

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


Часть 2

Контроль устройств

Аннотация

Руководство содержит описание для настройки и конфигурирования модулей «Efros Network Assurance» («Efros NA»), «Efros Firewall Assurance» («Efros FA»), «Efros Integrity Check Compliance» («Efros ICC») и «Efros Vulnerability Control» («Efros VC»).

Для работы с данными модулями необходимо убедиться в установке соответствующих лицензий в программном комплексе по защите системно-технической инфраструктуры «Efros Defence Operations» (далее – ПК «Efros DO» или комплекс).

Для перехода в раздел «Контроль устройств» необходимо выбрать в панели главного меню раздел «Контроль устройств», или, если панель свернута, нажать на пиктограмму «», панель автоматически раскроется и отобразятся все подразделы.

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.....	6
2	Работа с ПК «Efros DO». Раздел «Контроль устройств»	7
2.1	Устройства	7
2.1.1	Дерево устройств	8
2.1.1.1	Добавление устройства	9
2.1.1.2	Добавление группы устройств	15
2.1.1.3	Изменение параметров устройства/группы устройств	16
2.1.1.4	Удаление устройства/группы устройств	17
2.1.2	Вкладка «Статус» для одного устройства	17
2.1.2.1	Блок «Защищенность»	17
2.1.2.2	Блок «Уведомления»	18
2.1.2.3	Блок «Информация об устройстве»	19
2.1.2.4	Блок «Операции»	20
2.1.2.5	Конфигурирование устройства	21
2.1.3	Вкладка «Статус» для группы устройств	25
2.1.3.1	Блок «Уведомления»	25
2.1.3.2	Блок «Проверки безопасности»	26
2.1.3.3	Блок «Уязвимые устройства»	27
2.1.3.4	Блок «Доступность устройств»	27
2.1.4	Вкладка «Отчеты»	28
2.1.4.1	Просмотр отчета	29
2.1.4.2	Настройка отчета	31
2.1.5	Вкладка «События»	34
2.1.5.1	Фильтрация	35
2.1.6	Вкладка «Архив»	37
2.1.6.1	Просмотр архивной версии отчета	38
2.1.6.2	Создание отчета «Выборка»	41
2.1.6.3	Фильтрация	42
2.2	Проверки безопасности	44
2.2.1	Дерево со списком типов устройств	45
2.2.2	Вкладка «Стандарты»	45


2.2.2.1. Создание пользовательского стандарта безопасности	45
2.2.2.2. Создание пользовательских требований проверок в пользовательском стандарте.....	47
2.2.2.3. Настройка использования пользовательского стандарта.....	50
2.2.3. Вкладка «База требований»	51
2.2.3.1. Редактирование пользовательских проверок безопасности	51
2.2.3.2. Настройки пользовательских проверок безопасности	53
2.3 Проверки МЭ.....	54
2.3.1. Вкладка «Стандарты безопасности»	54
2.3.1.1. Создание нового стандарта безопасности.....	55
2.3.1.2. Создание нового требования	56
2.3.1.3. Копирование требования.....	59
2.3.2. Вкладка «Зонный анализ»	60
2.3.2.1. Создание нового стандарта зонного анализа	61
2.3.2.2. Создание нового требования для стандарта зонного анализа	63
2.3.2.3. Копирование требования из стандарта зонного анализа	65
2.3.3. Вкладка «Зоны»	65
2.3.3.1. Создание новой зоны.....	66
2.4 Профили отчетов.....	68
2.4.1. Дерево профилей отчетов.....	68
2.4.1.1. Создание пользовательского профиля отчетов	69
2.4.2. Вкладка «Конфигурации»	70
2.4.2.1. Создание пользовательского отчета	72
2.4.3. Вкладка «Проверки безопасности»	73
2.4.3.1. Настройка использования стандартов проверок безопасности	74
2.5 Обработчики событий	77
2.5.1. Создание пользовательского обработчика событий.....	78
2.5.2. Редактирование обработчика	81
2.6 Профили аутентификации	82
2.6.1.1. Создание профиля аутентификации	83
2.6.1.2. Редактирование профиля аутентификации	84
2.6.1.3. Настройки использования профиля аутентификации.....	84



2.7 SNMP профили	86
2.7.1.1. Создание SNMP профиля	87
2.7.1.2. Редактирование SNMP профиля	89
2.7.1.3. Настройки использования SNMP профиля	89
2.8 Доступность устройств	91
2.8.1.1. Настройка проверки доступности устройств	92
Перечень сокращений	93

1 Предварительные настройки

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

Для работы с модулями «Efros Network Assurance» («Efros NA»), «Efros Firewall Assurance» («Efros FA»), «Efros Integrity Check Compliance» («Efros ICC») и «Efros Vulnerability Control» («Efros VC») необходимо произвести следующие подготовительные действия:

- Загрузить внешние модули для работы с устройствами.
- Перевести переключатель «Состояние» в положение «Включен» .
- 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» активен . Более подробно см. документ «Руководство пользователя. Часть 1. Администрирование».

2 Работа с ПК «Efros DO». Раздел «Контроль устройств»

Функциональность раздела «Контроль устройств» составляется из нескольких функциональных модулей:

- Модуль «Efros NA» предназначен для контроля сетевой составляющей объектов защиты (далее – ОЗ), последующим отображением ОЗ на карте сети с возможностью моделирования прохождения трафика.
- Модуль «Efros FA» отвечает за анализ межсетевых экранов (далее – МЭ) и предоставляет возможность использовать оптимизацию правил, стандарты МЭ, зонный анализ.
- Модуль «Efros VC» отвечает за уязвимости, обнаруженные на ОЗ, предоставляет возможность построения векторов.
- Модуль «Efros ICC» предназначен для контроля целостности файлов ОС и контроля их конфигураций, текстовых файлов и т.д.

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 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.

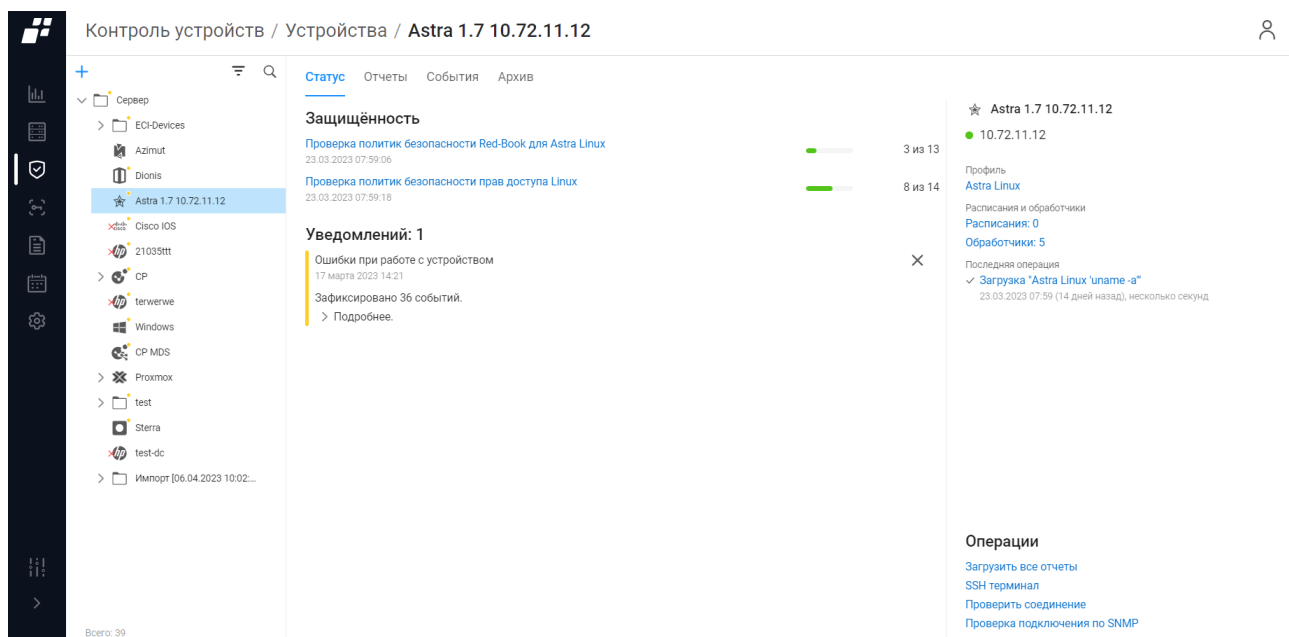


Рисунок 1 – Подраздел «Устройства»

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».

2.1.1. Дерево устройств

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

- кнопка «Добавить» () для создания нового устройства или новой группы устройств;
- поле поиска () для осуществления поиска в списке устройств;
- кнопка «Фильтр» () для фильтрации списка устройств в дереве устройств.

При наведении курсора на устройство в дереве устройств появится кнопка «Контекстное меню» (), с помощью которой можно выполнить следующие действия:

- «Изменить» – внести изменения в свойства устройства;
- «Создать копию» – создать копию выбранного устройства;
- «Загрузить конфигурации» – выполнить действия по конфигурированию




выбранного устройства;

- «Принять все изменения» – запустить подтверждения 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» – удалить устройство или группу устройств.

В правом верхнем углу иконки вендора устройства расположен круг, цвет которого отображает наличие или отсутствие уведомлений у устройства:

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

С левой стороны от иконки вендора устройства может отображаться:


- красный крест «» - последняя выполняемая с устройством операция закончилась ошибкой;
- красный ключ «» - последняя операция с устройством закончилась ошибкой аутентификации;
- оранжевый ключ «» - устройство переведено в сервисный режим.

В правом верхнем углу иконки группы устройств, в которую входит хотя бы одно устройство, расположен круг, цвет которого 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

Для добавления устройства пользователю необходимо выполнить следующие действия:

- 1) В дереве устройств нажать на кнопку «Добавить» () и из контекстного меню выбрать «Устройство».
- 2) Откроется страница «Создание устройства». На странице указать необходимые параметры в следующих вкладках (рис. 2):
 - «Свойства» – вкладка активна по умолчанию, необходимо указать параметры добавляемого устройства;
 - «Расписания» – позволяет настроить параметры использования расписаний для добавляемого устройства. Вкладка становится доступной только после создания устройства;
 - «Обработчики событий» – позволяет настроить параметры обработчиков событий для добавляемого устройства.

i 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.

← Создание устройства

Свойства Расписания Обработки событий

Название

Описание

Группа

Тип

Профиль отчетов

Проверка доступности ☐ Отключена

Сервисный режим ☐

Типы контроля

NETWORK ASSURANCE ☐

Параметры подключения

Адрес

Порт

Пользователь

Пароль

Использовать привилегированный пароль ☐

Профиль аутентификации

SNMP

SNMP профиль

Рисунок 2 – Страница «Создание устройства»

Состав и описание Полей вкладки «Свойства» приведены в таблице 1.

Таблица 1 – Состав и описание Полей вкладки «Свойства»

Поле	Описание
Поле «Название»	Текстовое поле для ввода имени устройства. Параметры ввода текста: от 1 до 250 любых символов
Поле «Описание»	Текстовое поле для ввода описания устройства. Параметры ввода текста: от 1 до 4000 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. Поле становится доступно только после выбора типа устройства
Поле «Проверка доступности»	Переключатель: включение/отключение проверки доступности устройства с указанной периодичностью (каждые 5 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»	
Переключатель «Network Assurance»	Переключатель. По умолчанию выключен. Переключатель отображается, если для данного типа устройства поддерживается данный тип контроля
Переключатель «Firewall Assurance»	Переключатель. По умолчанию выключен. Переключатель отображается, если для данного типа устройства поддерживается данный тип контроля
Переключатель «Integrity Check Compliance»	Переключатель. По умолчанию выключен. Переключатель отображается, если для данного типа устройства поддерживается данный тип контроля
Переключатель «Vulnerability Control»	Переключатель. По умолчанию выключен. Переключатель отображается, если для данного типа устройства поддерживается данный тип контроля
Переключатель «Change Manager»	Переключатель. По умолчанию выключен. Переключатель отображается при наличии лицензии на модуль «Efros CM» и только для устройств, поддерживающих тип контроля FA
Возможные	— Есть лицензия и выбранный тип устройства

информационные сообщения под переключателем	поддерживается; — Нет лицензии; — Есть лицензия, но выбранный тип устройства не поддерживается; — Достигнут или превышен лимит лицензий по количеству устройств
Дополнительные параметры подключения зависят от выбранного типа устройства в поле «Тип»	
Поле «Адрес»	IP-адрес или доменное имя устройства. Параметры для ввода текста: от 1 до 50 символов, формат от 0.0.0.0 до 255.255.255.255
Поле «Пользователь»	Логин пользователя для аутентификации на устройстве
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 на сервере ПК. В списке необходимо выбрать профиль аутентификации (имя учетной записи (логин) и пароль), которые будут использоваться при аутентификации на контролируемом устройстве. Если требуемого профиля нет, то пользователь может добавить его, выбрав значение «Новый профиль» в списке. В появившейся

	<p>вкладке заполнить поля для добавления на сервер ПК профиля аутентификации и нажать кнопку «Создать».</p> <p>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)</p>
Кнопка «Проверить подключение»	<p>По нажатию кнопки выполняется проверка подключения устройства.</p> <p>После завершения проверки слева от кнопки отображается результат проверки: «Успешно» или «Ошибка подключения». Текст результата является ссылкой, при выборе которой открывается окно с логом выполнения команды</p>
Группа полей «SNMP»	
Поле «SNMP профиль»	<p>Раскрывающийся список поля по умолчанию содержит значения «SNMP отключен» и «public» (предустановленный профиль для подключения по SNMPv2). Созданные пользовательские SNMP-профили также отображаются в списке.</p> <p>При выборе значения SNMP отключен справа в поле отображается кнопка Добавить (+) для перехода в окно добавления профиля SNMP. Добавление профиля возможно, как SNMPv2c с указанием community для подключения, так и SNMPv3 с указанием алгоритмов защиты и учетными данными.</p> <p>Пользователь также имеет возможность внести изменения в выбранный в поле профиль (SNMP или public), для чего необходимо после выбора профиля нажать справа в поле кнопку «Редактировать» (✎), внести изменения в открывшемся окне параметров профиля и нажать кнопку «Сохранить» (более подробно описано в разделе 0)</p>
Элементы управления	
Создать	При нажатии на кнопку введенные данные сохраняются
Отменить	При нажатии на кнопку введенные данные не сохраняются

- 3) Заполнить поля вкладки соответствующими параметрами.
- 4) Перейти на вкладку «Обработчики событий» (рис. 3). Состав и описание Полей вкладки приведено в таблице 2.

- 5) В поле «Использование» выбрать режим срабатывания обработчика событий (на вкладке отображаются только активные обработчики событий).

← Создание устройства

Свойства Расписания Обработчики событий

Обработчик событий	Использование
Выполнение конфигурирования и восстановления	Разрешено
Изменения контролируемых отчетов	Разрешено Запрещено
Ошибки конфигурирования и восстановления	Разрешено
Ошибки при работе с устройством	Разрешено
Первые ошибки при работе с устройством	Разрешено

Создать Отменить

Рисунок 3 – Вкладка «Обработчики событий»

Таблица 2 – Состав и описание Полей вкладки «Обработчики событий»

Поле	Описание
Поле «Обработчики событий»	Наименование обработчика событий
Поле «Использование»	Выбор режима использования расписания. Возможные значения: — Разрешено – разрешить выполнение расписания вне зависимости от настроек базового профиля; — Запрещено – запретить выполнение расписания вне зависимости от настроек базового профиля

- 6) Нажать кнопку «Создать».

Автоматически запустится процесс проверки заполнения всех обязательных полей и уникальности добавляемого устройства.

При обнаружении незаполненных обязательных полей под полем появится сообщение красного цвета: «Обязательное поле». Пользователю необходимо корректно заполнить поля страницы и повторно нажать кнопку «Создать».

2.1.1.2. Добавление группы устройств

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

- 1) В дереве устройств нажать кнопку «Добавить» (+) и из контекстного меню выбрать пункт «Группа».
- 2) Откроется страница «Создание группы» (рис. 4). Страница состоит из следующих вкладок:
 - «Свойства» – вкладка активна по умолчанию;
 - «Обработчики событий».

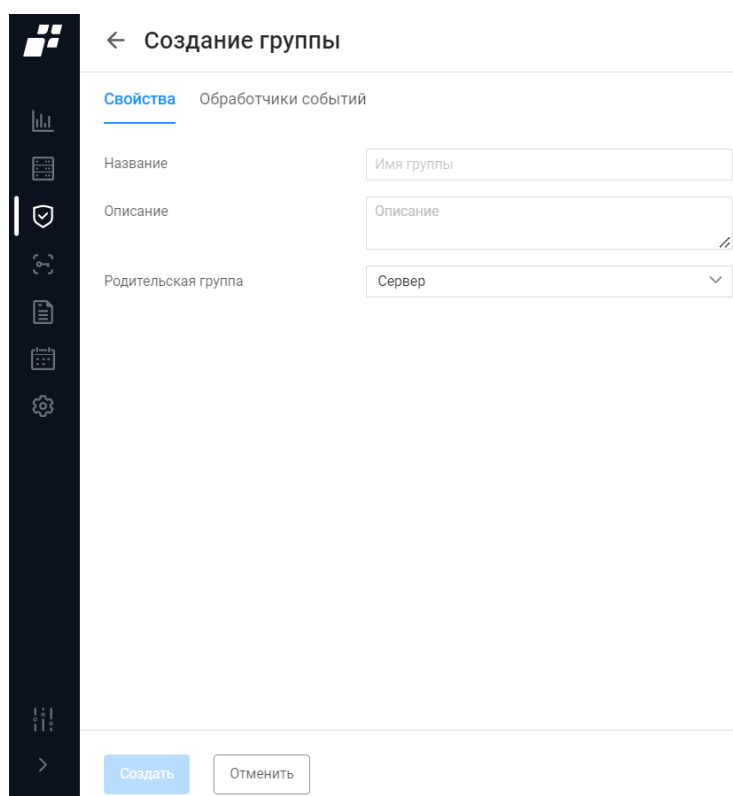


Рисунок 4 – Страница «Создание группы»

Состав и описание Полей вкладки «Свойства» приведены в таблице 3.

Таблица 3 – Состав и описание Полей вкладки «Свойства»

Поле	Описание
Поле «Название»	Текстовое поле для ввода названия группы устройств. Параметры ввода текста: от 1 до 250 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 4000 символов
Поле	Раскрывающийся список доступных для выбора групп, куда будет

«Родительская группа»	входить создаваемая группа устройств
Элементы управления	
Создать	При нажатии на кнопку введенные данные сохраняются
Отменить	При нажатии на кнопку введенные данные не сохраняются

- 3) Заполнить поля вкладки соответствующими параметрами.
- 4) Перейти на вкладку «Обработчики событий» (рис. 5). Состав и описание Полей вкладки приведено в таблице 2.
- 5) В поле «Использование» выбрать режим срабатывания обработчика событий.

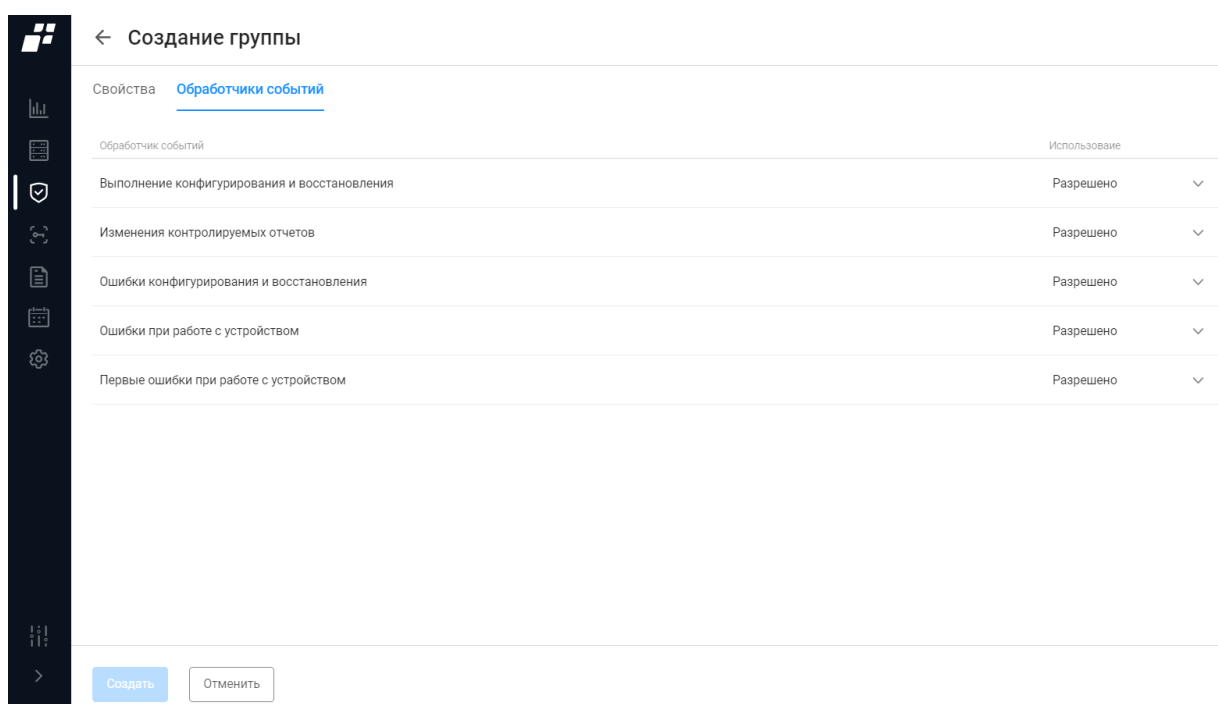


Рисунок 5 – Вкладка «Обработчики событий»

- 6) Нажать кнопку «Создать».

Автоматически запустится процесс проверки заполнения всех обязательных полей и уникальности добавляемой группы устройств.

При обнаружении незаполненных обязательных полей под полем появится сообщение красного цвета: «Обязательное поле». Пользователю необходимо корректно заполнить поля страницы и повторно нажать кнопку «Создать».

2.1.1.3. Изменение параметров устройства/группы устройств

Для изменения параметров устройства/группы устройств пользователю необходимо выполнить следующие действия:

- 1) В дереве устройств выделить необходимое устройство/группу устройств, раскрыть контекстное меню и выбрать в нем пункт «Изменить».
- 2) В открывшемся окне изменить параметры устройства/группы устройств. Поле

«Тип» в параметрах устройства недоступно для изменения.

3) Нажать кнопку «Сохранить».

Автоматически запустится процесс проверки заполнения всех обязательных полей и уникальности редактируемого устройства/группы устройств.

При обнаружении незаполненных обязательных полей появится сообщение красного цвета: «Обязательное поле». Пользователю необходимо корректно заполнить поля страницы и повторно нажать кнопку «Сохранить».

