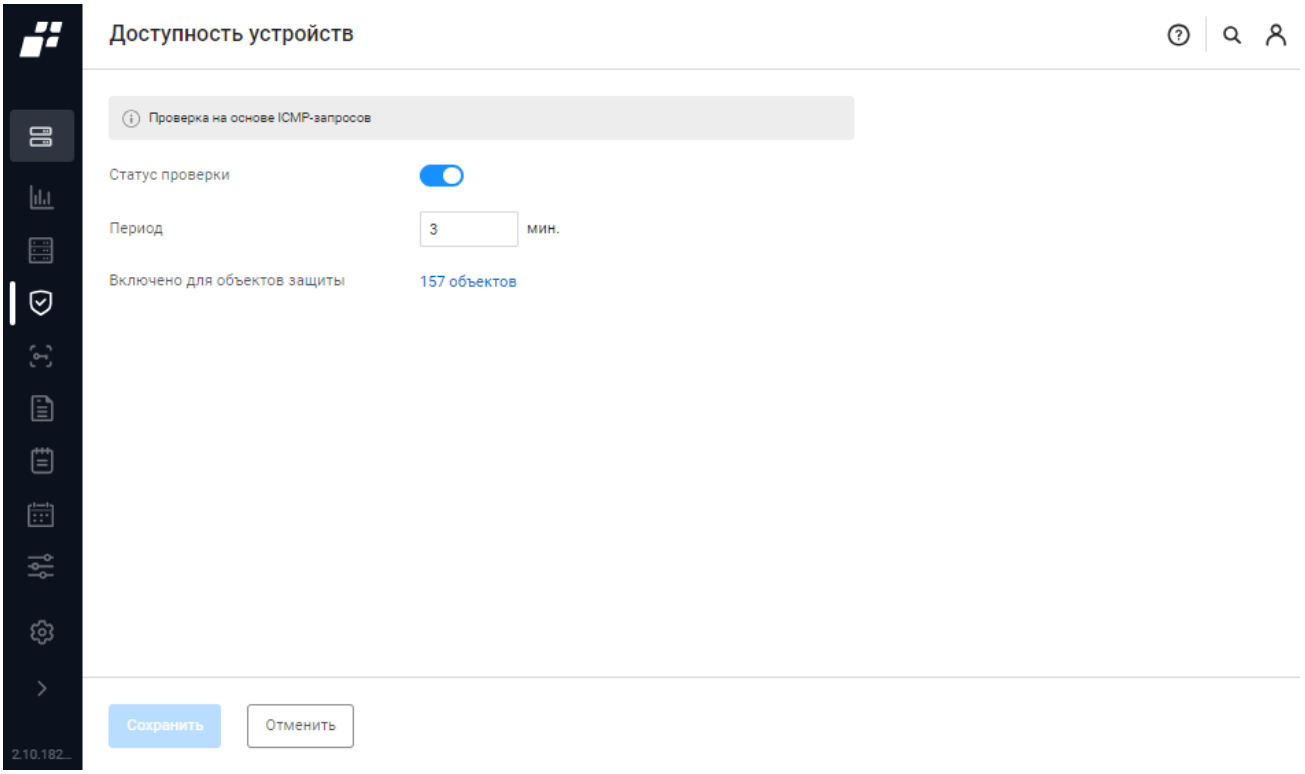


Рисунок 76 – Подраздел «Доступность устройств»

Доступность устройств проверяется с помощью ICMP-запросов и учитывает последние данные о работе с устройством в комплексе (подключение и задачи по выбранным протоколам). Состав и описание полей подраздела «Доступность устройств» приведены в таблице 23.