2.1.1.4. Удаление устройства/группы устройств

Для удаления устройства/группы устройств пользователю необходимо выполнить следующие действия:

- 1) В дереве устройств выделить необходимое устройство/группу устройств, раскрыть контекстное меню и выбрать в нем пункт «Удалить».
- 2) В открывшемся окне подтвердить операцию удаления устройства/группы устройств, нажав кнопку «Удалить».

2.1.2. Вкладка «Статус» для одного устройства

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

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

2.1.2.1. Блок «Защищенность»

Данный блок отображает результаты выполнения проверок на выбранном устройстве (рис. 6).

 Для группы устройств блок «Защищенность» не отображается.

Контроль устройств / Устройства / Cisco IOS190

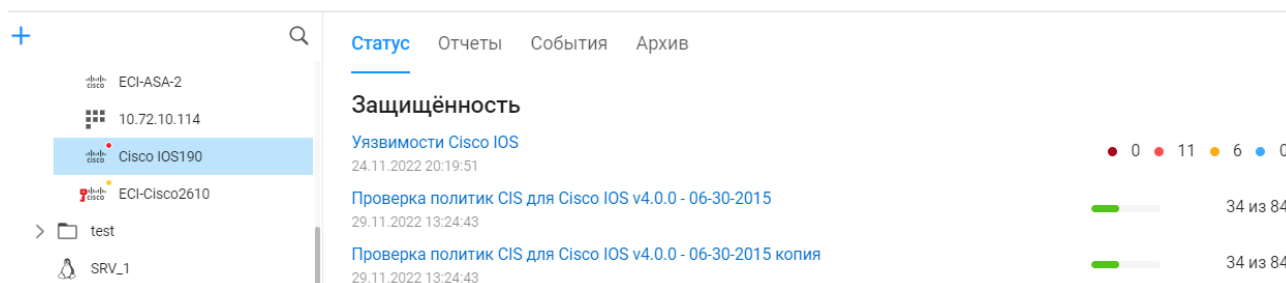


Рисунок 6 – Блок «Защищенность»

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;
- «●» — Скрытые уязвимости — уязвимости на устройствах, скрытые пользователем средствами комплекса. При отсутствии скрытых уязвимостей, иконка «●» и количество «0» не отображаются.

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 с 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»

Данный блок отображает уведомления о произошедших событиях контроля устройства и об ошибках выполнения заданий, заданных на устройстве (рис. 7).

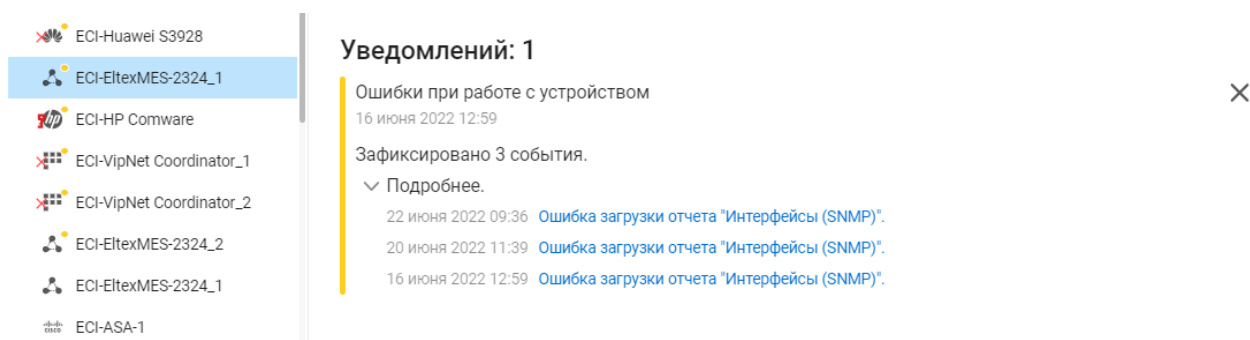


Рисунок 7 – Блок «Уведомления»

Уведомление содержит:

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

— текст 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 создании обработчика событий.

— Нарушение контроля целостности:

- нарушение целостности;
- ранее было зафиксировано нарушение целостности.

— 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» (X) для удаления выбранного 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» – переход в окно сравнения текущего отчёта с эталоном с возможностью принятия текущего отчета за эталон;
- «Переход к отчету» – переход в окно просмотра отчета.

2.1.2.3. Блок «Информация об устройстве»

Данный блок (рис. 8) 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 2.8);
 - активен (зеленый круг рядом с IP-адресом устройства) – устройство доступно (более подробно описано в подразделе 2.8).
- профиль отчетов;
- модель устройства;

- версия установленного на устройстве ПО, если оно есть у устройства;
- серийный номер;
- расписания и обработчики, если они настроены для устройства;
- последняя операция, производимая с устройством.

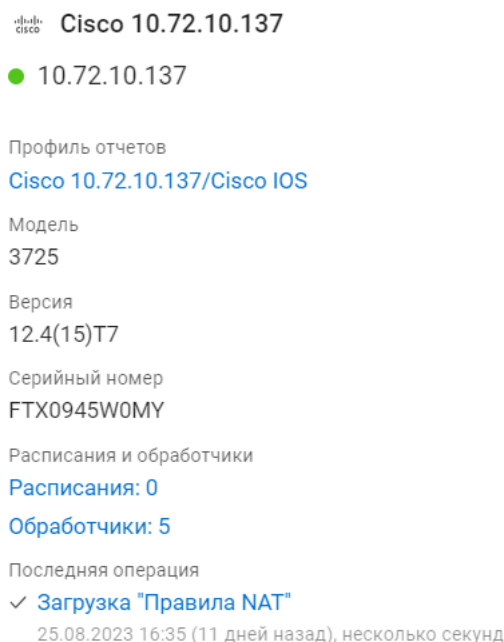


Рисунок 8 – Блок «Информация об устройстве»

Поле «Профиль» является ссылкой на подраздел «Профили», более подробно описано в подразделе 2.4.

Поле «Расписания и обработчики» содержит следующие ссылки:

- «Расписания» – открывает вкладку «Расписания» выбранного устройства для редактирования списка используемых расписаний;
- «Обработчики» – открывает вкладку «Обработчики событий» для редактирования списка используемых триггеров, связанных с выбранным устройством.

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

2.1.2.4. Блок «Операции»

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

- «Загрузить все отчеты» – позволяет начать загрузку всех отчетов с устройства;
- «SSH-терминал» – ссылка для соединения с ОЗ по протоколу SSH;
- «Подключиться по HTTPS» – ссылка для соединения с ОЗ по протоколу HTTPS;

- «Выполнить команды (конфигурировать устройство)» – позволяет задать команды напрямую;
- «Восстановить конфигурацию» – позволяет восстановить любую конфигурацию, существовавшую на устройстве;
- «Проверить соединение» – позволяет получить информацию о доступности ОЗ;
- «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 устройства» – позволяет обновить список вложенных устройств по выбранному родительскому устройству.

Операции

Загрузить все отчеты

SSH терминал

Выполнить команды

Восстановить конфигурацию

Проверить соединение



Скопировать running в startup

Проверка подключения по SNMP

Рисунок 9 – 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. рис. 9).

 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 положение активен . Более подробно см. документ «Руководство пользователя. Часть 1. Администрирование».

Для изменения конфигурации устройства необходимо выполнить следующие действия:

- 1) В блоке «Операции» нажать на ссылку «Выполнить команды».
- 2) В открывшемся окне «Конфигурирование оборудования» (рис. 10) в поле «Сохраненные наборы команд» выбрать из сохраненных или задать перечень команд конфигурирования в соответствующем поле, характерный для типа выбранного устройства. Поддерживается сохранение/изменение/удаление списков команд конфигурирования.

✕ Конфигурирование оборудования

① Команды будут выполнены последовательно из режима enable

Объекты защиты

Объекты защиты 1 объект

Сохраненные наборы команд Набор команд ▾ ... </>

Команды конфигурирования

Команды конфигурирования

Параметры

Пользователь admin Другие логин/пароль

Логин Логин пользователя

Пароль Пароль

Дополнительный пароль Пароль

Настройки

Перезагрузка устройства при потере связи ☐

Прервать при первой ошибке ввода команды ☒

Выполнить Отменить

Рисунок 10 – Окно «Конфигурирование оборудования»

- 3) В поле «Параметры» выбрать учетную запись, используя переключатель. 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.

- 4) В поле «Настройки» с помощью переключателя включить требуемые настройки поведения оборудования при появлении нештатной ситуации.
- 5) Нажать кнопку «Выполнить».

В случае необходимости восстановления работоспособности устройства, для выполнения доступна команда по восстановлению загрузочной конфигурации сетевого оборудования с использованием ранее сохраненной настройки конфигурации.

Для этого, в блоке «Операции» необходимо выбрать операцию «Восстановить конфигурацию». После подключения к устройству и загрузки его конфигурации,

откроется окно «Восстановление конфигурации» (рис. 11, 12).

✕ Восстановление конфигурации

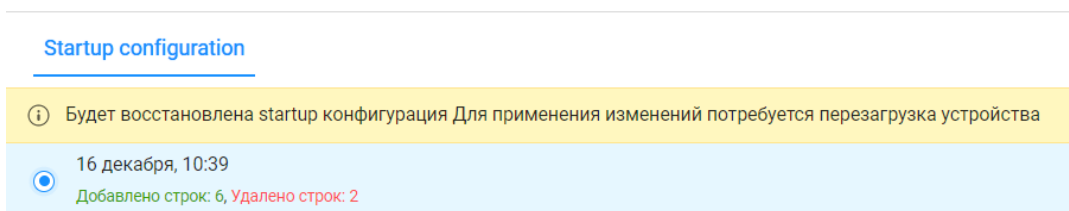


Рисунок 11 – Окно «Восстановление конфигурации»

Для восстановления конфигурации устройства необходимо выполнить следующие действия:

- 1) В окне «Восстановление конфигурации» выбрать сохраненную ранее конфигурацию. При необходимости можно просмотреть выбранную для восстановления конфигурацию, нажав кнопку «Показать отличия». В открывшемся окне можно сравнить архивную версию отчета, выбранного для восстановления конфигурации, и текущую версию конфигурации (рис. 13).
- 2) Нажать кнопку «Восстановить».

В результате произойдет обновление конфигурации выбранного устройства.

✕ Подтверждение восстановления конфигурации

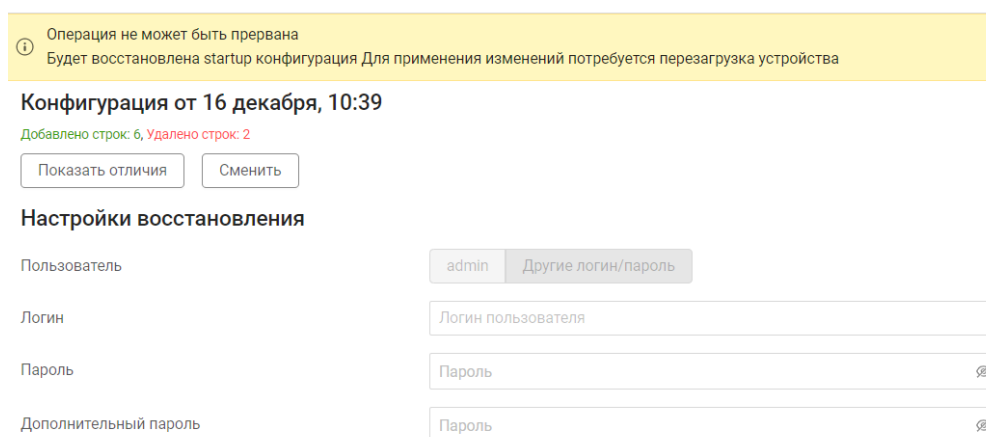


Рисунок 12 – Окно «Подтверждение восстановления конфигурации»

Таблица 4 – 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: — пользователь, указанный при заведении устройства в комплекс (admin); — другой пользователь – пользователь, который создан на устройстве
Поле «Логин»	Логин пользователя, работающего с устройством
Поле «Пароль»	Пароль пользователя, работающего с устройством
Поле «Дополнительный пароль»	Дополнительный пароль для привилегированного режима

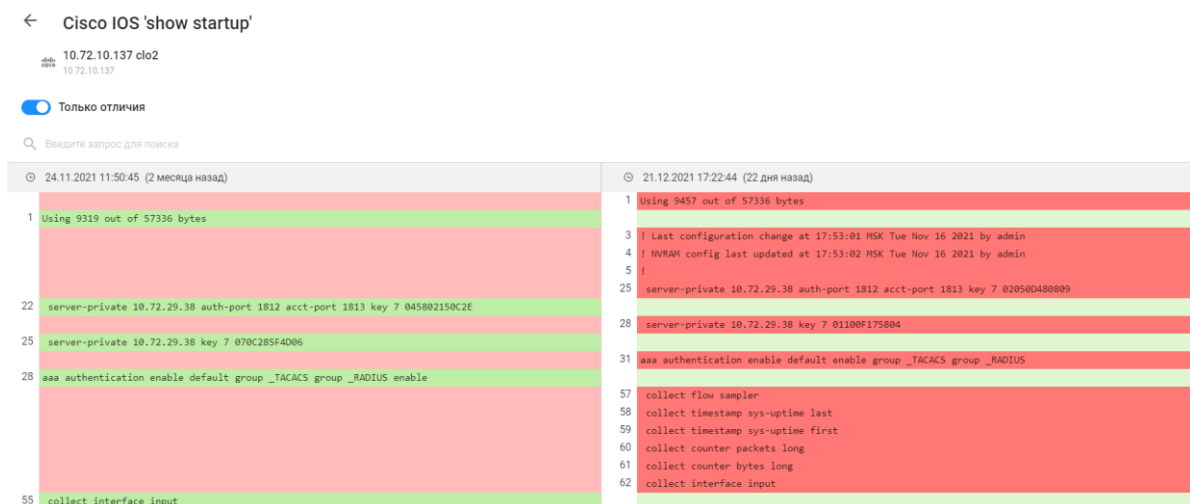


Рисунок 13 – Страница «Сравнение отчетов»

2.1.3. Вкладка «Статус» для группы устройств

Вкладка «Статус» (рис. 14) содержит сведения, относящиеся к группе устройств, выделенной в дереве устройств, и разделена на блоки:

- «Уведомления»;
- «Проверки безопасности»;
- «Уязвимые устройства»;
- «Доступность устройств».

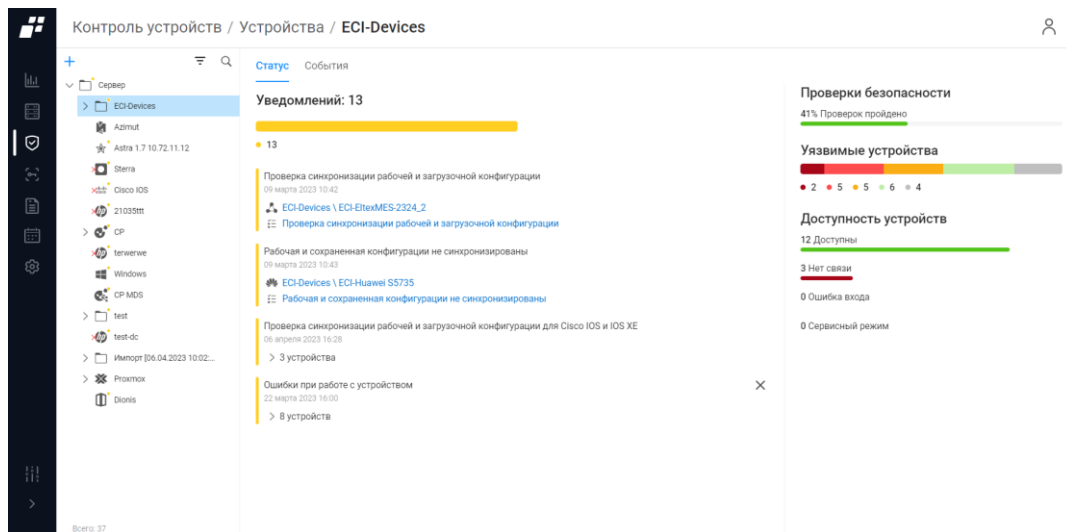


Рисунок 14 – Вкладка «Статус» для группы устройств

2.1.3.1. Блок «Уведомления»

Данный блок отображает уведомления о произошедших событиях контроля группы устройств и об ошибках выполнения заданий, заданных для устройств в группе устройств (рис. 15).

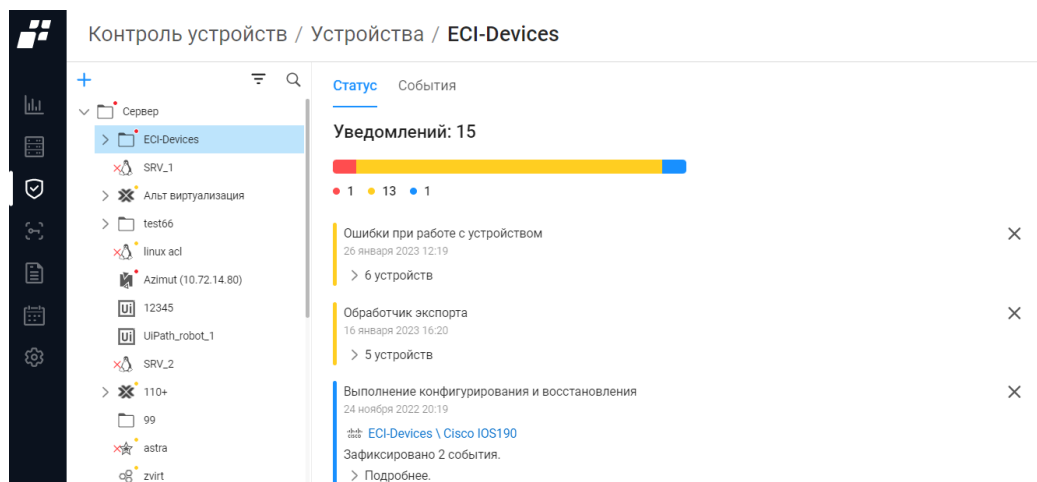



Рисунок 15 – Блок «Уведомления»

Уведомление содержит:

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

- Нарушение контроля целостности:
 - нарушение целостности (когда текущий отчёт отличается от эталона);
 - ранее было зафиксировано нарушение целостности (когда 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 выбранного 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» – переход в форму сравнения текущего отчёта с эталоном с возможностью принятия текущего отчета за эталон;
- «Переход к отчету» – переход в окно просмотра отчета.

2.1.3.2. Блок «Проверки безопасности»

Данный блок отображает результаты выполнения проверок на выбранном устройстве (рис. 16)

Проверки безопасности

46% Проверок пройдено




Рисунок 16 – 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. 17).

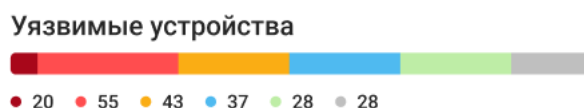


Рисунок 17 – Блок «Уязвимые устройства»

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

- «●» – при проверке обнаружена хотя бы 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. 18) содержит графическое представление информации о статусах контролируемых устройств, которые входят в выделенную группу – 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.

Доступность устройств

9 Доступны

5 Нет связи

0 Ошибка входа

0 Сервисный режим

Рисунок 18 – Блок «Доступность устройств»

2.1.4. Вкладка «Отчеты»

Вкладка «Отчеты» (рис. 19) содержит список отчетов, разрешенных для загрузки с выбранного устройства/группы устройств и содержащих значения параметров контролируемого оборудования/группы оборудования.

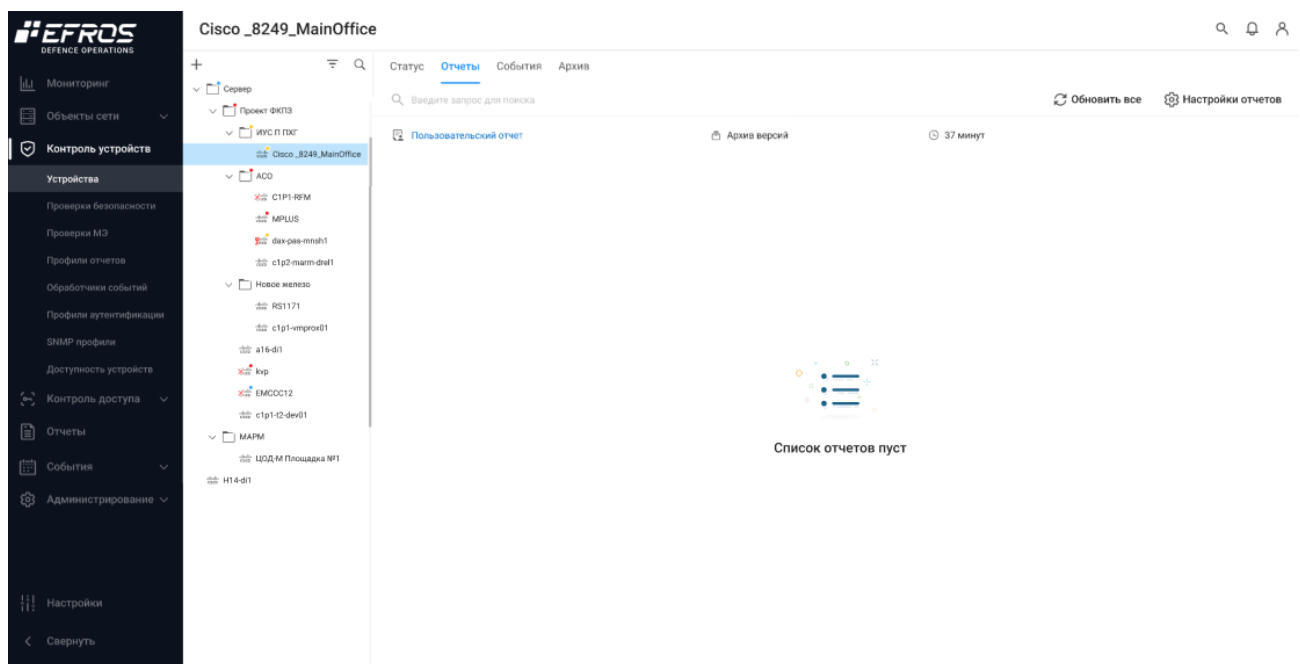








Рисунок 19 – Вкладка «Отчеты»






На вкладке список отчетов группируется по двум типам: «Конфигурации» и «Проверки». Каждый тип отчета представлен в виде раскрывающегося списка. Для каждой записи списка отображаются следующие данные:

— пиктограммы отчетов типа «Конфигурации»:

- текстовый «»;
- структурированный «»;
- пользовательский отчет «»;
- отчет типа «Фильтр» «», созданный на основе другого отчета путем фильтрации данных;

- отчет «Правила межсетевых экранов» «»;
- правила NAT «»

— пиктограммы отчетов типа «Проверки»:




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

❗ Эталонные отчеты обозначаются пиктограммой «».



❗ 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.

- название. Является ссылкой, при переходе открывается окно для просмотра отчета.
- операции – состояние загруженного отчета.
- время запуска – время, прошедшее с момента загрузки последней версии отчета.

Над списком отчетов располагаются:

- поле поиска ( Введите запрос для поиска) для поиска искомой записи в списке;
- поле «Настройки отчетов» ( Настройки отчетов) – позволяет задать режим использования отчета, более подробно см. п.п. 2.1.4.2;
- кнопка «Обновить все» ( Обновить все) – для обновления всех отчетов одновременно.

При наведении курсора на строку с отчетом появляются следующие кнопки:

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

2.1.4.1. Просмотр отчета

Для просмотра отчета необходимо кликнуть по выбранному отчету. В результате откроется форма просмотра отчета. На рис. 20 приведена страница с текстовой формой отчета.

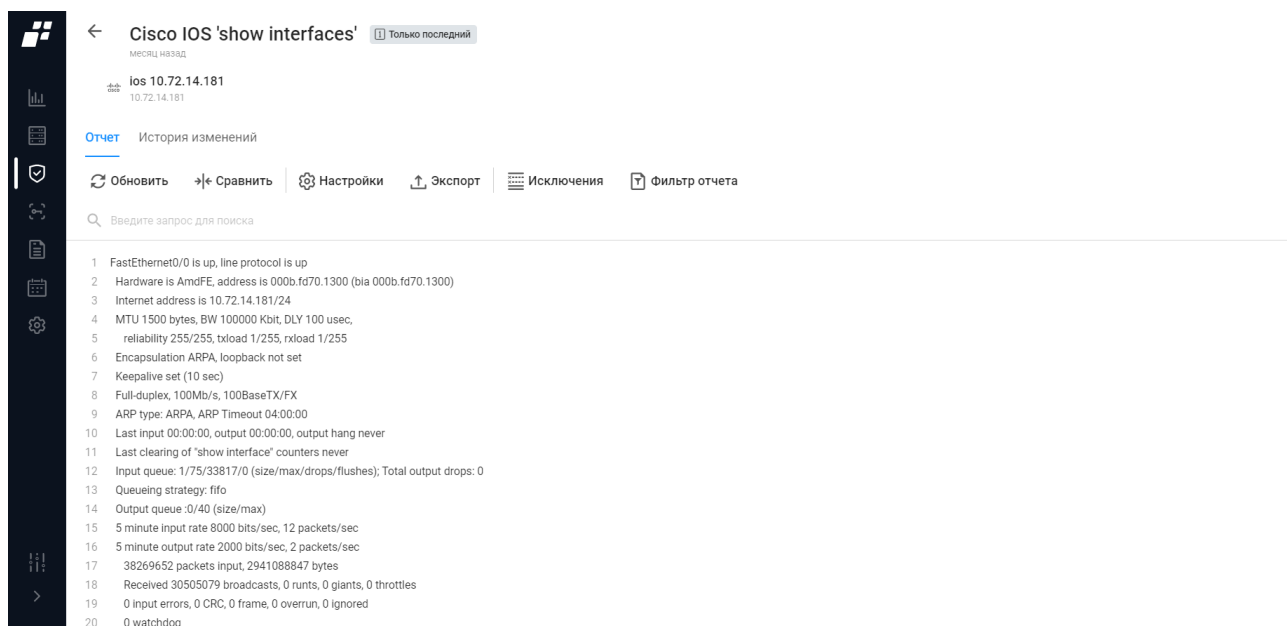


Рисунок 20 – Страница текстовой формы отчета

Страница содержит следующие вкладки:

- «Отчет»;
- «История изменений».

На вкладке «Отчет» 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»;
- кнопка «Фильтр отчета» (Фильтр отчета) используется для настройки параметров поиска, фильтрации в текстовых отчетах по заданным параметрам.

Для просмотра изменений необходимо перейти на вкладку «История изменений» (рис. 21).

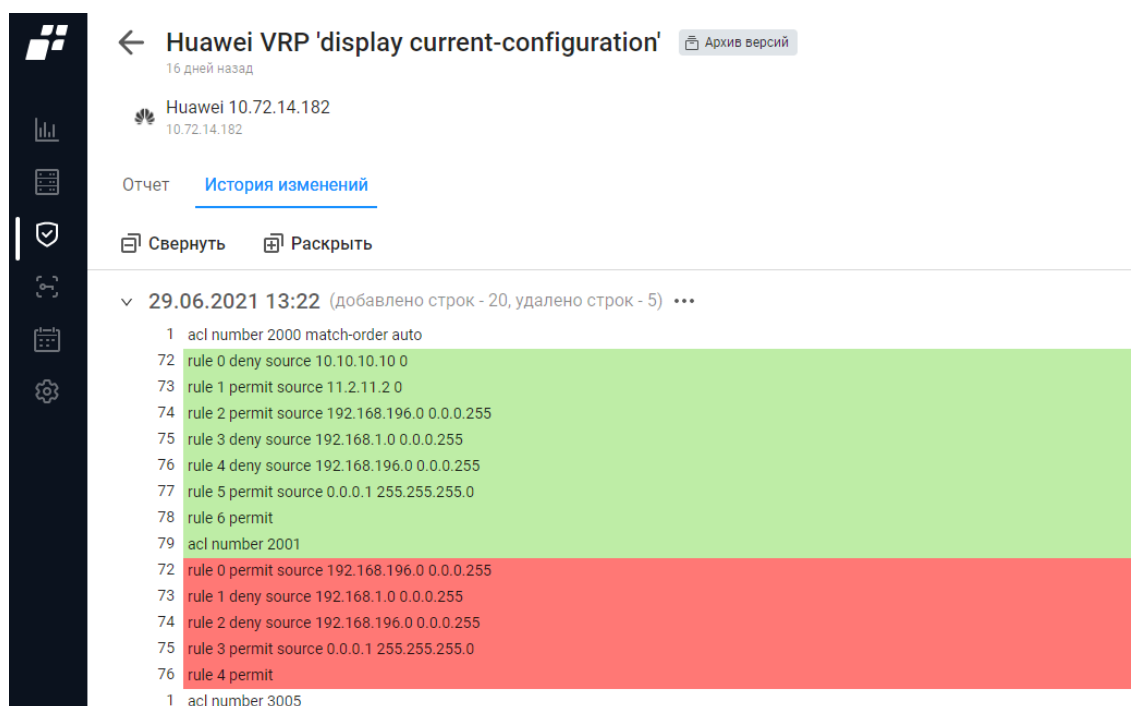





Рисунок 21 – Страница текстовой формы отчета, вкладка «История изменений»


Над страницей доступны следующие функции:

- кнопка «Свернуть» ( Свернуть) позволяет преобразовать представление отчета в табличный вид;
- кнопка «Раскрыть» ( Раскрыть) позволяет преобразовать представление отчета в виде дерева.

2.1.4.2. 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. 19) выбрать необходимый отчет 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. 22, рис. 23), состав и описание значений полей окна приведены в таблице 5.
- 4) Нажать кнопку «Сохранить». Окно настройки отчета закроется, внесенные изменения будут сохранены.

✕ Linux '/sbin/ausearch -m USER_AUTH -x /bin/su -sv no

Использование

Только последний ▾

Контроль изменений

Архив версий

Только последний

Запрещено

Сохранить

Отменить

Рисунок 22 – Окно настройки отчета типа «Конфигурации»

← **Уязвимости Cisco IOS**

Использование

Наследовать (Разрешено) ▾

Запрещено

Наследовать (Разрешено)


Рисунок 23 – Окно настройки отчета типа «Проверки»

Таблица 5 – Состав и описание Полей окон настройки отчета для устройства

Поле	Описание
Поле «Использование»	Выбор режима использования отчета. Возможные значения для типов отчета «Конфигурации»: — «Контроль изменений» – вне зависимости от настроек

Поле	Описание
	<p>базового профиля будет выполняться контроль целостности загруженного с устройства отчета;</p> <ul style="list-style-type: none"> — «Архив версий» – в базе данных комплекса будут храниться все измененные версии отчета, загруженные с устройства; — «Только последний» – в БД комплекса хранится только последняя измененная версия отчета, загруженного с устройства; — «Запрещено» – загрузка отчета с устройств запрещена вне зависимости от настроек профиля устройства; — «Наследовать (XXXX)» – применить настройки профиля устройства. В скобках отображается значение, установленное для отчета в профиле устройства. <p>Возможные значения для типов отчета «Проверки»:</p> <ul style="list-style-type: none"> — «Разрешено» – разрешить проверку вне зависимости от настроек профиля устройства; — «Запрещено» – запретить проверку вне зависимости от настроек профиля устройства; — «Наследовать (XXXX)» – применить настройки профиля выбранного устройства. В скобках отображается значение, установленное для правила в профиле устройства

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. 19) нажать кнопку «Настройки отчетов» ( Настройки отчетов).
- 3) Откроется окно настройки отчетов выбранного устройства (рис. 24), где в поле «Профиль устройства» расположен раскрывающийся список всех профилей устройства.

✕ Настройки отчетов

Профиль отчетов
Главная циска / Cisco_main_7210

Конфигурации Проверки безопасности

Введите запрос для поиска

Имя	Тип контроля	Использование
Cisco IOS 'show arp'	NA	Архив версий
Cisco IOS 'show running'	NA	Архив версий
Cisco IOS 'show config'	NA	Архив версий
Cisco IOS 'show ip route'	NA	Архив версий
Cisco IOS 'show version'	NA	Архив версий
Правила межсетевых экранов	NA FA	Архив версий
Маршруты (SNMP)	NA	Архив версий
Cisco ASA 'show route'	NA	Архив версий
Cisco ASA Конфигурация	NA	Архив версий
UserReportName	NA	Архив версий

Сохранить Отменить

Рисунок 24 – Окно настройки отчетов выбранного устройства

- 4) На вкладке «Конфигурации» из раскрывающегося списка поля «Использование» выбрать необходимое значение для каждого отчета. Состав и описание значений полей окна приведены в таблице 5.
- 5) На вкладке «Проверки» выбрать из перечня значений раскрывающегося списка поля «Использование» требуемое значение варианта использования проверки для выбранного профиля. Состав и описание значений полей окна приведены в таблице 5.
- 6) В окне настройки отчетов нажать кнопку «Сохранить». Окно настройки отчетов устройства закроется, внесенные изменения будут сохранены.

2.1.5. Вкладка «События»

Вкладка «События» содержит перечень всех событий, произошедших на устройстве (рис. 25).

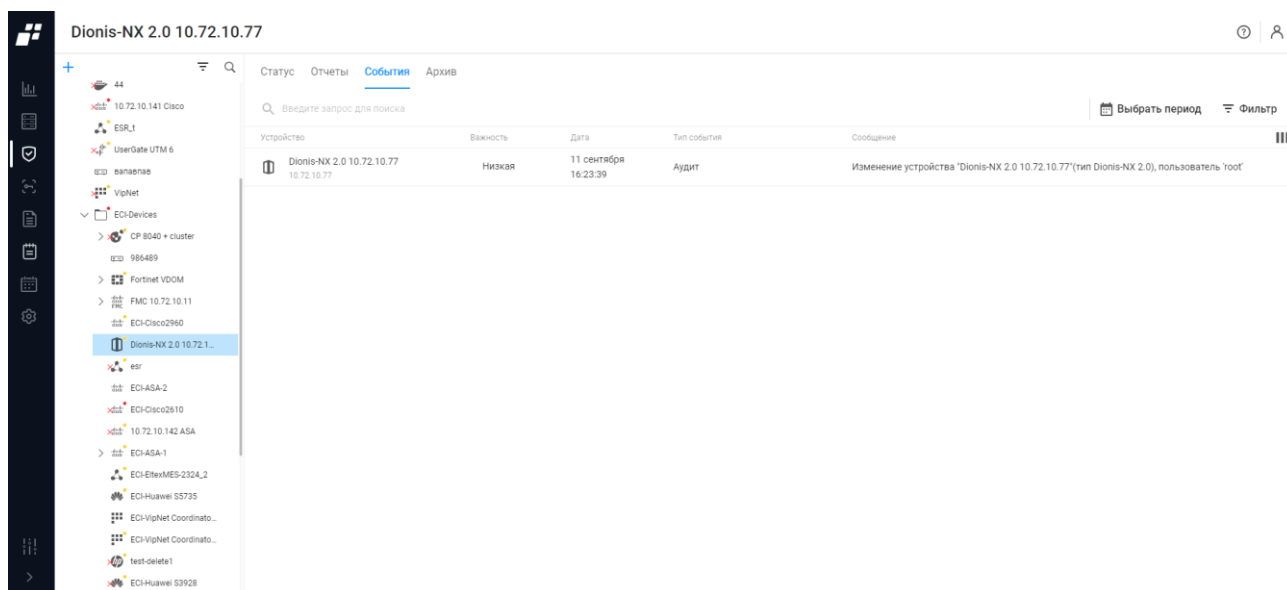


Рисунок 25 – Вкладка «События»

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

- устройство – содержит пиктограмму производителя устройства, название и/или IP-адрес.
- важность – уровень значимости зафиксированного события.
- дата – дата фиксации события в числовом формате.
- тип события – событие, зафиксированное на устройстве.
- сообщение – краткое описание произошедшего на устройстве события.

Над списком событий располагаются:

- поле поиска (🔍 Введите запрос для поиска) для поиска искомой записи в списке;
- кнопка «Выбрать период» (📅 Выбрать период) позволяет задать период для отображения событий в определенный промежуток времени;
- кнопка «Фильтр» (≡ Фильтр) для фильтрации событий по заданным параметрам;
- кнопка «Колонки» (≡) для изменения отображения колонок на странице.

Состав вкладки «События» для группы устройств аналогичен составу вкладке «События» для одного устройства.

2.1.5.1. Фильтрация

Для фильтрации событий необходимо нажать кнопку «Фильтр» (≡ Фильтр). Откроется окно фильтрации, приведенное на рис. 26. Состав и описание Полей окна фильтрации приведены в таблице 6.

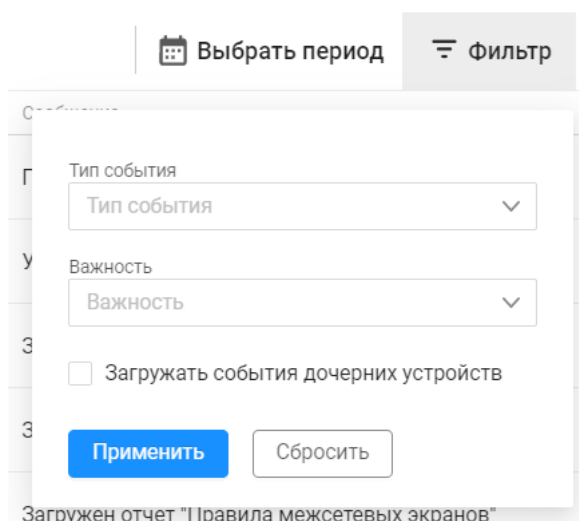




Рисунок 26 – Окно фильтрации

Таблица 6 – Состав и описание Полей окна фильтрации на вкладке «События»

Поле	Описание
Поле «Тип события»	Выбор типа события из раскрывающегося списка
Поле «Важность»	Выбор важности события: — высокая; — средняя; — низкая
Поле «Загружать события дочерних устройств»	Поле для простановки флага: загружать события дочерних устройств
Элементы управления	
Применить	По нажатию кнопки окно фильтрации закрывается, введенные настройки фильтрации применяются
Сбросить	По нажатию кнопки окно фильтрации закрывается без применения введенных настроек

Далее необходимо заполнить параметры фильтрации и нажать кнопку «Применить». На странице отобразятся события, соответствующие заданным параметрам фильтрации. Для отмены заданных правил фильтрации и отображения в списке всех записей необходимо повторно нажать на кнопку «Фильтр» и нажать кнопку «Сбросить». Для фильтрации по периоду необходимо нажать кнопку « Выбрать период» и в открывшемся окне-календаре задать начало и конец периода.

2.1.6. Вкладка «Архив»

Вкладка «Архив» содержит список всех загруженных в БД комплекса версий отчетов устройства/группы устройств, для которых установлен режим использования «Архив версий» или «Контроль изменений» (рис. 27). В архив попадают текстовые «», структурированные «» отчеты и отчеты типа «Проверки».

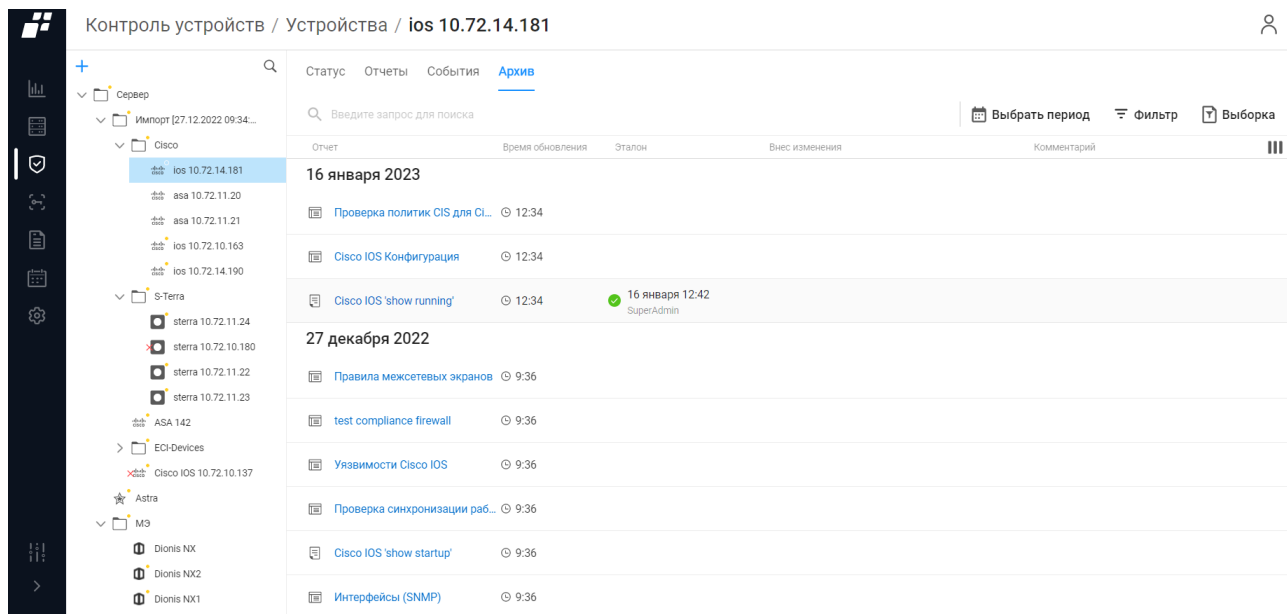




Рисунок 27 – Вкладка «Архив»

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

- отчет – содержит пиктограмму типа отчета и название отчета;
- время обновления – дата последнего обновления отчета в числовом формате;
- эталон – содержит пиктограмму с датой, если архивная версия отчета принята за эталон;
- внес изменения – логин пользователя, внесшего изменения в отчет;
- комментарий – пояснения по отчету.

Над списком отчетов располагаются:

- поле поиска ( Введите запрос для поиска) для поиска искомой записи в списке;
- кнопка «Выбрать период» ( Выбрать период) позволяет задать период для отображения архивных отчетов в определенный промежуток времени;
- кнопка «Фильтр» ( Фильтр) для фильтрации списка архивных отчетов;
- кнопка «Выборка» ( Выборка) для создания отчета типа «Выборка» (более подробно см. п.п. 0);
- кнопка «Колонки» () позволяет определить отображение необходимых столбцов на странице. При необходимости с помощью флага можно менять

количество отображаемых столбцов на странице. Первый столбец всегда отображается на странице.

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. 28 приведена страница структурированного отчета.

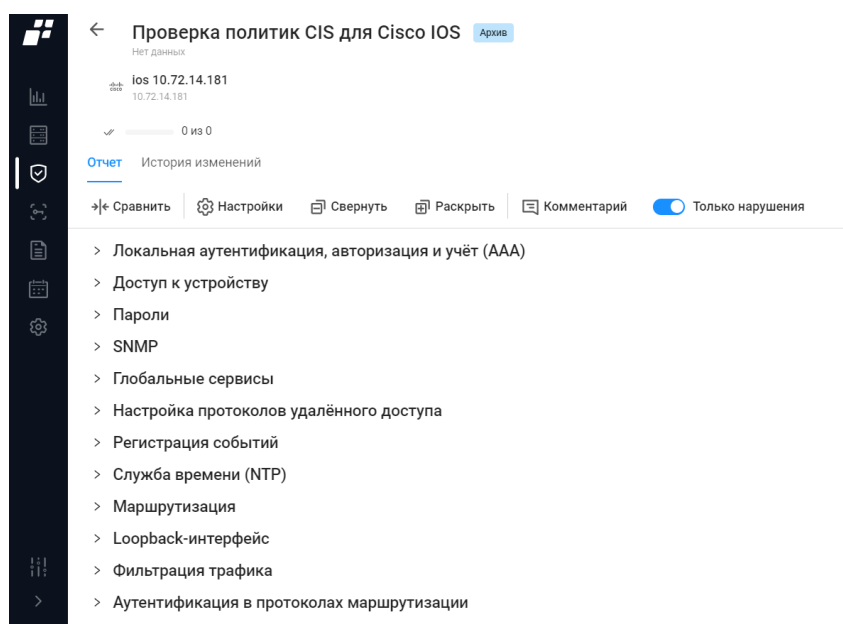


Рисунок 28 – Страница структурированного отчета, вкладка «Отчет»

Над страницей располагаются:

- кнопка «Сравнить» (Сравнить) для сравнения ранее загруженных на сервер ПК «Efros DO» версий этого отчета;
- кнопка «Настройки» (Настройки) позволяет настроить использование отчета;
- кнопка «Свернуть» (Свернуть) позволяет преобразовать представление отчета в табличный вид. Кнопка отображается только для структурированных отчетов;
- кнопка «Раскрыть» (Раскрыть) позволяет преобразовать представление отчета в виде дерева. Кнопка отображается только для структурированных отчетов;
- кнопка «Комментарий» (Комментарий) позволяет оставить комментарий к отчету;
- переключатель «Только нарушения» позволяет включить отображение только нарушений. Кнопка отображается только для структурированных отчетов.

На рис. 29 приведена страница текстового отчета.