Таблица 23 – Состав и описание полей страницы подраздела «Доступность устройств»

Поле	Описание
Поле «Статус проверки»	Содержит переключатель с двумя положениями: — «Активен» ( ) – функция проверки доступности устройства включена; — «Неактивен» ( ) – функция проверки доступности устройства выключена
Поле «Период»	Циклический временной промежуток проверки доступности устройств
Поле «Включено для объектов защиты»	Ссылка, показывающая количество устройств, на которых включена проверка доступности. При нажатии на ссылку открывается окно включения/отключения проверки доступности устройств, контролируемых комплексом

2.7.1. Настройка проверки доступности устройств

Для настройки проверки доступности устройств необходимо выполнить следующие действия:

1) Нажать на странице подраздела «Доступность устройств» ссылку в поле «Включено для объектов защиты».
2) В открывшемся окне «Проверка доступности на устройствах» (рис. 77):

— для настройки каждого устройства отдельно – выбрать в поле «Состояние» требуемое положение переключателя «Отключено» или «Включено»;

— для настройки группы устройств – выбрать в окне установкой флагов требуемые устройства и выбрать в отобразившемся над списком устройств поле «Использование» требуемую настройку проверки доступности устройств «Включено» или «Отключено».

Для включения в группу всех устройств – установить флаг в поле «Объект защиты» в заголовке таблицы списка.

3) Нажать кнопку «Сохранить». Окно закроется, внесенные изменения будут сохранены, в поле «Включено для объектов защиты» изменится количество, на которых включена проверка доступности.

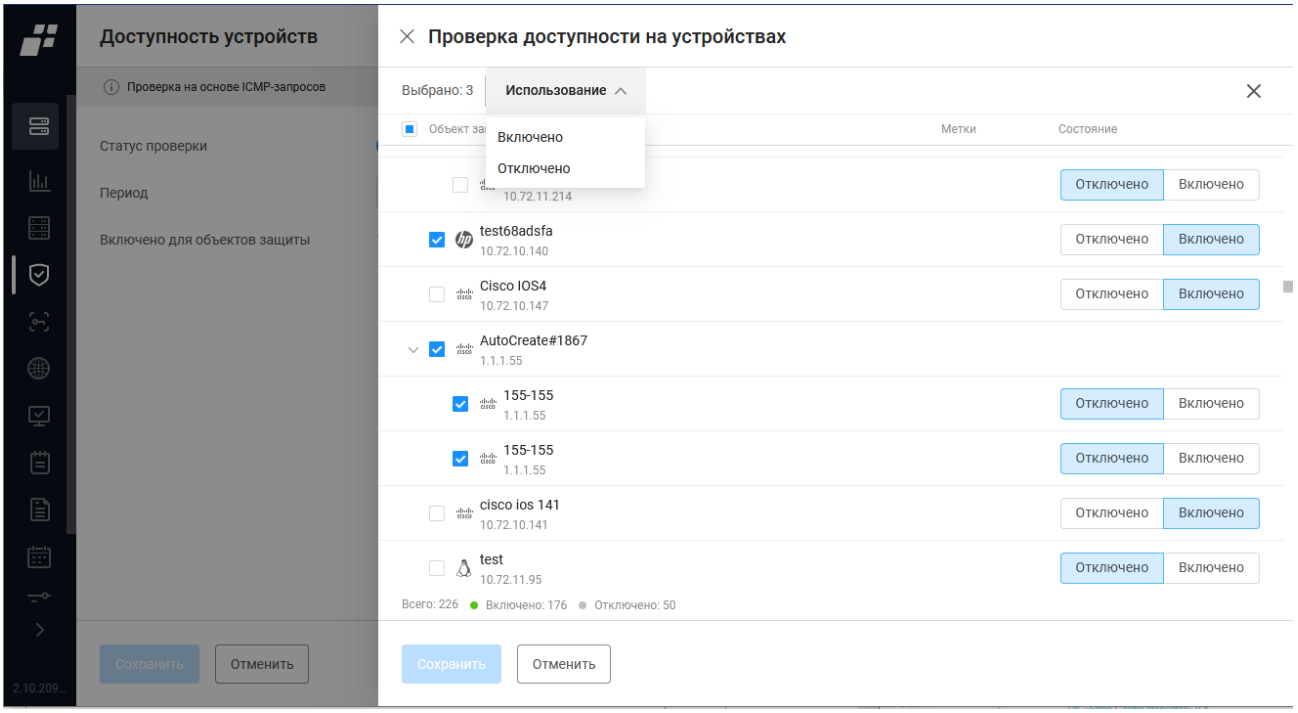


Рисунок 77 – Окно «Проверка доступности на устройствах»

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

Рекомендуемая последовательности работы для настройки возможностей контроля целостности функционального модуля «Efros Integrity Check Compliance» («Efros ICC») приведена в документе «Руководство пользователя. Часть 3. Контроль устройств. Приложение А. Настройка возможностей контроля целостности функционального модуля «Efros ICC».

Приложение Б
Регулярные выражения стандарта PCRE, допустимые к применению в ПК «Efros DO»

Регулярные выражения – формальный язык поиска и осуществления манипуляций с подстроками в тексте, основанный на использовании метасимволов. Для поиска используется строка-образец, состоящая из символов и метасимволов и задающая правило поиска (см. таблицу 24).

Таблица 24 – Пример поиска символов

Символ	Описание	Пример	Соответствие
Обычный	Все символы, кроме специальных, соответствуют сами себе	а	М**а**м**а** мыл**а** р**а**му
		от	**от** к**от**а
		12	(8**12**) 3**12**-24-67

Большинство символов в регулярном выражении представляют сами себя за исключением специальных символов [ ] { } ( ) \ | . ? * $ ^ + (см. таблицу 25).
Для того, чтобы использовать эти символы в качестве текста, их необходимо экранировать символом «\» (обратная косая черта).

Таблица 25 – Примеры использования специальных символов

Символ	Описание	Пример	Соответствие
^	Начало строки	^a	**а**аа ааа
$	Конец строки	а$	ааа аа**а**
\b	Граница слова	\ba	**а**аа **а**аа
		a\b	аа**а** аа**а**
\B	Не граница слова	\Ba\B	а**а**а а**а**а
\G	Предыдущий успешный поиск	\Ga	**ааа** ааа (поиск остановился на четвертой позиции – там, где не нашлось а)
		\Gаха-	**аха-аха-**аха последнее «аха» не будет захвачено, т.к. успешный поиск состоит из «аха-»
.	Любой символ, кроме символа новой строки \n	к.т	**кот**, **кит**, **кат**ок

Также, вместо символа «.» можно использовать **[\s\S]** – это все пробельные и непробельные символы, включая символ новой строки «\n».

Б.1 Символьные классы

Набор символов в квадратных скобках [ ], позволяет указывать, что на данном месте в строке может стоять один из перечисленных символов (см. таблицу 26). Например, **[абв]** задаёт возможность появления в тексте одного из трёх указанных символов, а **[1234567890]** задает соответствие одной из цифр. Также возможно указание диапазона символов, **[А-Яа-я]** соответствует всем буквам русского алфавита, за исключением **ё** и **Ё**. Если требуется указать символы, которые не входят в набор, то используется символ «^» внутри квадратных скобок. Например, **[^0-9]** означает любой символ кроме цифр.
Некоторые символьные классы можно заменить специальными метасимволами:

Таблица 26 – Регулярные выражения с использованием квадратных скобок

Символ	Эквивалент	Соответствие
\d	[0-9]	Цифровой символ
\D	[^0-9]	Не цифровой символ
\s	[\f\n\r\t\v]	Пробельный символ
\S	[^ \f\n\r\t\v]	Непробельный символ
\w	[[:word:]]	Буквенный или цифровой символ или знак подчеркивания
\W	[^[:word:]]	Любой символ, кроме буквенного или цифрового символа или знака подчеркивания

Обозначения пробельных символов:

1. **\f** – разрыв страницы
2. **\n** – перевод строки
3. **\r** – возврат каретки
4. **\t** – горизонтальная табуляция
5. **\v** – вертикальная табуляция

Б.2 Квантификация (поиск последовательностей)

Квантификатор после символа, символьного класса или группы определяет, сколько раз предшествующее выражение может встречаться (см. таблицу 27). Следует учитывать, что квантификатор может относиться более чем к одному символу в регулярном выражении только, если это символьный класс или группа.