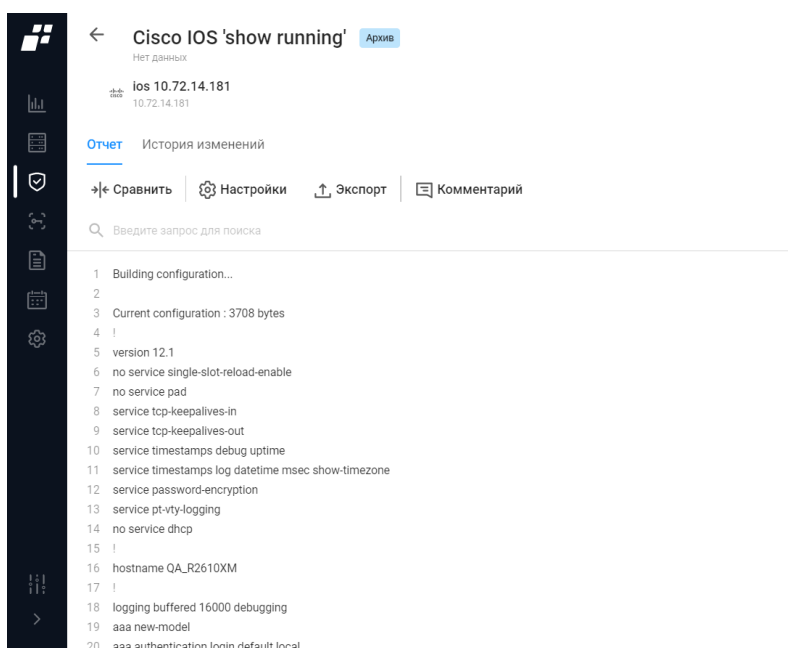






Рисунок 29 – Страница текстовой формы отчета, вкладка «Отчет»

Над страницей располагаются:

- кнопка «Сравнить» ( Сравнить) для сравнения ранее загруженных на сервер ПК «Efros DO» версий этого отчета;
- кнопка «Настройки» ( Настройки) позволяет настроить использование отчета;
- кнопка «Экспорт» ( Экспорт) выгрузка отчета на рабочую машину;
- кнопка «Комментарий» ( Комментарий) позволяет оставить комментарий к отчету.

Для просмотра истории изменений архивного отчета необходимо перейти на вкладку «История изменений». На рис. 30 показана вкладка «История изменений» для структурированной формы отчета.

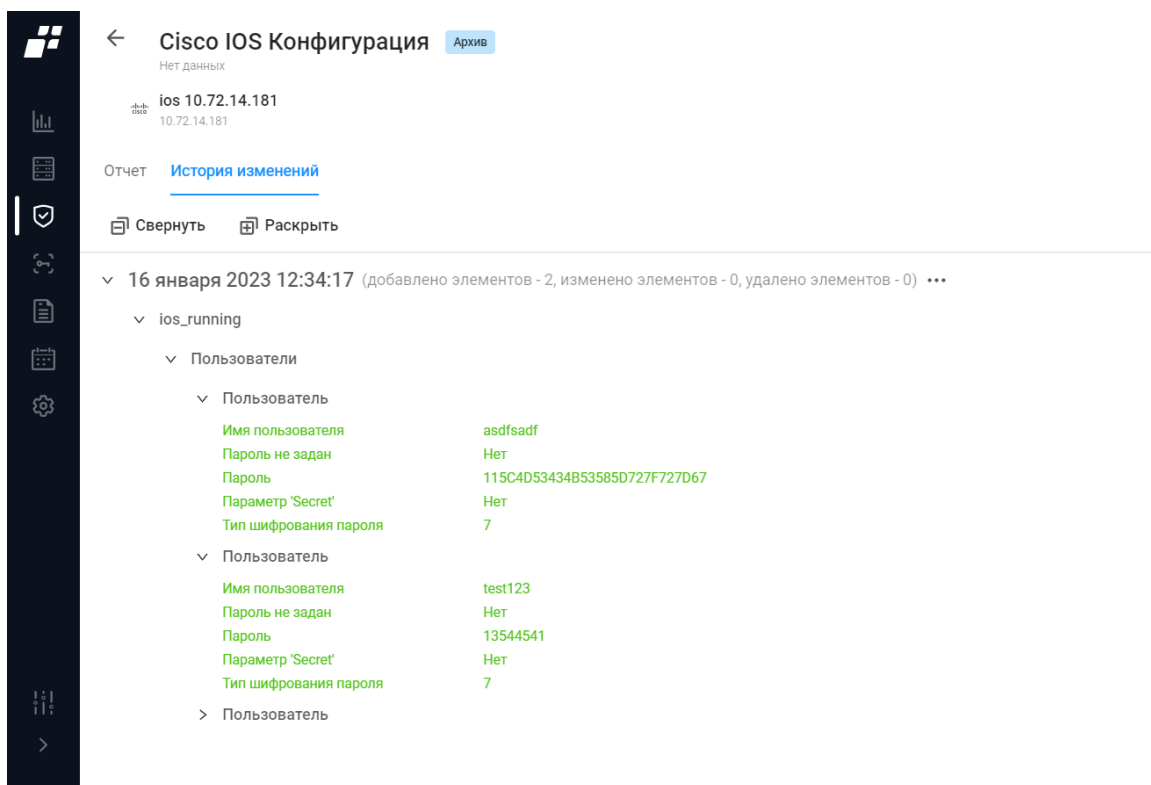


Рисунок 30 – Структурированная форма отчета, вкладка «История изменений»


На рис. 31 показана вкладка «История изменений» для текстовой формы отчета.



Рисунок 31 – Текстовая форма отчета, вкладка «История изменений»

2.1.6.2. Создание отчета «Выборка»

Для создания отчета «Выборка» необходимо выполнить следующие шаги:

- 1) Нажать на кнопку «Выборка» ( Выборка). Откроется окно создания отчета, приведенное на рис. 32. Состав Полей окна и правила их заполнения приведены в таблице 7.

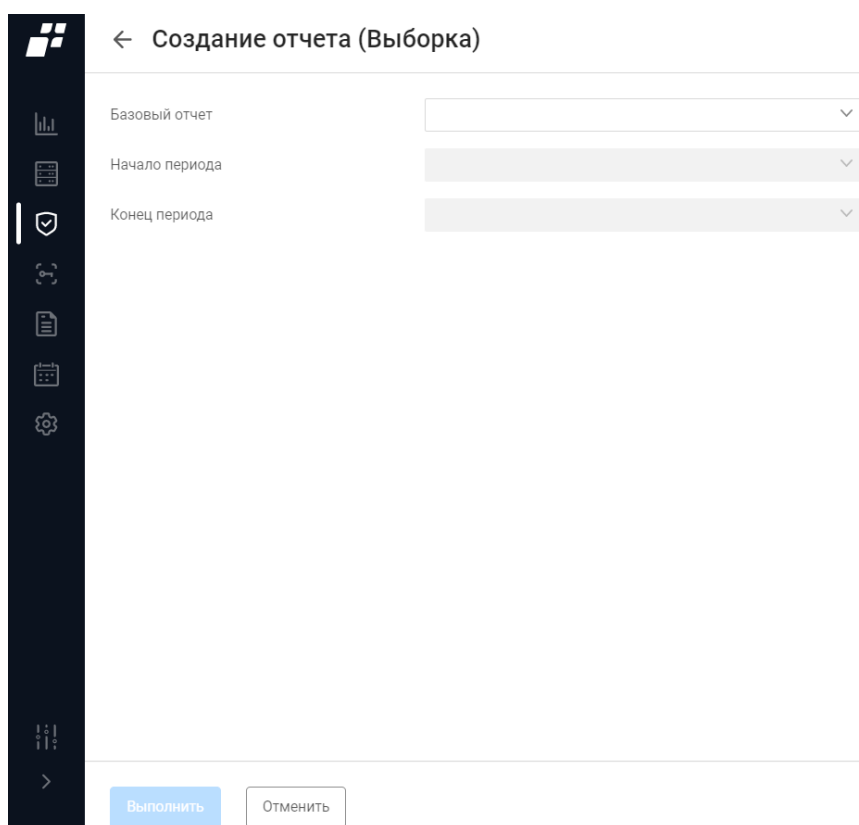
Скриншот интерфейса программы. Вверху окна заголовок «Создание отчета (Выборка)» с кнопкой «Назад». Слева — темная панель с иконками: диаграмма, таблица, отчет с галочкой (выделен), диаграмма, документ, календарь, настройки. В центре три поля: «Базовый отчет» (выпадающий список), «Начало периода» (выпадающий список), «Конец периода» (выпадающий список). Внизу — кнопки «Выполнить» (синяя) и «Отменить» (серая).

Рисунок 32 – Окно создания отчета (Выборка)

Таблица 7 – Состав и описание Полей окна создания отчета

Поле	Описание
Поле «Базовый отчет»	Выбор варианта базового отчета, на основании которого будет формироваться отчет «Выборка»
Поле «Начало периода»	Предлагается автоматически после выбора базового отчета
Поле «Конец периода»	Предлагается автоматически после выбора базового отчета
Элементы управления	
Выполнить	При нажатии кнопки введенные данные сохраняются
Отменить	При нажатии кнопки окно закрывается без применения введенных данных


- 2) Заполнить поля окна соответствующими параметрами.

3) Нажать кнопку «Выполнить».

Автоматически запускается процесс проверки заполнения всех обязательных полей и уникальности добавляемого отчета по названию.

При обнаружении незаполненных обязательных полей под полем появится сообщение красного цвета: «Обязательное поле». Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Выполнить».

2.1.6.3. Фильтрация

Для фильтрации отчетов необходимо нажать кнопку «Фильтр» ( Фильтр). Откроется окно фильтрации, приведенное на рис. 33. Состав Полей окна и правила их заполнения приведены в таблице 8.

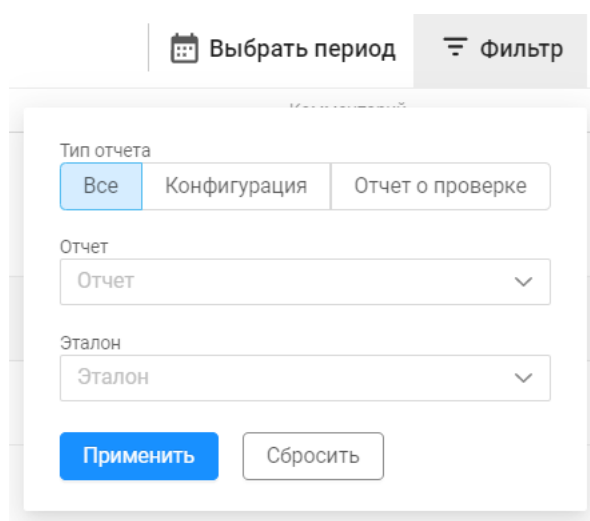


Рисунок 33 – Окно фильтрации

Таблица 8 – Состав и описание Полей окна фильтрации на вкладке «Архив»

Поле	Описание
Поле «Тип отчета»	Переключатель: <ul style="list-style-type: none">— «Все»;— «Конфигурация»;— «Отчет о проверке»
Поле «Отчет»	Поле с раскрывающимся перечнем отчетов (зависит от типа устройства). Для выбора отчета необходимо поставить флаг в соответствующем поле
Поле «Эталон»	Поле с вариантами: <ul style="list-style-type: none">— «Нет»;— «Эталон»;— «Архивный эталон». Для выбора необходимого параметра нужно проставить флаг в соответствующем поле

Поле	Описание
Элементы управления	
Применить	По нажатию кнопки окно фильтрации закрывается, введенные настройки фильтрации применяются
Сбросить	По нажатию кнопки окно фильтрации закрывается без применения введенных настроек



Далее необходимо заполнить параметры фильтрации и нажать кнопку «Применить». После чего окно фильтрации закроется, на странице отобразятся архивные отчеты, соответствующие заданным параметрам фильтрации. Для отмены заданных правил фильтрации и отображения в списке всех записей необходимо повторно нажать на кнопку «Фильтр» и нажать кнопку «Сбросить».

— вкладка «База требований».

2.2.1. Дерево со списком типов устройств

Иерархический список стандартов, сгруппированный по типам устройств.



Над деревом доступны следующие функции:

- кнопка «Фильтр» () для фильтрации списка типов устройств;
- поле поиска () для поиска искомой записи в списке.




2.2.2. Вкладка «Стандарты»

Вкладка «Стандарты» содержит перечень стандартов проверок безопасности для выделенного в дереве типа устройства (см. рис. 34).

На вкладке отображается следующая информация:


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

Над списком стандартов располагаются:

- поле поиска () для ввода последовательности символов из искомой записи;
- кнопка «Фильтр» ( **Фильтр**) для фильтрации стандартов по типу стандарта;
- кнопка «Стандарт» ( **Стандарт**) для создания нового пользовательского стандарта (см. п.п. 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 на вкладке «Стандарты» кнопку «Стандарт» ( **Стандарт**).
- 2) На открывшейся странице «Создание стандарта безопасности» (рис. 35) заполнить поля необходимыми параметрами. Состав и описание полей окна «Создание стандарта безопасности» приведены в таблице 9.
- 3) Нажать кнопку «Создать».

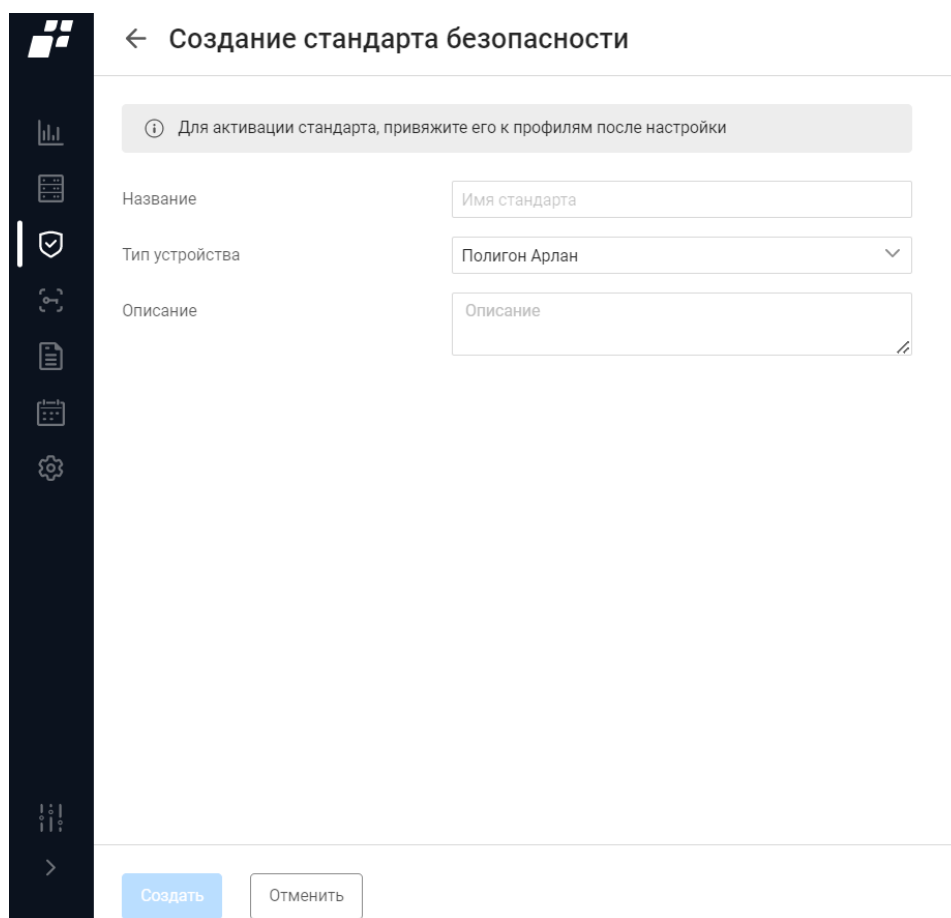



Рисунок 35 – Страница «Создание стандарта безопасности»

Таблица 9 – 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 «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. Необходимо добавить требования (см. п.п. 2.2.2.2) и, при необходимости, изменить параметры режима их использования на контролируемых в комплексе устройствах (см. п. 2.2.3). Создание пользовательского стандарта возможно с помощью кнопки «Копировать»

(). Кнопка появляется при наведении курсора на строку предустановленного стандарта. Далее откроется окно создания стандарта безопасности (рис. 35). 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;
- 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. 36).

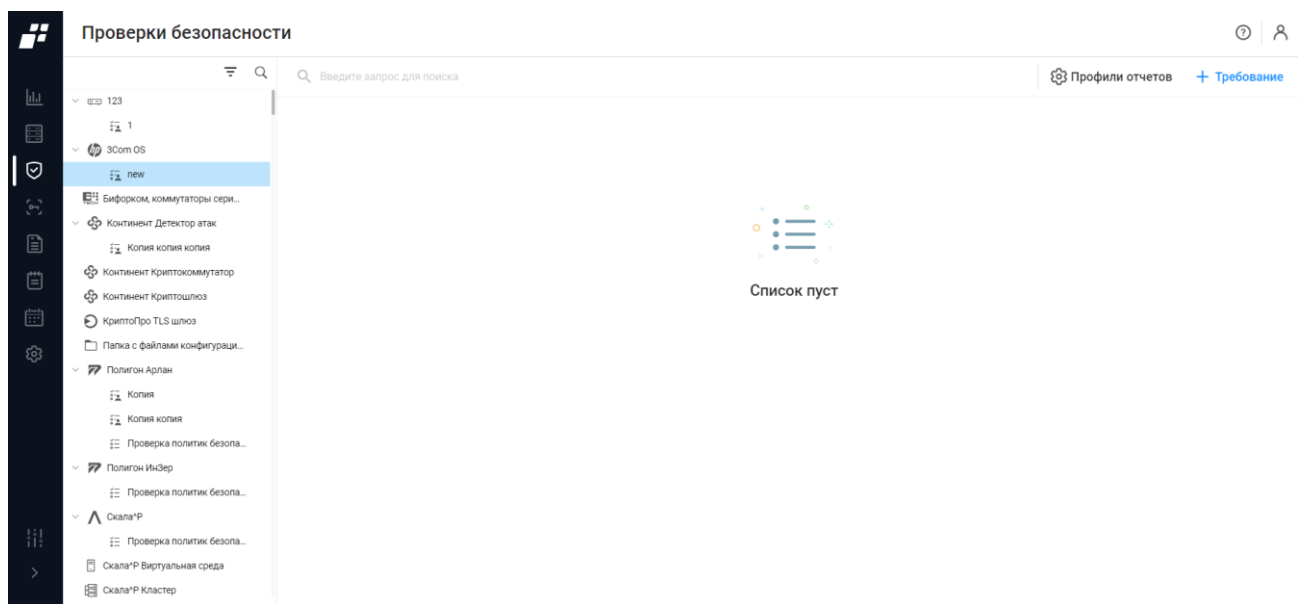


Рисунок 36 – Страница с пользовательским стандартом


- 3) Нажать на кнопку «Требование» ( **Требование**) и выбрать из контекстного меню пункт «Создать новое».
- 4) На открывшейся странице «Создание требования» (рис. 37) заполнить необходимые поля и нажать кнопку «Создать». Состав и описание полей окна «Создание требования» приведены в таблице 10.


Рисунок 37 – Страница «Создание требования»

Таблица 10 – 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»	Поле с раскрывающимся списком существующих категорий по базе требований для выбранного производителя. Также можно создать новую категорию
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»; — «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
Поле «Тестирование требования»	Поле для проверки выполнения требования с заданными условиями
Элементы управления	
Создать	При нажатии кнопки выполняется сохранение внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу без сохранения внесенных данных

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

- 1) Нажать на кнопку «Требование» ( **Требование**) и из контекстного меню выбрать пункт «Выбрать».
- 2) В открывшемся окне «Выбор требований» (рис. 38) можно выбрать требования из общей базы требований или из требований для конкретного типа устройства.

✕ Выбор требований

База требований ▼

База требований
Проверка политик безопасности для Eitex MES

Фильтр

☐ Название и описание

☐ SNMP

- ☐ Необходим запрет доступа по протоколу SNMP без ограничений доступа группами
Если Group при использовании SNMP не применяются, то потенциально возможна атака с любого адреса сети. Необходимо ог...
- ☐ Необходим запрет доступа по протоколу SNMP с правами на запись
Доступ по протоколу SNMP с правами на запись позволяет удалённо управлять устройством. Рекомендуется отключать SNMP...
- ☐ Необходим запрет на использование в SNMP community строки 'private'
Название 'private' достаточно распространено, а использование заранее известных данных для получения неавторизованног...
- ☐ Необходим запрет на использование в SNMP community строки 'public'
Проверьте, что настройках SNMP нет стандартных строк community. Проверка: hostname# sh run | in community
- ☐ Необходим запрет на использование протокола SNMP
Протокол SNMP позволяет производить управление и мониторинг сетевыми устройствами. Требуется отключить данный про...
- ☐ Необходимо разрешить отправку SNMP trap при попытке аутентификации
Необходимо разрешить отправку SNMP trap сообщений с параметрами аутентификации. Проверка: hostname#sh snmp
- ☐ При использовании SNMP, необходимо настроить SNMP trap сервер
Если SNMP включён и разрешены сообщения trap, то необходимо настроить разрешения trap только для систем управления, п...
- ☐ Требуется настроить группы для доступа по протоколу SNMP v3
SNMP v3 поддерживает более высокий уровень безопасности благодаря возможности использовать аутентификацию и шифр...

Всего: 48 Выбранных: 0

Добавить Отменить

Рисунок 38 – Окно «Выбор требований»


Состав и описание Полей окна «Выбор требований» приведены в таблице 11.

Таблица 11 – Состав и описание Полей окна «Выбор требований»

Поле	Описание
Поле «Источник требования»	Поле с выбором источника требования: — база требований; — требования для конкретного типа устройств
Поле «Список требований»	Список требований, зависящий от выбора в поле «Источник требований»
Элементы управления	
Поле «Поиск»	Поиск символов из искомой записи
Кнопка «Фильтр»	Для фильтрации списка требований
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 пользовательского стандарта

Для настройки пользовательской проверки безопасности необходимо, после добавления требований и их редактирования, выполнить настройку использования пользовательского стандарта. Для этого необходимо:

- 1) В дереве типов устройств выделить тип устройства, которому был добавлен пользовательский стандарт.
- 2) В заголовке открывшейся страницы пользовательского стандарта нажать кнопку «Профили отчетов» ( Профили отчетов).

В открывшемся окне выполнить настройку использования стандарта проверки для всех устройств, к которым он может быть применен. Для этого в области «Использование» в раскрывающемся списке выбрать значение «Разрешено».

2.2.3. Вкладка «База требований»

Вкладка «База требований» содержит список требований безопасности для выделенного типа устройств в дереве типов устройств (рис. 39).