Таблица 27 – Примеры использования квантификаторов

Символ	Описание	Пример	Соответствие
*	Ноль или более. Эквивалент {0,}	сто*	**сто**, **стоо**, **стооо**, **ст**
+	Один или более раз. Эквивалентно {1,}	сто+	**сто**, **стоо**, **стооо**, ст
?	Ноль или одно. Эквивалент {0,1}	сто?	**сто**, **стоо**, **стооо**, **ст**
{n}	Ровно n раз	сто{3}	сто, стоо, **стооо**

Символ	Описание	Пример	Соответствие
{m,n}	От m до n включительно	сто{2,3}	сто, **стоо**, **стооо**, стоооо
{m,}	Не менее m	сто{2,}	сто, **стоо**, **стооо**, **стоооо**
{,n}	Не более n	сто{,3}	**сто**, **стоо**, **стооо**, стоооо

Если символы в скобках не образуют квантификатора, их специальное значение игнорируется.
Часто используется последовательность «.*» (точка, звездочка) или «.*?» (точка, звездочка, вопросительный знак) для обозначения любого количества любых символов между двумя частями регулярного выражения (подробнее см. ниже в подразделе Б.3).

Б.3 Жадная и ленивая квантификация

В некоторых реализациях квантификаторам в регулярных выражениях соответствует максимально длинная строка из возможных. Это может оказаться значительной проблемой. Например, часто ожидают, что выражение **(<.*>)** найдёт в тексте теги HTML. Однако, если в тексте есть более одного HTML-тега, то этому выражению соответствует целиком строка, содержащая множество тегов.
** Текст** для примера, **** «жадной» **** и «ленивой» квантификации ** **
Эту проблему можно решить двумя способами.
Учитывать символы, не соответствующие желаемому образцу (**<[^>]*>** для вышеописанного случая).
Определить квантификатор как «ленивый» – большинство реализаций позволяют это сделать, добавив после него знак вопроса.
Использование «ленивых» квантификаторов может повлечь за собой обратную проблему, когда выражению соответствует слишком короткая, в частности, пустая строка. Если необходимо, чтобы выражение нашло как минимум один символ, то вместо «*» нужно использовать «+».
Чтобы выделить отдельные теги, можно применить «ленивую» версию этого выражения: (**<.*?>**).
Ей соответствует не вся показанная выше строка, а отдельные теги
** Текст** для примера, ****жадной**** и ленивой квантификации ** **
В таблице 28 приведены символы «жадной» и «ленивой» квантификации.

Таблица 28 – Символы «жадной» и «ленивой» квантификации

Жадный	Ленивый
*	*?
+	+?
{n,}	{n,}?

Б.4 Перечисление

Вертикальная черта разделяет допустимые варианты. Например, «a | b» соответствует **a** или **b**. Следует помнить, что перебор вариантов выполняется слева направо, как они указаны.

Если требуется указать перечень вариантов внутри более сложного регулярного выражения, то его нужно заключить в группу. Например, «gray | grey» или «gr (a|e) y» описывают строку **gray** или **grey**. В случае с односимвольными альтернативами предпочтителен вариант «gr [ae] y», так как сравнение с символьным классом выполняется проще, чем обработка группы с проверкой на все её возможные модификаторы и генерацией обратной связи.

Б.5 Обратная связь

Одно из применений группировки – повторное использование ранее найденных групп символов (подстрок, блоков, отмеченных подвыражений, захватов). При обработке выражения подстро́ки, найденные по шаблону внутри группы, сохраняются в отдельной области памяти и получают номер, начиная с единицы. Каждой подстроке соответствует пара скобок в регулярном выражении. Квантификация группы не влияет на сохранённый результат, то есть, сохраняется лишь первое вхождение. Обычно поддерживается до 9 нумерованных подстрок с номерами от 1 до 9, но некоторые интерпретаторы позволяют работать с бо́льшим количеством. Впоследствии в пределах данного регулярного выражения можно использовать обозначения от «\1» до «\9» для проверки на совпадение с ранее найденной подстрокой.

Например, регулярное выражение «(та|ту)-\1» найдёт строку «та-та» или «ту-ту», но пропустит строку «та-ту».

Также ранее найденные подстроки можно использовать при замене по регулярному выражению. В таком случае в замещающий текст вставляются те же обозначения, что и в пределах самого выражения.

Б.6 Группировка

Примеры использования группировки приведены в таблице 29.

Таблица 29 – Примеры использования группировки

Символ	Описание	Пример	Соответствие
( )	Для группировки. Шаблон внутри как единое целое. может быть квантифицирован	(ab){3}	abc**ababab**cdab
(?:шаблон)	Группировка без обратной связи. Не будет создавать групп	a(?:bc|b|x)cc	**abcc**axcc, abcc**axcc**
		обработ(?:ка|тчик)	если требуется найти или «обработка», или «обработчик», но не важно, какое именно слово найдено

Символ	Описание	Пример	Соответствие
(?>шаблон)	Атомарная группировка, запрещает возвращаться назад по строке, если часть шаблона уже найдена	a(?>bc|b|x)cc	abcc**axcc** но не **abcc**axcc: вариант x найден, остальные проигнорированы

Б.7 Просмотр вперёд и назад

В большинстве реализаций регулярных выражений есть способ производить поиск фрагмента текста, «просматривая» (но не включая в найденное) окружающий текст, который расположен до или после искомого фрагмента текста. Просмотр с отрицанием используется реже и «следит» за тем, чтобы указанные соответствия, напротив, не встречались до или после искомого текстового фрагмента (см. таблицу 30).

Таблица 30 – Перечень файлов для постановки на контроль

Представление	Вид просмотра	Пример	Соответствие
(?=шаблон)	Позитивный просмотр вперёд	Людовик(?=XVI)	ЛюдовикXV, **Людовик**XVI, **Людовик**XVIII, ЛюдовикLXVII, ЛюдовикXXL
(?!шаблон)	Негативный просмотр вперёд (с отрицанием)	Людовик(?!XVI)	**Людовик**XV, ЛюдовикXVI, ЛюдовикXVIII, **Людовик**LXVII, **Людовик**XXL
(?<=шаблон)	Позитивный просмотр назад	(?<=Сергей)Иванов	Сергей **Иванов**, Игорь Иванов
(?<!шаблон)	Негативный просмотр назад (с отрицанием)	(?<!Сергей)Иванов	Сергей Иванов, Игорь **Иванов**

Перечень сокращений

AES	–	Advanced Encryption Standard
DES	–	Data Encryption Standard
FA	–	Firewall Assurance
HTTPS	–	HyperText Transfer Protocol Secure
ICC	–	Integrity Check Compliance
ICMP	–	Internet Control Message Protocol
IP	–	Internet Protocol
MD5	–	Message Digest 5
NA	–	Network Assurance
NAT	–	Network Address Translation
NFA	–	Network Flow Analysis
PCRE	–	Perl Compatible Regular Expressions
SHA	–	Secure Hash Algorithm
SNMP	–	Simple Network Management Protocol
SSH	–	Secure SHell
TELNET	–	Teletype Network
TSP	–	Time Stamp Protocol
UDP	–	User Datagram Protocol
VC	–	Vulnerability Control
БД	–	База данных
МЭ	–	Межсетевой экран
ОЗ	–	Объект защиты
ПК	–	Программный комплекс
СУБД	–	Система управления базами данных