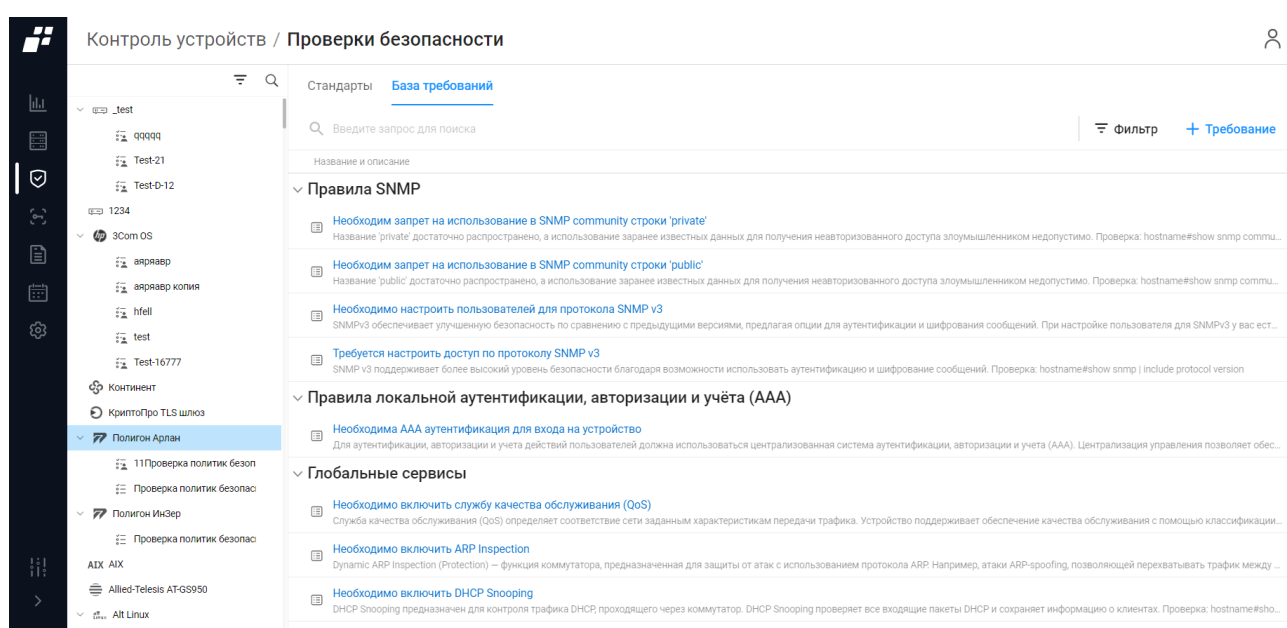





Рисунок 39 – Вкладка «База требований»

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

- иконка требования;
- название и описание требования.

Над списком требований располагаются:

- поле поиска ( Введите запрос для поиска) для поиска искомой записи в списке;
- кнопка «Фильтр» ( Фильтр) для фильтрации списка стандартов;
- кнопка «Требование» ( Требование) для создания нового пользовательского требования или выбора требования из базы требований (см. п.п. 2.2.2.2).

2.2.3.1. Редактирование пользовательских проверок безопасности

Для редактирования пользовательских проверок безопасности необходимо выполнить следующее:

- 1) В дереве типов устройств выделить тип устройства, которому была добавлена пользовательская проверка безопасности.
- 2) Выбрать созданную проверку безопасности.
- 3) Выбрать требование, которое необходимо откорректировать, и нажать на название требования. Появится окно для внесения изменений (рис. 40). Состав и описание Полей окна приведено в таблице 12.

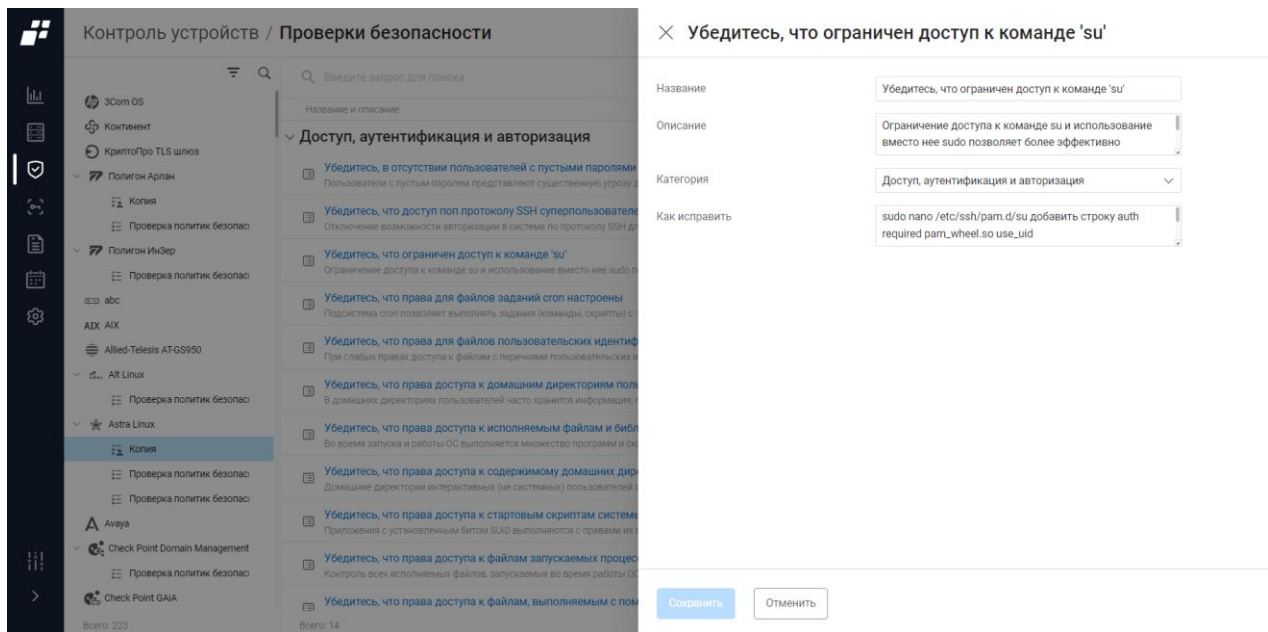


Рисунок 40 – Окно просмотра настроек требования

Таблица 12 – 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 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


4) Внести необходимые изменения в поля окна и нажать кнопку «Сохранить».

Автоматически запустится процесс проверки заполнения всех обязательных полей и уникальности добавляемой проверки безопасности.

При обнаружении незаполненных обязательных полей под полем появится сообщение красного цвета: «Обязательное поле». Пользователю необходимо корректно заполнить поля страницы и повторно нажать кнопку «Сохранить».

2.2.3.2. Настройки пользовательских проверок безопасности

Для настройки пользовательской проверки безопасности необходимо выполнить следующее:

- 1) В дереве типов устройств выделить тип устройства, которому был добавлен пользовательский стандарт.
- 2) В заголовке открывшейся страницы пользовательского стандарта нажать кнопку «Профили отчетов» ( Профили отчетов).

В открывшемся окне выполнить настройку использования стандарта проверки для всех устройств, к которым он может быть применен. Для этого в области «Использование» в раскрывающемся списке выбрать значение «Разрешено».

2.3 Проверки МЭ

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

В данном подразделе 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:

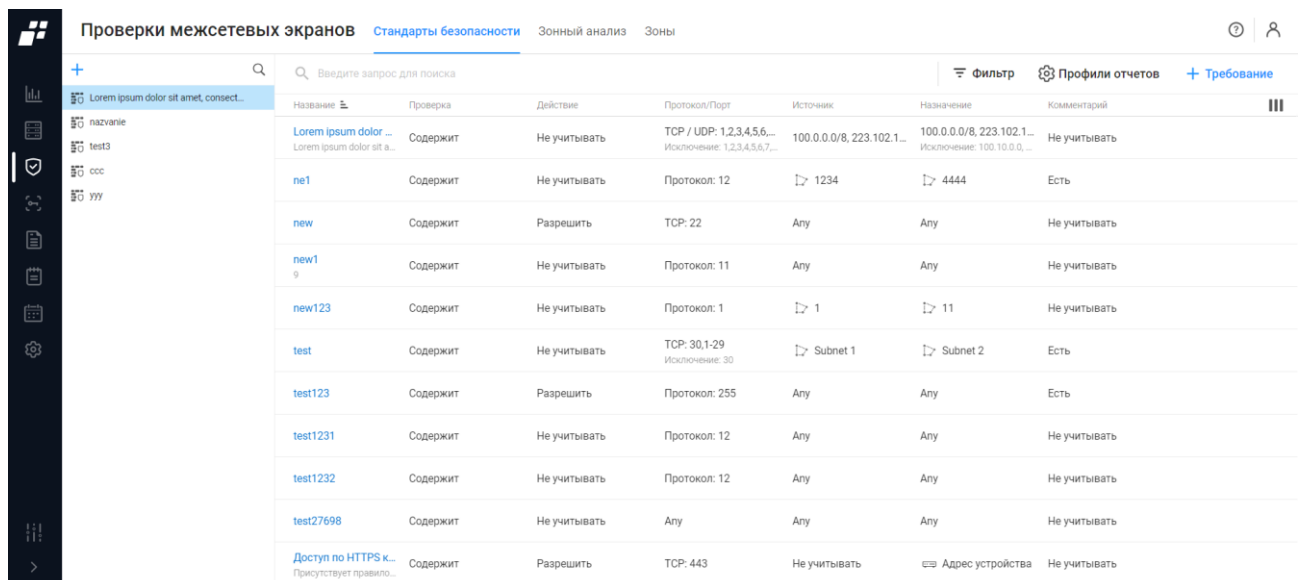
- «Стандарты безопасности»;
- «Зонный анализ»;
- «Зоны».

2.3.1. Вкладка «Стандарты безопасности»

i 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 в окно создания стандарта безопасности.

Рабочая область вкладки «Стандарты безопасности» (рис. 41) включает в себя:

- дерево стандартов безопасности;
- перечень требований в виде таблицы.






Название	Проверка	Действие	Протокол/Порт	Источник	Назначение	Комментарий
>Lorem ipsum dolor sit amet, consectetur adipiscing elit...	Содержит	Не учитывать	TCP / UDP: 1,2,3,4,5,6... Исключение: 1,2,3,4,5,6,7...	100.0.0.0/8, 223.102.1...	100.0.0.0/8, 223.102.1... Исключение: 100.10.0.0...	Не учитывать
ne1	Содержит	Не учитывать	Протокол: 12	1234	4444	Есть
new	Содержит	Разрешить	TCP: 22	Any	Any	Не учитывать
new1	Содержит	Не учитывать	Протокол: 11	Any	Any	Не учитывать
new123	Содержит	Не учитывать	Протокол: 1	1	11	Не учитывать
test	Содержит	Не учитывать	TCP: 30,1-29 Исключение: 30	Subnet 1	Subnet 2	Есть
test123	Содержит	Разрешить	Протокол: 255	Any	Any	Есть
test1231	Содержит	Не учитывать	Протокол: 12	Any	Any	Не учитывать
test1232	Содержит	Не учитывать	Протокол: 12	Any	Any	Не учитывать
test27698	Содержит	Не учитывать	Any	Any	Any	Не учитывать
Доступ по HTTPS к...	Содержит	Разрешить	TCP: 443	Не учитывать	Адрес устройства	Не учитывать

Рисунок 41 – Подраздел «Проверки МЭ»

Над деревом стандартов располагаются:

- кнопка «Создание стандарта» (+) для создания нового стандарта;
- поле поиска (Q) для поиска искомой записи в списке.



При наведении курсора на строку с необходимым стандартом в дереве стандартов в правом углу строки появится контекстное меню «». При раскрытии контекстного меню следующие кнопки:

- кнопка «Создать копию» () для создания копии стандарта безопасности;
- кнопка «Удалить» () для удаления стандарта безопасности.

Над списком требований располагаются:


- поле поиска ( Введите запрос для поиска) для поиска искомой записи в списке;
- кнопка «Фильтр» ( Фильтр) для фильтрации списка требований;
- кнопка «Профили отчетов» ( Профили отчетов) для настройки использования пользовательского требования;
- кнопка «Требование» ( Требование) для создания нового требования или для копирования требований из существующего стандарта;
- кнопка «Колонки» () позволяет определить отображение необходимых столбцов на странице. При необходимости с помощью флага можно менять количество отображаемых столбцов на странице. Первый столбец всегда отображается на странице.

При наведении курсора на требование, в правой части экрана появляются следующие кнопки:

- кнопка «Создать копию» () для создания копии требования;
- кнопка «Удалить» () для удаления требования.

2.3.1.1. Создание нового стандарта безопасности

Для создания нового пользовательского стандарта безопасности необходимо выполнить следующие действия:

- 1) В дереве стандартов безопасности нажать кнопку добавления стандарта () или кнопку «Создать стандарт», если стандарт создается впервые после установки комплекса.
- 2) В открывшемся окне «Создание стандарта безопасности» (рис. 42) заполнить необходимые поля и нажать кнопку «Создать». Состав и описание полей окна приведено в таблице 13.

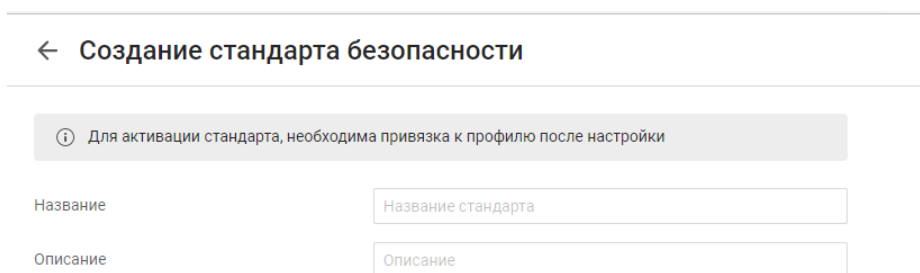


Рисунок 42 – Страница «Создание стандарта безопасности»

Таблица 13 – 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

Добавленный стандарт безопасности не содержит требований. Необходимо добавить требования в созданный стандарт и, при необходимости, изменить параметры режима его использования на контролируемых комплексом устройствах.


Добавление требований в стандарты возможно путем:

- создания новых пользовательских требований;
- копирования требований из существующих стандартов безопасности.

2.3.1.2. Создание нового требования

 После установки ПК «Efros DO» список требований пуст, на странице отображается сообщение «Список требований пуст» и кнопки «Создать новое», «Копировать из стандарта».

Для создания нового пользовательского требования необходимо:

- 1) Нажать кнопку «Требование» ( **Требование**) и из контекстного меню выбрать пункт «Создать новое».
- 2) На открывшейся странице «Создание требования» (рис. 43) заполнить необходимые поля и нажать кнопку «Создать». Состав и описание полей окна

«Создание требования» приведены в таблице 14.

← Создание требования

❗ В требовании должно быть не более 2-х условий "Не учитывать"

Название

Название требования

Описание

Описание

Проверка ❗

Содержит

Не содержит

Действие

Не учитывать

Разрешить

Запретить

Протоколы / порты

Не учитывать

Алу

Значение

Источник

Не учитывать

Алу

Зона

Подсеть

Назначение

Не учитывать

Алу

Зона

Подсеть

Комментарий

Не учитывать

Есть

Нет

Тестирование

Объекты защиты

Выберите объект защиты

Посмотреть отчет

Создать

Отменить

Рисунок 43 – Окно «Создание требования»

Таблица 14 – Состав и описание полей окна 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; — «Не содержит» – стандарт не содержит проверки
Поле «Действие»	Поле с переключателями: — «Не учитывать»; — «Разрешить»; — «Запретить»
Поле «Протоколы/Порты»	Поле с переключателями: — «Не учитывать»;

Поле	Описание
	— «Any»; — «Значение»
Поле «Протоколы»*	Раскрывающийся список для выбора протокола и указания порта
Поле «Исключение портов»*	Текстовое поле для ввода исключенного порта(ов) для обмена данными
Поле «Источник»	Поле с переключателем: — «Не учитывать»; — «Any»; — «Зона»; — «Подсеть»
Поле «Внутренние адреса»**	Поле с раскрывающимся списком адресов зон
Кнопка «Добавить исключение»**	Для добавления поля с адресом зоны для исключения
Поле «Адрес устройства»***	Поле для ввода IP-адреса устройства
Поле «Исключение»***	Поле для ввода IP-адресов, которые будут исключаться из подсети
Поле «Назначение»	Поле с переключателем: — «Не учитывать»; — «Any»; — «Зона»; — «Подсеть»
Поле «Внутренние адреса»***	Поле с раскрывающимся списком адресов
Кнопка «Добавить исключение»***	Для добавления поля с адресом зоны для исключения
Поле «Адрес устройства»***	Поле для ввода IP-адреса устройства
Поле «Исключение»***	Поле для ввода IP-адресов, которые будут исключаться из подсети
Поле «Комментарий»	Поле с переключателями: — «Не учитывать»; — «Есть»; — «Нет»

Поле	Описание
Тестирование	
Поле «Объекты защиты»	Поле со ссылкой на существующие ОЗ в БД комплекса
Кнопка «Посмотреть отчет»	При нажатии кнопки позволяет увидеть создаваемое требование в режиме тестирования
Элементы управления	
Создать	При нажатии кнопки выполняется сохранение внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу без сохранения внесенных данных
* Поля появляются при выборе переключателя «Значение»; **Поля появляются при выборе переключателя «Зона»; ***Поля появляются при выборе переключателя «Подсеть»	

Для активации добавленного стандарта необходимо после добавления требований или редактирования, выполнить настройку использования пользовательского стандарта:

- 1) В дереве списка стандартов выделить добавленный стандарт.
- 2) Нажать кнопку «Профили отчетов» (⚙️ **Профили отчетов**).
- 3) В открывшемся окне (рис. 44) выполнить настройку использования стандарта безопасности для всех устройств, к которым он может быть применен. Для этого в области «Использование» в раскрывающемся списке выбрать значение «Разрешено».

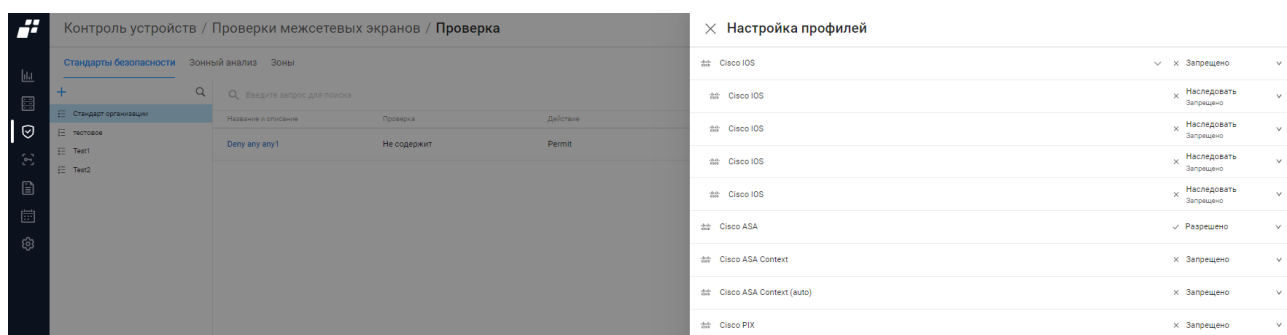


Рисунок 44 – Окно «Настройка профилей»

2.3.1.3. Копирование требования

Для добавления требований в стандарт безопасности из базы требований существующих стандартов безопасности, необходимо выполнить следующие действия:

- 1) Нажать кнопку «Требование» (+ **Требование**) и из раскрывающегося списка выбрать «Копировать из стандарта». На рис. 45 приведено окно

«Выбор требований».

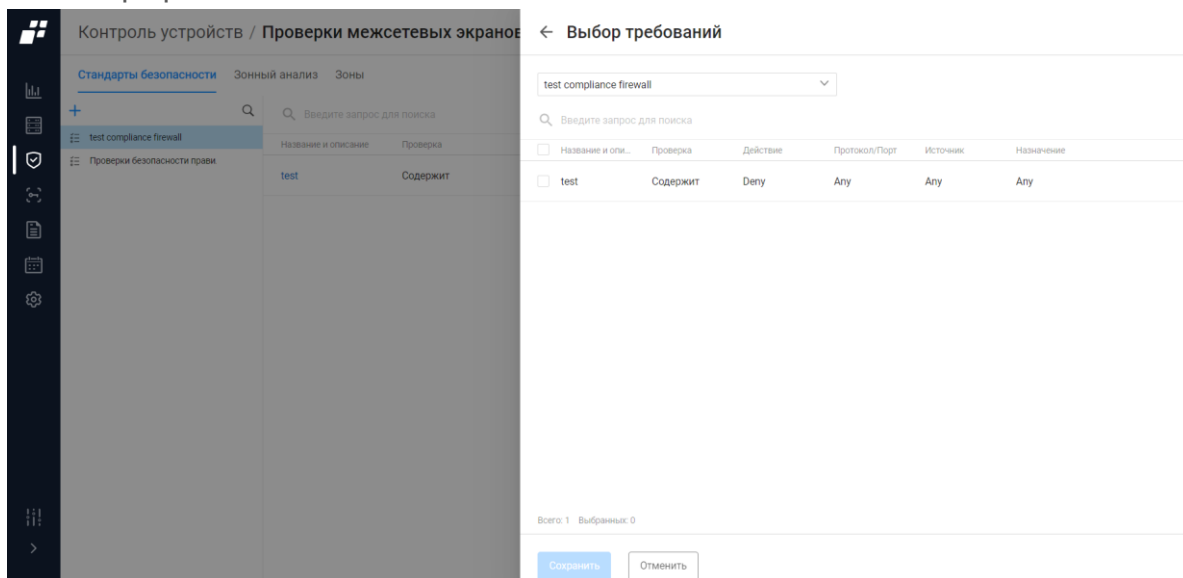


Рисунок 45 – Окно «Выбор требований»

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

2.3.2. Вкладка «Зонный анализ»



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

Вкладка «Зонный анализ» (рис. 46) предназначена для проверки транзитного трафика по зонам.

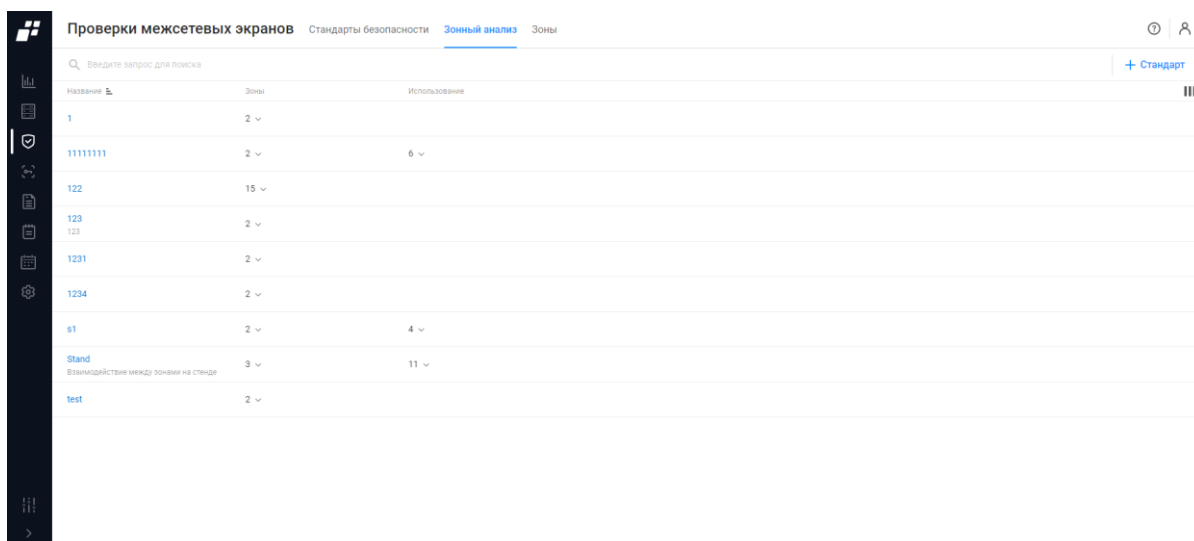





Рисунок 46 – Вкладка «Зонный анализ»




Список реализован в виде таблицы. Для каждой записи списка отображаются следующие данные:

- название стандарта зонного анализа;
- количество зон, которые стандарт контролирует;
- информация о том, в каких профилях отчетов используется стандарт зонного анализа (количество профилей отчетов).

Над списком стандартов располагаются:

- кнопка «Стандарт» ( Стандарт) для создания нового стандарта зонного анализа»;
- поле поиска ( Введите запрос для поиска) для поиска искомой записи в списке;
- кнопка «Колонки» () для изменения отображения колонок на странице.

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


- кнопка «Создать копию» () позволяет создать копию стандарта;
- кнопка «Удалить» () позволяет удалить выбранный стандарт;
- кнопка «Использование» () позволяет настроить использование стандартов зонного анализа для определенных профилей отчетов.

Добавление требований в стандарты возможно путем:

- создание новых пользовательских требований;
- копирование требований из существующих стандартов зонного анализа.

2.3.2.1. Создание нового стандарта зонного анализа

Для создания нового пользовательского стандарта зонного анализа необходимо выполнить следующие действия:

- 1) В дереве стандартов зонного анализа нажать кнопку добавления стандарта ( Стандарт).
- 2) В открывшемся окне «Создание стандарта зонного анализа» (рис. 47) заполнить необходимые поля и нажать кнопку «Создать». Состав и описание полей окна приведены в таблице 15.

← Создание стандарта зонного анализа

Название

Описание

Использование ⓘ Выбор профилей отчетов доступен после создания стандарта

Зоны ⓘ

Зона

Зона


Матрица доступа

Выберите зоны

Невозможно построить матрицу, если выбрано менее 2-х зон

Рисунок 47 – Страница «Создание стандарта зонного анализа»

Таблица 15 – 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 «Зона»	Раскрывающийся список зон для формирования матрицы доступа
Поле «Матрица доступа»	Позволяет настроить требования запрета и/или разрешения трафика между зонами.  Матрица доступа автоматически заполняется после выбора зон в поле «Зоны».
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 и при необходимости изменить параметры режима его использования на контролируемых комплексом устройствах.

2.3.2.2. Создание нового требования для стандарта зонного анализа

Для создания нового пользовательского требования необходимо:

- 1) В матрице доступа выбрать зону и перейти по ссылке (на рис. 48. выделено красным цветом).

← Создание стандарта зонного анализа

Название:

Описание:

Использование ⓘ: Выбор профилей отчетов доступен после создания стандарта

Зоны ⓘ:

- ASU_TP-AZIMUT + [икона удаления] [икона просмотра]
- LOCAL-ESR + [икона удаления] [икона просмотра]

Матрица доступа


Источник \ Назначение	ASU_TP-AZIMUT	LOCAL-ESR
ASU_TP-AZIMUT		Не учитывать
LOCAL-ESR	Не учитывать	


Создать Отменить

Рисунок 48 – Окно «Создание стандарта зонного анализа»

- 2) В открывшемся окне (рис. 49) заполнить необходимые поля и нажать кнопку «Изменить». Состав и описание полей окна создания требования приведены в таблице 14.

✕ ASU_TP-AZIMUT - LOCAL-ESR

Источник ASU_TP-AZIMUT 

Назначение LOCAL-ESR 

Описание

Тип доступа

Рисунок 49 – Окно создания нового требования

Таблица 16 – Состав и описание полей окна создания нового требования

Поле	Описание
Поле «Источник»	Отправитель трафика. Определяется автоматически. Недоступен для корректировки
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»; — «Запрет»; — «Разрешение»
Поле «Запрет»	Появляется при выборе переключателя «Запрет». Переключатель: — «Полный»; — «Частичный»/ При выборе «Частичный» необходимо указать протокол обмена данными
Поле	Появляется при выборе переключателя «Разрешение».


Поле	Описание
«Разрешение»	Переключатель: — «Полное»; — «Частичное». При выборе «Частичное» необходимо указать протокол или порт обмена данными
Поле «Протокол/порт»	Раскрывающийся список: — «TCP»; — «UDP»; — «TCP/UDP»; — «ICMP»; — «Другой протокол». Поле появляется при выборе значения «Частичное» в поле «Запрет»
Поле «Остальные взаимодействия»	Позволяет настроить требования обратного действия. Переключатель: — «Не учитывать»; — «Полностью запрещены»; — «Частично запрещены». При выборе «Частично разрешены» необходимо указать протокол или порт обмена данными
Кнопка «Добавить исключения»	Раскрывающийся список: — «Источник»; — «Назначение»; — «Протокол/порт»
Элементы управления	
Создать	При нажатии на кнопку введенные данные сохраняются
Отменить	При нажатии на кнопку введенные данные не сохраняются

2.3.2.3. Копирование требования из стандарта зонного анализа

Для добавления стандарта с помощью копирования необходимо выполнить следующее:

- 1) Нажать кнопку «Сделать копию» (.
- 2) В открывшемся окне произвести корректировку необходимых параметров и нажать кнопку «Создать».

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. 50.) предназначена для создания необходимых зон для выполнения зонного анализа. На странице список зон реализован в виде дерева.

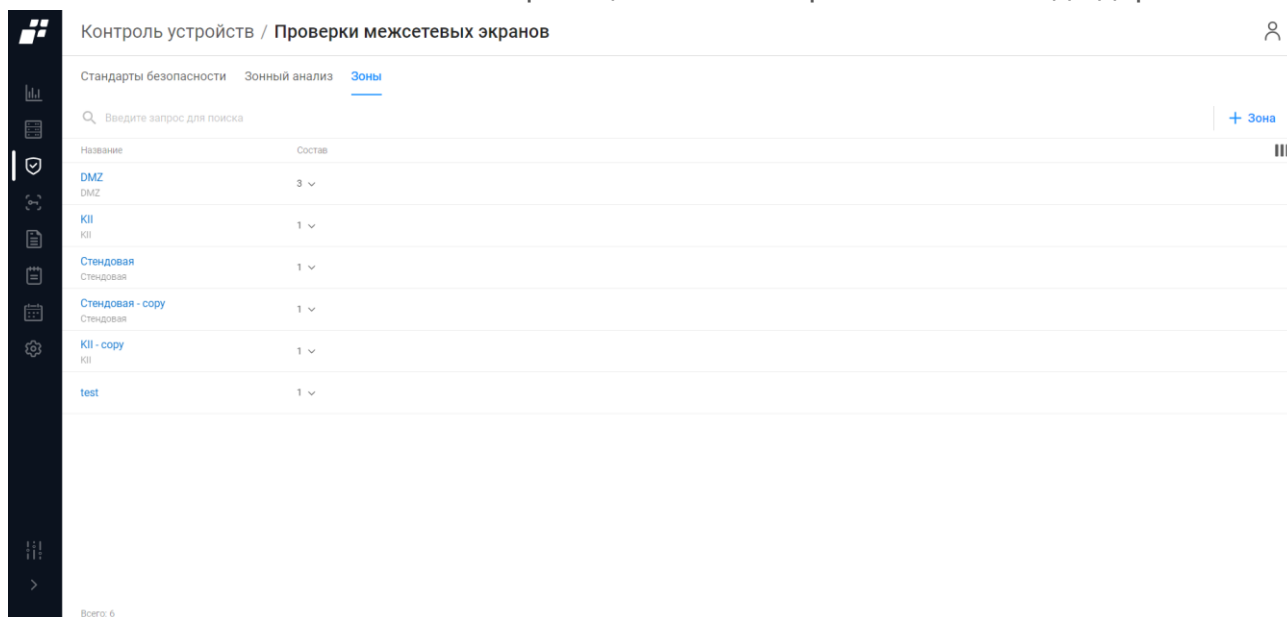


Рисунок 50 – Вкладка «Зоны»

Для каждой записи списка отображаются название зоны и состав зоны (IP-адрес/IP-адрес с маской/диапазон).

Над списком зон доступны следующие функции:

- кнопка «Зона» (Зона) открывает страницу «Создание зоны»;
- поле поиска (Введите запрос для поиска) для поиска искомой записи в списке;
- кнопка «Колонки» () для изменения отображения колонок на странице.

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

- кнопка «Создать копию» () позволяет создать копию зоны;
- кнопка «Удалить» () позволяет удалить выбранную зону.

2.3.3.1. Создание новой зоны

Для добавления новой зоны необходимо выполнить следующие действия:

- 1) Нажать кнопку «Зона» (Зона).
- 2) В открывшемся окне «Создание зоны» (рис. 51) заполнить необходимые поля и нажать кнопку «Создать». Состав и описание полей страницы приведены в таблице 17.

← Создание зоны

Название

Описание

Состав зоны ⓘ

☒ Подсеть ☐ Хост ☐ Диапазон

Рисунок 51 – Страница «Создание зоны»

Таблица 17 – 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»	Переключатель: — «Подсеть»; — «Хост»; — «Диапазон»
Элементы управления	
Создать	При нажатии на кнопку введенные данные сохраняются
Отменить	При нажатии на кнопку введенные данные не сохраняются

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. 52) 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.

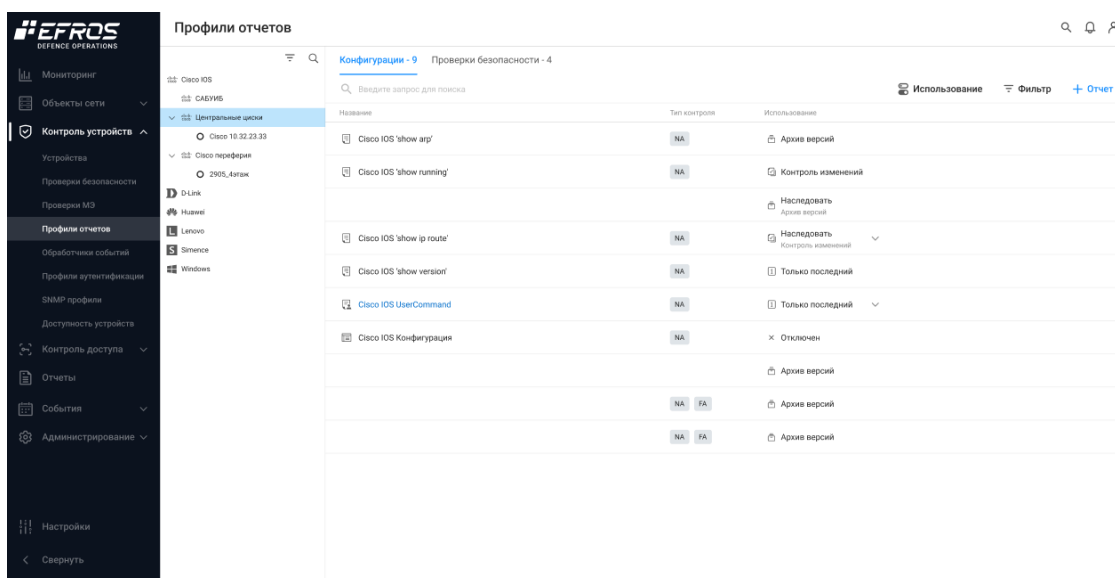


Рисунок 52 – Подраздел «Профили отчетов»



Рабочая область подраздела состоит из:

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

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. Администрирование»).

Над деревом доступны следующие функции:

- кнопка «Фильтр» () для фильтрации профилей отчетов по типу устройства;
- поле поиска ( Введите запрос для поиска) для поиска искомой записи в списке.

При наведении курсора на профиль отчета появится кнопка «Создание профиля»

отчетов» (**+**), которая позволяет создать пользовательский профиль отчета для выбранного типа устройства.

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

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

2.4.1.1. Создание пользовательского профиля отчетов

Для создания пользовательского профиля отчетов устройства необходимо выполнить следующие действия:

- 1) Навести курсор на базовый профиль отчета и нажать на кнопку «Создание профиля отчета» (**+**).
- 2) Откроется страница «Создание профиля отчета» (рис. 53). На странице заполнить необходимые поля и нажать кнопку «Создать». Состав и описание полей страницы приведены в таблице 18.

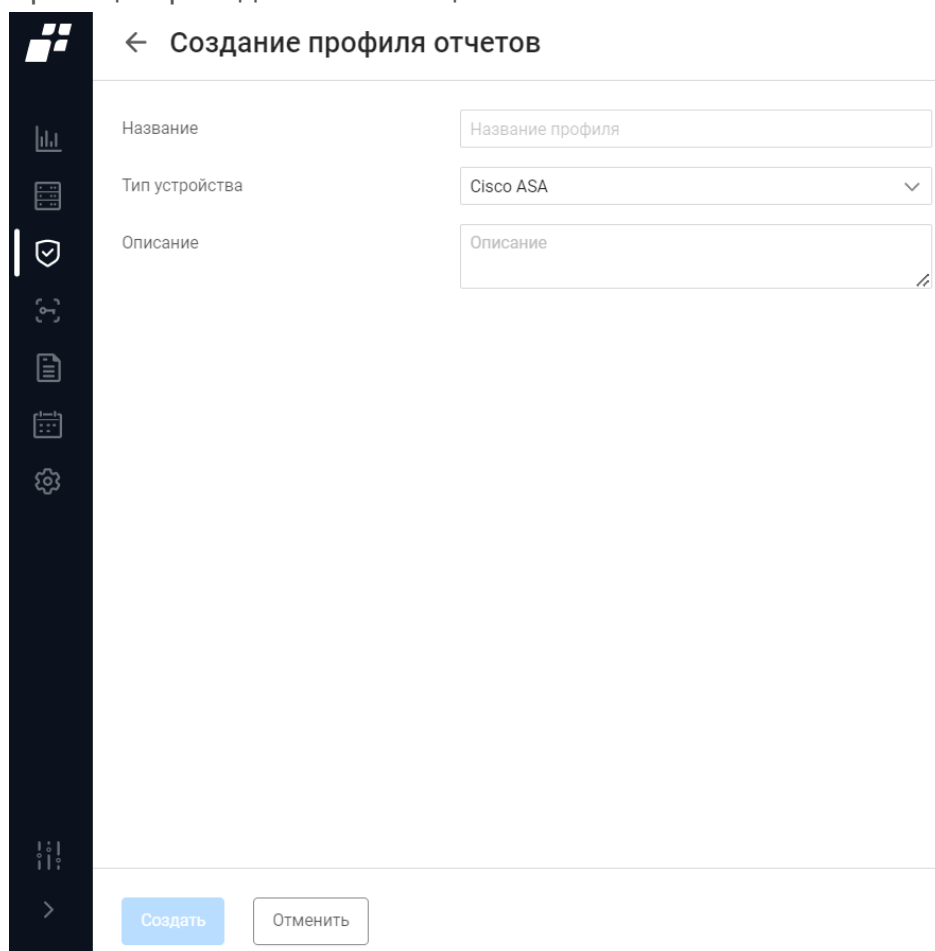



Рисунок 53 – Страница «Создание профиля отчетов»

Таблица 18 – Состав и описание полей страницы «Создание профиля отчетов»

Поле	Описание
Поле «Название»	Текстовое поле для ввода названия профиля отчета. 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 отчета. 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

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 п.п. 2.4.2.1). На вкладке «Проверки безопасности» автоматически отображаются проверки из подразделов «Проверки безопасности» и «Проверки МЭ».





 Дочерний профиль отчета автоматически появляется только при изменении настроек устройства («Контроль устройств» → «Устройства» → вкладка «Отчеты») и несовпадении с существующими пользовательскими профилями отчетов. В дереве профилей такой профиль будет отмечен значком «O».

2.4.2. Вкладка «Конфигурации»

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

На вкладке отображается следующая информация:

— иконка формы отчета:

- «» – текстовая форма отчета;
- «» – структурированная форма отчета;
- «» – пользовательский отчет;
- «» – отчет по правилам межсетевых экранов.

— название отчета;

— тип контроля (тип лицензии, отвечающий за данный отчет);

— тип использования отчета.

Над списком отчетов располагаются:

— поле поиска ( Введите запрос для поиска) для поиска искомой записи в списке;

- Для изменения использования отчета в профилях необходимо сделать следующее:

- Контроль устройств / Профили

Конфигурации - 11 Проверки безопасности - 22

Введите запрос для поиска

Использование Фильтр + Отчет

Название	Использование
Cisco ASA 'show access-list'	Только последний
Cisco ASA 'show route'	Только последний
Cisco ASA 'show running'	Архив версий
Cisco ASA 'show startup'	Контроль изменений Архив версий Только последний Запрещено
Cisco ASA 'show version'	
Cisco ASA Additional Compliance Text Report	Только последний
Cisco ASA Конфигурация	Архив версий
Интерфейсы (SNMP)	Архив версий
Маршруты	Архив версий
Маршруты (SNMP)	Только последний
Правила межсетевых экранов	Архив версий

Рисунок 54 – Настройка использования отчетов выбранного профиля

Таблица 19 – Состав и описание колонки «Использование»

Поле	Описание
Поле «Использование»	<p>Выбор режима использования отчета. Возможные значения:</p> <ul style="list-style-type: none"> — «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 только последняя измененная версия отчета, загруженного с устройства; — «Запрещено» – загрузка отчета с устройств запрещена вне зависимости от настроек базового профиля; — «Наследовать (только последний)» – применить настройки базового профиля. В скобках отображается значение,

Поле	Описание
	установленное для отчета в базовом профиле (отображается для пользовательских отчетов)

2.4.2.1. Создание пользовательского отчета

Для создания нового (пользовательского) отчета необходимо выполнить следующие шаги:

- 1) В дереве профилей отчетов выделить необходимый профиль отчета.
- 2) На вкладке «Конфигурации» в правом верхнем углу нажать кнопку «Отчет» (+ Отчет).
- 3) В открывшемся окне «Создание отчета» (рис. 55) заполнить необходимые параметры, в зависимости от вида добавляемого отчета, и нажать кнопку «Создать». Состав и описание Полей страницы «Создание отчета» приведены в таблице 20.

← Создание отчета

① Отчет будет доступен для всех устройств данного типа с включенным контролем "NETWORK ASSURANCE"

Название:

Тип отчета:

Команда ①:

Использование:

Тестирование

Выберите устройство на котором будет выполнена данная команда

Устройство:

Создать Отменить

← Создание отчета

① Отчет будет доступен для всех устройств данного типа с включенным контролем "INTEGRITY CHECK COMPLIANCE"

Название:

Тип отчета:

Шаблон:

Маска контролируемых файлов:

Маска исключения файлов:

Поиск во вложенных папках: ☒

Использование:

Тестирование

Выберите устройство на котором будет выполнена данная команда

Устройство:

Создать Отменить

Рисунок 55 – Страница «Создание отчета» для разного типа отчетов

Таблица 20 – Состав и описание 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 зависят от выбранного типа отчета

Поле	Описание
Поле «Использование»	Переключатель для включения/выключения режима использования отчета
Поле «Тестирование»	Позволяет выбрать устройство, на котором будет выполнена заданная команда
Элементы управления	
Создать	При нажатии на кнопку введенные данные сохраняются
Отменить	При нажатии на кнопку введенные данные не сохраняются

2.4.3. Вкладка «Проверки безопасности»

Вкладка «Проверки безопасности» содержит список проверок, которые связаны с профилем устройства, выбранным в дереве профилей (рис. 56).

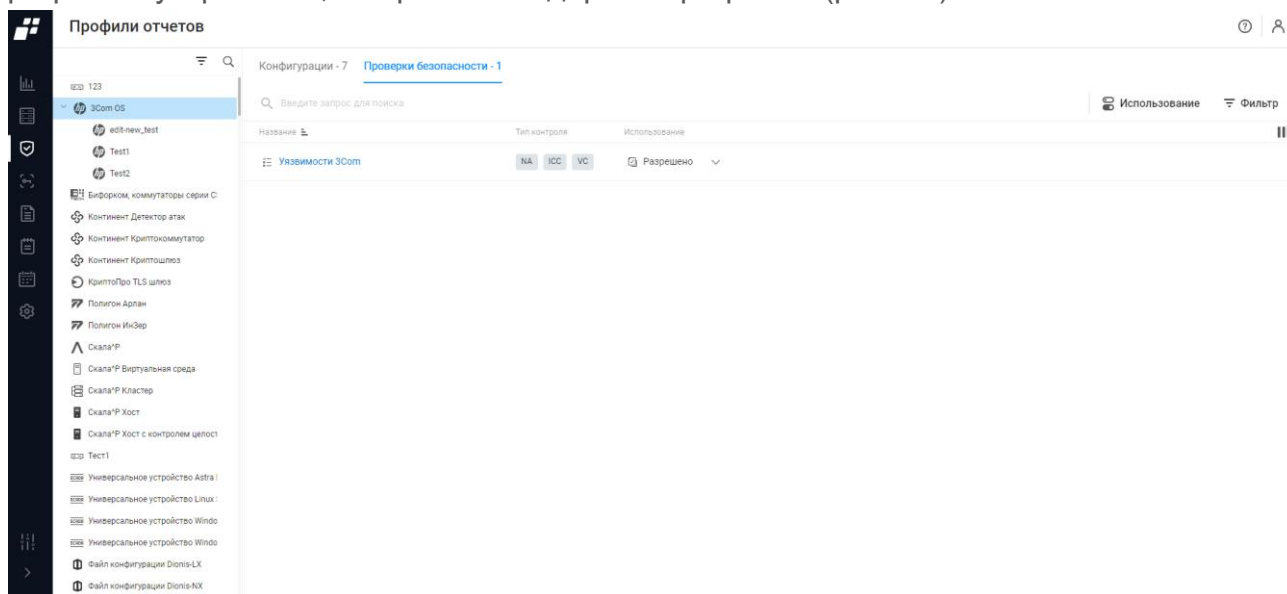





Рисунок 56 – Вкладка «Проверки безопасности»

Для каждой записи списка отображаются следующие данные:

- иконка проверки;
- название проверки;
- тип контроля (тип лицензии, отвечающий за данный отчет);
- тип использования проверки.

Над списком проверок располагаются:

- поле поиска ( Введите запрос для поиска) для поиска искомой записи в списке;
- кнопка «Использование» ( Использование) для перехода в окно просмотра и настройки использования профилей для устройств;
- кнопка «Фильтр» ( Фильтр) для настройки фильтрации по типу использования.

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

2.4.3.1. Настройка использования стандартов проверок безопасности

Для внесения изменений в настройки режима использования проверок безопасности для базовых профилей (профилей, автоматически добавленных в комплекс при подключении к нему внешних модулей) пользователю необходимо выполнить следующие действия:

- 1) В дереве профилей отчетов выделить необходимый профиль отчета и перейти на вкладку «Проверки безопасности».
- 2) В строке проверки в поле «Использование» выбрать необходимое значение (рис. 57):
 - «Разрешено» – разрешить проверку вне зависимости от настроек базового профиля;
 - «Запрещено» – запретить проверку вне зависимости от настроек базового профиля.

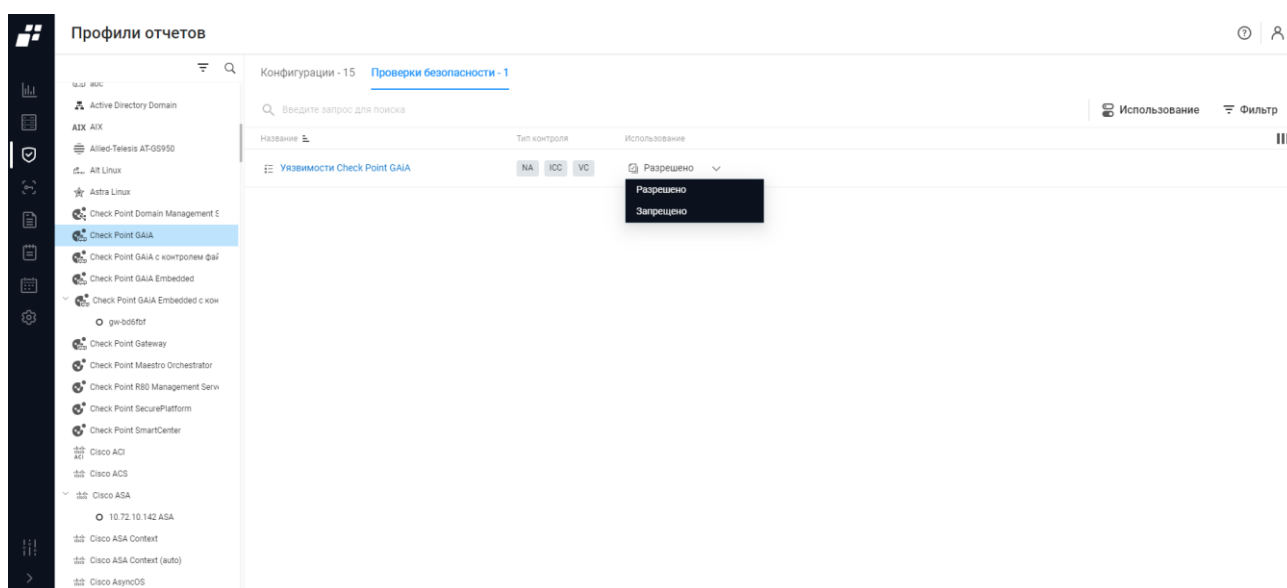


Рисунок 57 – Настройка проверок безопасности

Для настройки всех проверок одного профиля отчета пользователю необходимо выполнить следующие действия:

- 1) В дереве профилей выделить необходимый профиль устройства.
- 2) На вкладке «Проверки безопасности» нажать на название проверки.
- 3) Откроется окно настройки правил выбранной проверки (рис. 58), в которой необходимо заполнить поля и нажать кнопку «Сохранить». Состав и описание Полей окна приведены в таблице 21.

✕ Настройки правил "Проверка политик безопасности CIS для Cisco ASA"

Использование

Настройки отчета

Наследовать настройки всех правил ☒

Ensure 'Host Name' is set	✕ Наследовать Запрещено
Ensure 'Domain Name' is set	✕ Наследовать Запрещено
Ensure 'Enable Password' is set	✕ Наследовать Запрещено
Ensure 'Password Recovery' is disabled	✕ Наследовать Запрещено
Set the password lifetime in days to less than or equal to 180	✕ Наследовать Запрещено
Set the minimum number of characters that must be changed between the old and the new passwords, to be to be greater than or equal to 14	✕ Наследовать Запрещено
Set the minimum number of upper case characters in the password, to be to be greater than or equal to 1	✕ Наследовать Запрещено
Set the minimum number of lower case characters in the password, to be to be greater than or equal to 1	✕ Наследовать Запрещено
Set the minimum number of numeric characters in the password, to be to be greater than or equal to 1	✕ Наследовать Запрещено
Set the minimum number of special characters in the password, to be to be greater than or equal to 1	✕ Наследовать Запрещено

Рисунок 58 – Окно настройки всех правил

Таблица 21 – Состав и описание полей окна настройки проверок устройства

Поле	Описание
Поле «Использование»	Выбор режима использования проверки. Возможные значения: — «Разрешено» – разрешить проверку вне зависимости от настроек базового профиля; — «Запрещено» – запретить проверку вне зависимости от настроек базового профиля
Группа полей «Настройки отчетов»	
Поле «Наследовать настройки всех правил»	Содержит переключатель с двумя положениями: — Включен () – редактирование настроек проверки запрещено; — Выключен () – пользователь имеет возможность внесения изменений в настройки отдельных правил проверки
Поле «Правила»	Поле с перечнем правил проверки
Элементы управления	
Сохранить	При нажатии кнопки выполняется сохранение внесенных изменений

Поле	Описание
Отменить	При нажатии кнопки выполняется переход на страницу без сохранения внесенных данных

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. 59) позволяет пользователю задать триггеры (условия) для реакции комплекса на события, которые произошли на устройствах или в самом комплексе.

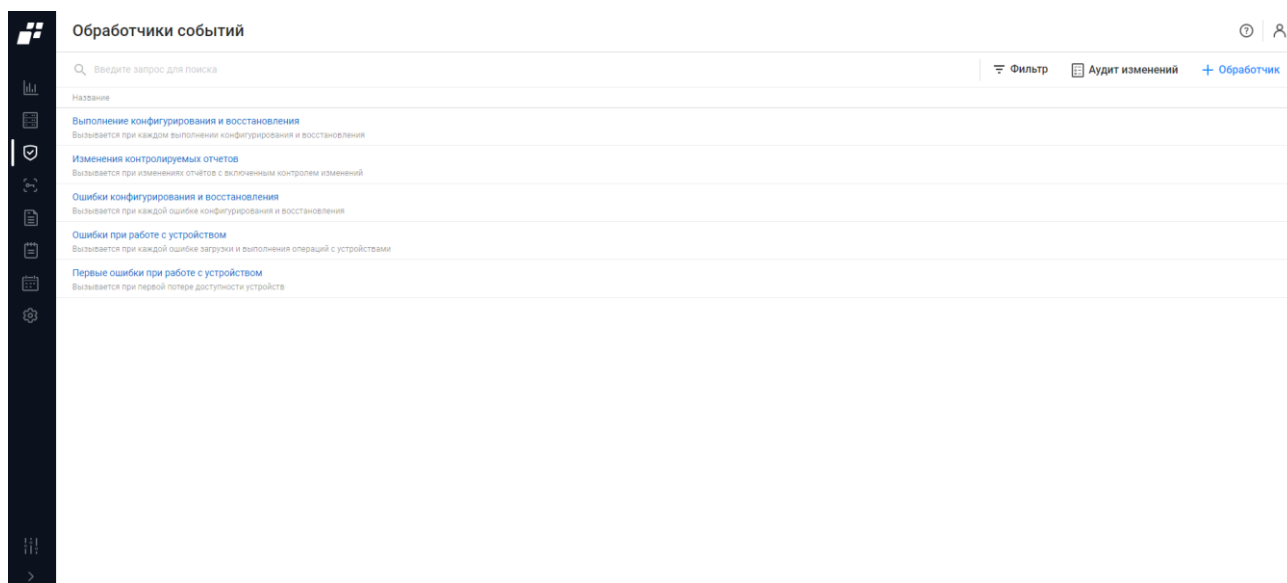


Рисунок 59 – Подраздел «Обработчики событий»

Для каждой записи списка отображаются название и описание обработчика событий. Над списком располагаются:

- поле поиска (🔍 Введите запрос для поиска) для поиска искомой записи в списке;
- кнопка «Фильтр» (🗒 Фильтр) для фильтрации списка событий;
- кнопка «Аудит изменений» (📋 Аудит изменений) для перехода в окно включения/выключения загрузки отчетов при получении событий об изменении конфигурации устройства;
- кнопка «Обработчик» (➕ Обработчик) для перехода на страницу создания нового обработчика событий.

По умолчанию в списке обработчиков событий отображаются как активные, так и отключенные обработчики. Наименования неактивных обработчиков событий отображаются затененными.

Удаление встроенных обработчиков невозможно, но пользователь может редактировать и отключать их.

2.5.1. Создание пользовательского обработчика событий

Для добавления пользовательского обработчика событий в комплекс необходимо выполнить следующие действия:

- 1) На странице нажать кнопку «Обработчик» ([+ Обработчик](#)).
- 2) В открывшемся окне «Создание обработчика» (рис. 60) заполнить необходимые параметры. Состав и описание Полей страницы приведены в таблице 22.

Рисунок 60 – Страница «Создание обработчика»

Таблица 22 – Состав и описание страницы «Создание обработчика»

Поле	Описание
Поле «Статус»	При установленном переключателе осуществляется обработка событий, при снятом – триггер выключен
Поле «Название»	Название обработчика
Поле «Описание»	Текстовое поле для ввода описания обработчика. Параметры ввода текста: от 1 до 4000 любых символов
Поле «Условия»	Выбор условий через кнопку «Условие» (+ Условие) для выполнения правил обработки событий
Поле «Действия»	Выбор типа выполняемого действия через кнопку «Действие» (+ Действие)
Элементы управления	
Создать	При нажатии на кнопку введенные данные сохраняются
Отменить	При нажатии на кнопку введенные данные не сохраняются

- 3) В поле «Условия» нажать кнопку «Условие» ([+ Условие](#)). Из раскрывающегося

списка выбрать тип события, при совершении которого ожидается реакция системы (рис. 61).

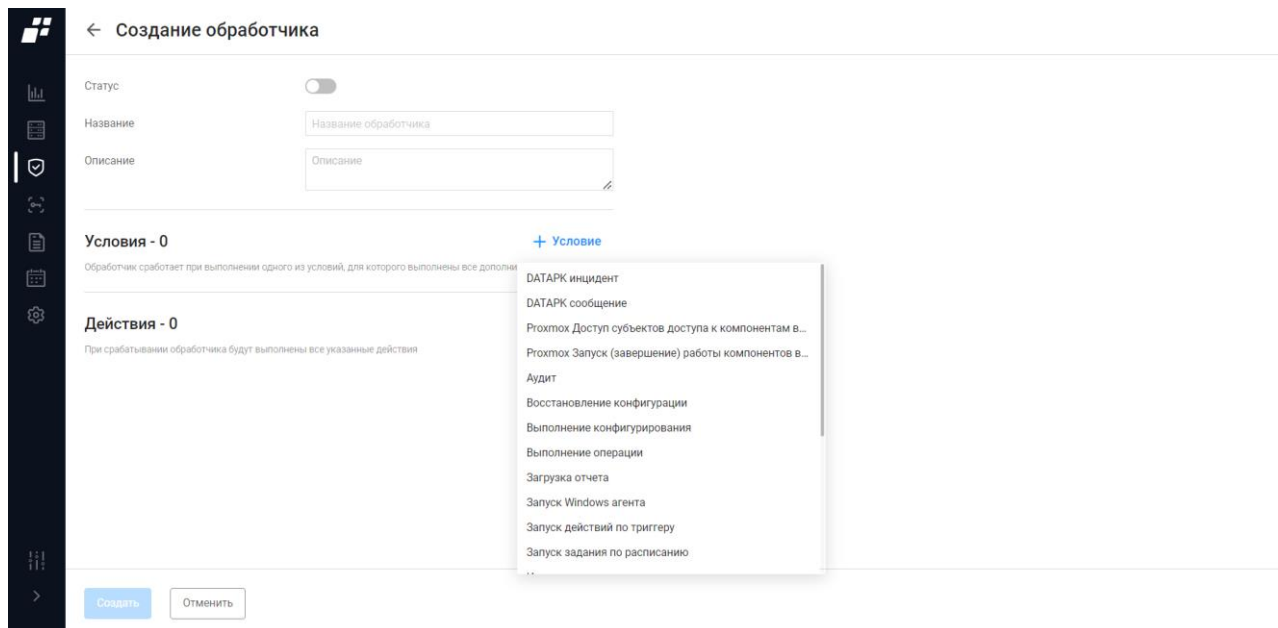


Рисунок 61 – Окно создания условий для обработчика событий

- 4) При необходимости выбрать «Дополнительные условия» в поле «Условия». Из раскрывающегося списка значений выбрать параметр события, для которого задается условие. В зависимости от вида выбранного параметра в окне отобразится ряд вариантов значений (рис. 62).

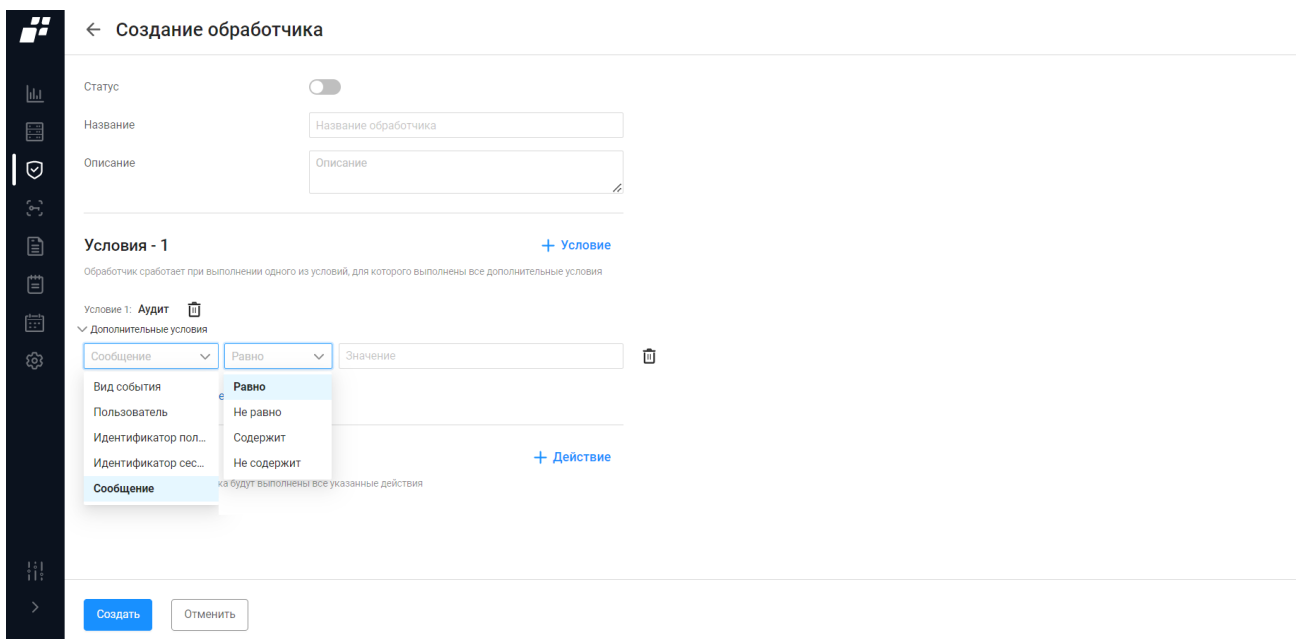


Рисунок 62 – Выбор дополнительных условий

- 5) В поле «Действия» нажать кнопку «Действие» (+ Действие). Из

раскрывающегося списка выбрать тип события, при совершении которого ожидается реакция системы. Затем для каждого события выбрать тип действия, которое будет выполнено в комплексе в ответ на произошедшее событие (рис. 63).

← Создание обработчика

Статус ☐

Название

Описание

Условия - 1 [+ Условие](#)

Обработчик сработает при выполнении одного из условий, для которого выполнены все дополнительные условия

Условие 1: Аудит

✓ Дополнительные условия

Сообщение Равно 1

[+ дополнительное условие](#)

Действия - 0 [+ Действие](#)

При срабатывании обработчика будут выполнены все указанные действия

Выполнить операцию "Проверить соединение"
Загрузить отчёты
Создать уведомление

[Создать](#) [Отменить](#)

Рисунок 63 – Окно создания действий для обработчика событий

← Создание обработчика

Статус ☐

Название

Описание

Условия - 1 [+ Условие](#)

Обработчик сработает при выполнении одного из условий, для которого выполнены все дополнительные условия

Условие 1: Аудит

✓ Дополнительные условия

Сообщение Равно 1

[+ дополнительное условие](#)

Действия - 1 [+ Действие](#)

При срабатывании обработчика будут выполнены все указанные действия

Действие 1: Выполнить операцию "Проверить соединение"

☐ Выполнять на источнике события

☒ Выполнять на устройствах:

[Создать](#) [Отменить](#)

Рисунок 64 – Дополнительные параметры для действий


- 6) Проставить флаг в требуемой строке и выбрать устройство при необходимости (рис. 64).
- 7) Нажать кнопку «Создать».

2.5.2. Редактирование обработчика

Для изменения пользовательского обработчика событий необходимо выполнить следующие действия:

- 1) Выбрать обработчик событий, который требуется отредактировать. Нажать на имя обработчика. Откроется окно редактирования обработчика.
- 2) Для включения или выключения обработчика установить/снять переключатель «Статус».
- 3) Добавить новые или удалить неактуальные типы событий в области «Условия».

Для удаления условия нажать кнопку «Удалить» ().

- 4) Добавить новые или удалить неактуальные действия в области «Действия». Для удаления действия нажать кнопку «Удалить» ().
- 5) Нажать кнопку «Сохранить». Произойдет возврат в форму настройки обработки событий, внесенные изменения будут сохранены.

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. 65) позволяет настроить параметры аутентификации пользователей на оборудовании.

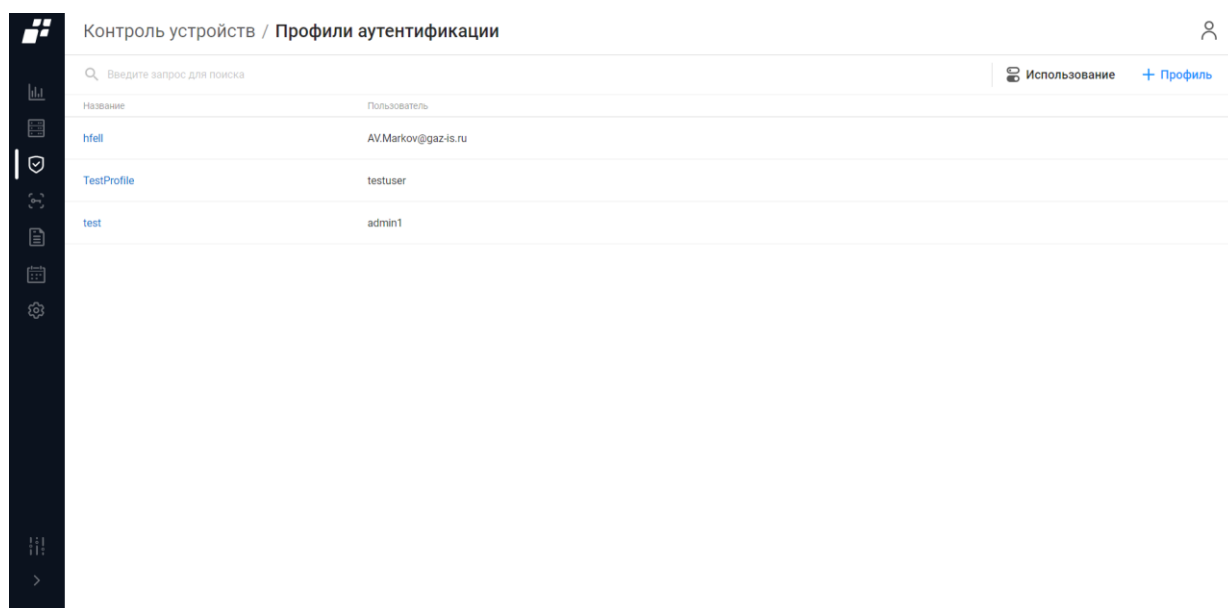






Рисунок 65 – Подраздел «Профили аутентификации»

Для каждой записи списка отображаются следующие данные:

- название профиля аутентификации;
- пользователь — логин, под которым происходит подключение пользователя к устройству для внесения изменений в настройки устройства.

Над списком профилей располагаются:

- поле поиска ( Введите запрос для поиска) для поиска искомой записи в списке;
- кнопка «Использование» ( Использование) для перехода в окно просмотра и настройки использования профиля аутентификации;
- кнопка «Профиль» ( Профиль) для перехода на страницу создания нового профиля аутентификации.

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

2.6.1.1. Создание профиля аутентификации

Для создания нового профиля аутентификации необходимо выполнить следующие действия:

- 1) Нажать на кнопку «Профиль» (**+ Профиль**).
- 2) На открывшейся странице «Создание профиля аутентификации» (рис. 66) заполнить поля и нажать кнопку «Создать». Состав и описание полей страницы приведены в таблице 23.

← Создание профиля аутентификации

Название	<input type="text" value="Название профиля"/>
Пользователь	<input type="text" value="Логин пользователя"/>
Пароль	<input type="password" value="Пароль"/>
Дополнительный пароль	<input type="password" value="Пароль"/>

Рисунок 66 – Страница «Создание профиля аутентификации»

Таблица 23 – 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
Поле «Пароль»	Указать пароль, под которым будет происходить авторизация на контролируемых комплексом устройствах
Поле «Дополнительный	Ввести дополнительный пароль для привилегированного режима

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


2.6.1.2. Редактирование профиля аутентификации

Для изменения параметров профиля необходимо выполнить следующие действия:

- 1) В подразделе «Профили аутентификации» выбрать профиль, который необходимо откорректировать.
- 2) Откроется окно редактирования выбранного профиля аутентификации.
- 3) Внести необходимые изменения.
- 4) Нажать кнопку «Сохранить».

2.6.1.3. Настройки использования профиля аутентификации

Для настройки использования профиля аутентификации необходимо выполнить следующие действия:

- 1) Нажать на странице со списком профилей кнопку «Использование» ( Использование).
- 2) В открывшемся окне «Использование "Профили аутентификации"» (рис. 67) выбрать необходимые ОЗ и указать профиль аутентификации. Состав и описание полей окна приведено в таблице 24.
- 4) Нажать кнопку «Сохранить».

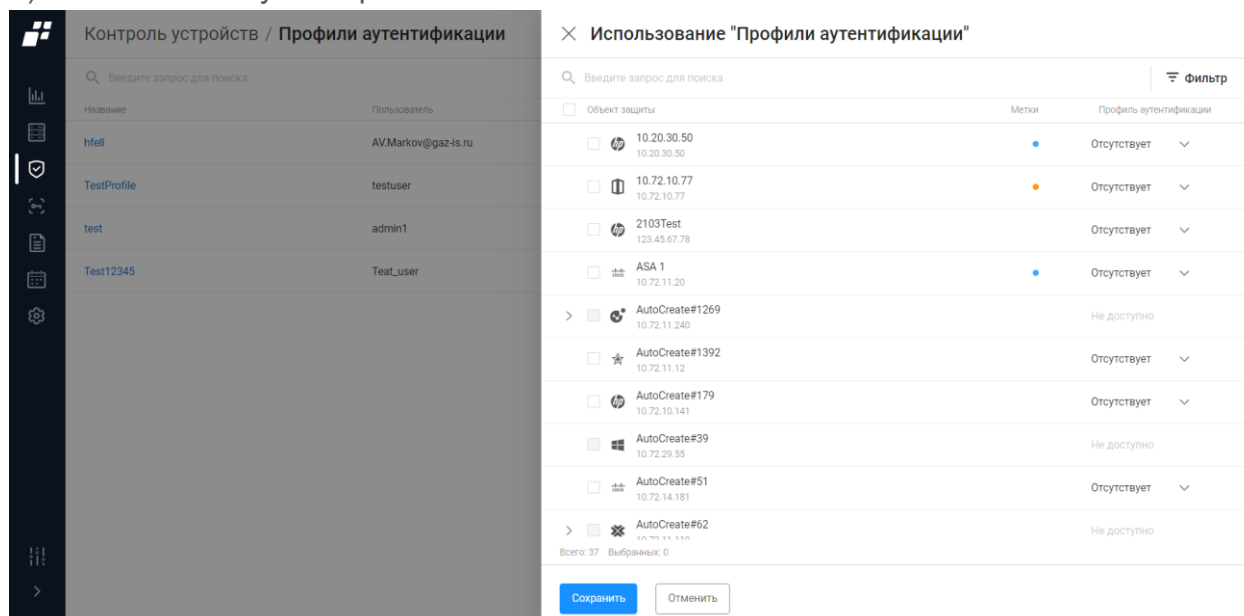


Рисунок 67 – Окно «Использование "Профили аутентификации"»

Таблица 24 – Состав и описание Полей окна «Использование "Профили аутентификации"»

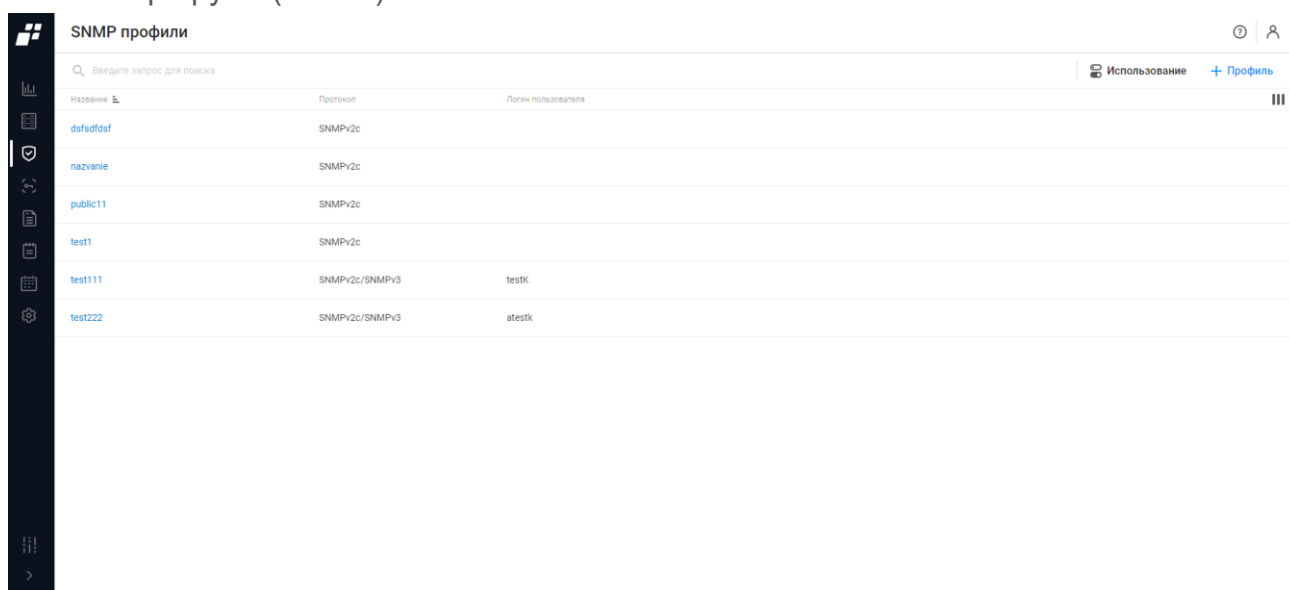
Поле	Описание
Поле для флага	Для выбора ОЗ
Поле «Объект защиты»	Список доступных ОЗ в комплексе. Для выбора ОЗ необходимо поставить флаг в поле для флагов
Поле «Метки»	Особые метки пользователей комплекса
Поле «Профиль аутентификации»	Раскрывающийся список существующих профилей аутентификации. Изначально профиль 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

2.7 SNMP профили

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

Подраздел «SNMP профили» (рис. 68) позволяет получить информацию по интерфейсам и маршрутам по протоколу SNMP от устройств и сформировать два типа отчета:

- «Интерфейсы (SNMP)»;
- «Маршруты (SNMP)».



Название	Протокол	Логин пользователя
dsfsdfsdf	SNMPv2c	
nazvanie	SNMPv2c	
public11	SNMPv2c	
test1	SNMPv2c	
test111	SNMPv2c/SNMPv3	testK
test222	SNMPv2c/SNMPv3	atestk

Рисунок 68 – Подраздел «SNMP профили»

Для каждой записи списка отображаются следующие данные:

- название SNMP профиля;
- протокол;
- логин пользователя.

Над списком SNMP профилей располагаются:

- поле поиска ( Введите запрос для поиска) для поиска искомой записи в списке;
- кнопка «Использование» ( Использование) для перехода в окно просмотра и настройки использования SNMP профиля;
- кнопка «Профиль» ( Профиль) для перехода на страницу создания нового SNMP профиля;
- кнопка «Колонки» () позволяет определить отображение необходимых столбцов на странице. При нажатии кнопки раскрывается окно со списком столбцов на странице (см. рис. 68). При необходимости с помощью флага можно


менять количество отображаемых столбцов на странице. Первый столбец всегда отображается на странице.

При наведении курсора на профиль аутентификации, появляется кнопка «Удалить»

() для удаления SNMP профиля.

2.7.1.1. Создание SNMP профиля

Для создания нового SNMP-профиля необходимо выполнить следующие действия:

- 1) Нажать кнопку «Профиль» ( Профиль).
- 2) В открывшемся окне «Создание SNMP профиля» заполнить все поля (рис. 69) и нажать кнопку «Создать». Состав и описание полей страницы приведены в таблице 25.

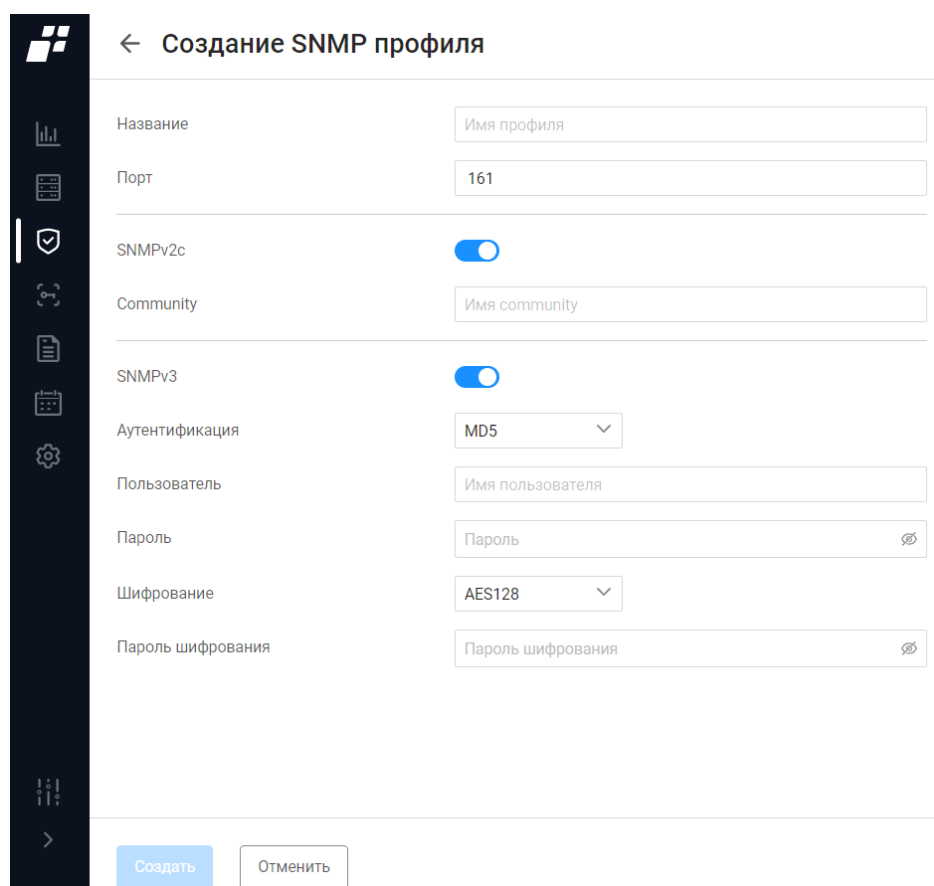






Рисунок 69 – Страница «Создание SNMP профиля»

Таблица 25 – Состав и описание полей страницы «Создание SNMP профиля»

Поле	Описание
Поле «Название»	Текстовое поле для ввода названия SNMP профиля. Параметры ввода текста: от 1 до 250 любых символов
Поле «Порт»	Порт на устройстве, на который будут отправляться SNMP-запросы

Поле	Описание
Поле «SNMPv2c»	Версия v2c протокола SNMP для подключения к контролируемому устройству. Переключатель: — «Включено» (); — «Отключено» ()
Поле «Community»	Идентификатор, используемый для аутентификации на контролируемом устройстве при использовании протокола SNMPv2c. Рекомендуемое значение «public». Поле обязательно к заполнению при использовании SNMPv2c. Поле становится активным при включенном переключателе SNMPv2c
Поле «SNMPv3»	Версия 3 протокола SNMP для подключения к контролируемому устройству. Переключатель: — «Включено» (); — «Отключено» ()
Поле «Аутентификация»	Выбор алгоритма хеширования при аутентификации контролируемого устройства при использовании протокола SNMPv.3. Доступны следующие варианты: — «MD5 (Message Digest 5)»; — «SHA (Secure Hash Algorithm)»; — «None». Поле становится активным при включенном переключателе SNMPv3
Поле «Пользователь»	Имя (логин) учетной записи пользователя, которая будет использоваться для авторизации на контролируемом устройстве по протоколу SNMPv.3. Поле обязательно к заполнению при использовании SNMPv.3. Поле становится активным при включенном переключателе SNMPv3
Поле «Пароль»	Пароль учетной записи пользователя, которая будет использоваться для авторизации на контролируемом устройстве по протоколу SNMPv.3. Поле обязательно к заполнению при использовании SNMPv.3. Поле становится активным при включенном переключателе SNMPv3
Поле «Шифрование»	Выбор алгоритма для подключения к контролируемому устройству при использовании протокола SNMPv.3. Возможные варианты для выбора:

Поле	Описание
	— «AES128 (Advanced Encryption Standard)»; — «DES (Data Encryption Standard)». — для отказа от шифрования выбрать значение «None». Поле становится активным при включенном переключателе SNMPv3
Поле «Пароль шифрования»	Пароль для управления контролируемым устройством при использовании протокола SNMPv.3. Поле обязательно к заполнению при использовании SNMPv.3. Поле становится активным при включенном переключателе SNMPv3
Элементы управления	
Создать	При нажатии на кнопку введенные данные сохраняются
Отменить	При нажатии на кнопку введенные данные не сохраняются


2.7.1.2. Редактирование SNMP профиля

Для изменения параметров SNMP профиля пользователю необходимо выполнить следующие действия:

- 1) Выбрать профиль, который необходимо откорректировать.
- 2) Нажать на имя профиля.
- 3) В открывшейся страницы редактирования выполнить необходимые изменения.
- 3) Нажать кнопку «Сохранить».

2.7.1.3. Настройки использования SNMP профиля

Для настройки использования SNMP профиля необходимо выполнить следующие действия:

- 1) Нажать на странице со списком профилей кнопку «Использование» ( Использование).
- 2) В открывшемся окне «Использование "SNMP профили"» (рис. 70) выбрать необходимые ОЗ и указать необходимый SNMP профиль, затем нажать кнопку «Сохранить». Состав и описание полей окна «Использование "SNMP профили"» приведены в таблице 26.

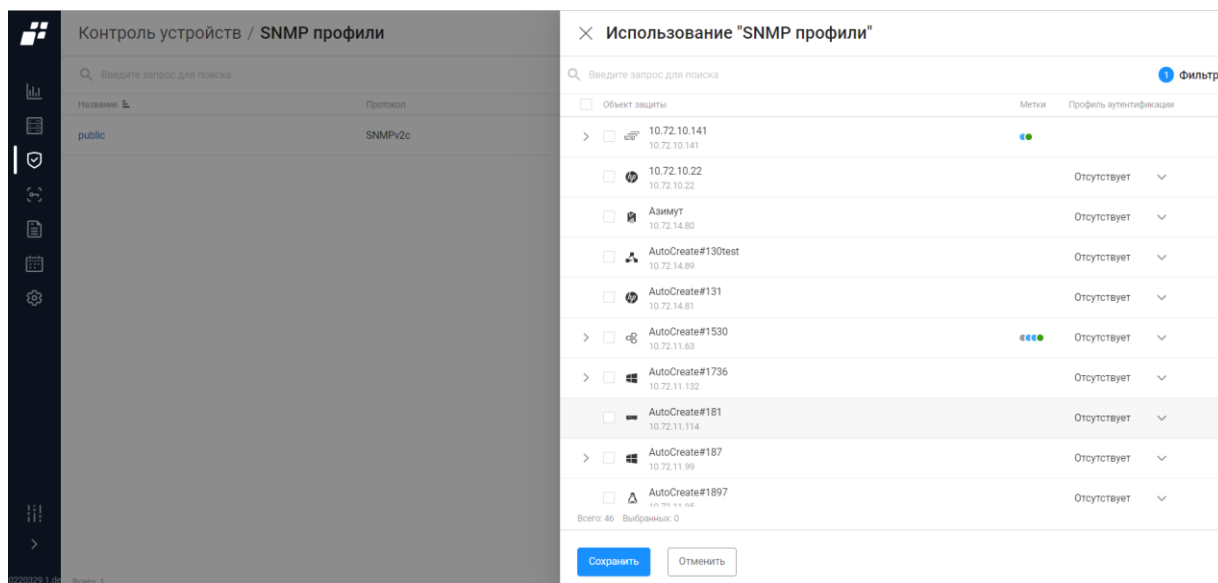


Рисунок 70 – Окно «Использование "SNMP профили"»

Таблица 26 – Состав и описание Полей окна «Использование "SNMP профили"»

Поле	Описание
Поле для флага	Для выбора ОЗ
Поле «Объект защиты»	Список доступных ОЗ в комплексе. Для выбора ОЗ необходимо поставить флаг в поле для флагов
Поле «Метки»	Особые метки пользователей комплекса
Поле «SNMP профиль»	Раскрывающееся окно с существующими SNMP профилями. Изначально профиль отсутствует
Элементы управления	
Поле поиска	Для ввода последовательности символов из искомой записи
Кнопка «Фильтр»	Позволяет отфильтровать ОЗ по выбранным параметрам
Сохранить	При нажатии на кнопку введенные данные сохраняются
Отменить	При нажатии на кнопку введенные данные не сохраняются

2.8 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. 71) позволяет пользователю включать (отключать) функции проверки доступности устройств с указанием интервала в минутах. 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 27.

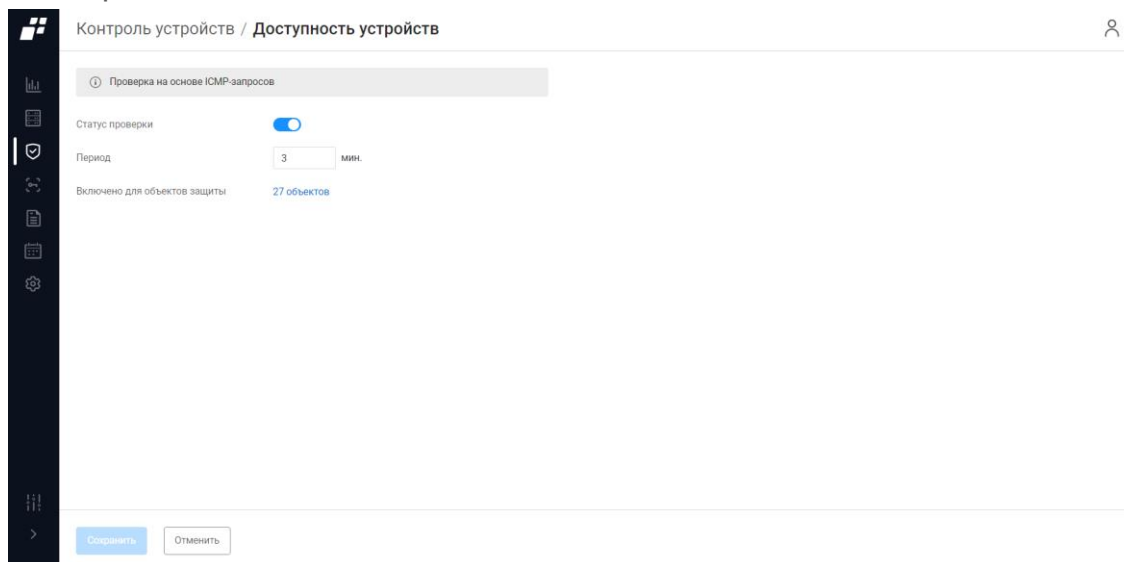




Рисунок 71 – Подраздел «Доступность устройств»

Таблица 27 – Состав и описание Полей страницы подраздела «Доступность устройств»

Поле	Описание
Поле «Статус проверки»	Содержит переключатель с двумя положениями: — «Включен» () – функция проверки доступности устройства включена; — «Выключен» () – функция проверки доступности устройства выключена
Поле «Период»	Циклический временной промежуток проверки доступности устройств
Поле «Включено для объектов защиты»	Ссылка, показывающая количество ОЗ, на которых назначена данная проверка. При нажатии на ссылку раскрывается список устройств

2.8.1.1. Настройка проверки доступности устройств

Для настройки проверки доступности устройств необходимо выполнить следующие действия:

- 1) Нажать на странице ссылку в поле «Включено для объектов защиты».
- 2) В открывшемся окне «Проверка доступности на устройствах» (рис. 72) выбрать необходимые ОЗ и указать необходимость проверки, выбрав одно из положений переключателя, затем нажать кнопку «Сохранить». Состав и описание полей окна «Проверка доступности на устройствах» приведены в таблице 28.

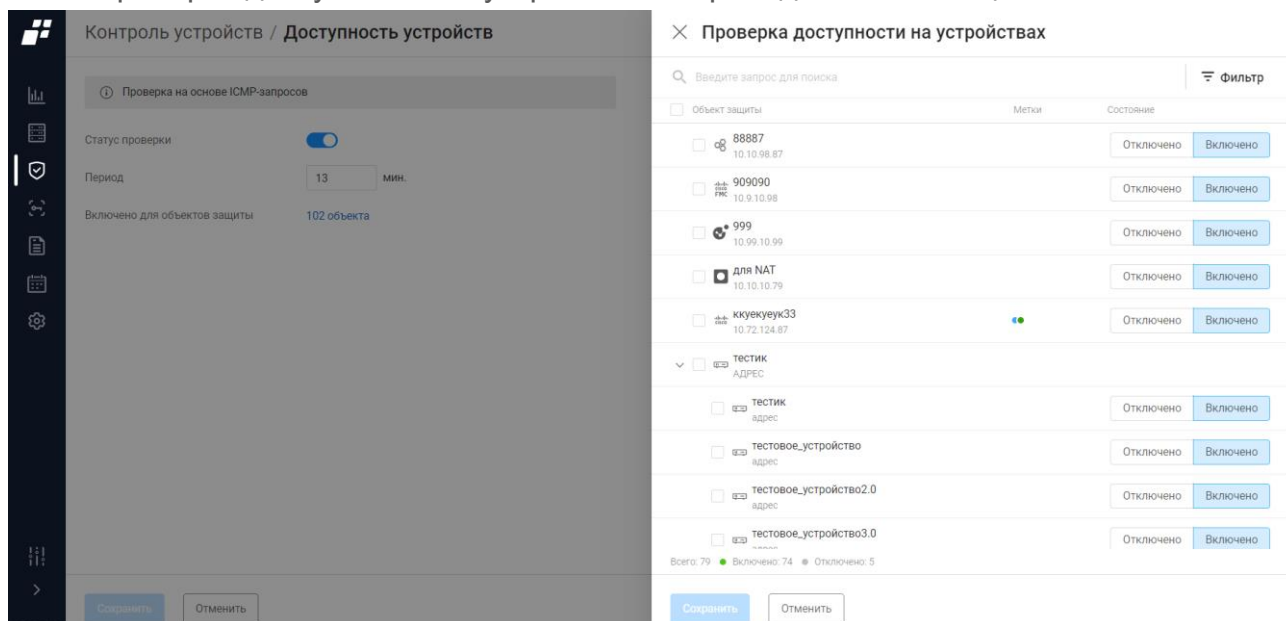


Рисунок 72 – Окно «Проверка доступности на устройствах»

Таблица 28 – Состав и описание Полей окна «Проверка доступности на устройствах»

Поле	Описание
Поле для флага	Для выбора ОЗ
Поле «Объекты защиты»	Список доступных ОЗ в комплексе. Для выбора ОЗ необходимо поставить флаг в поле для флагов
Поле «Метки»	Особые метки пользователей комплекса
Поле «Состояние»	Переключатель: — «Отключен» — проверка доступности на устройстве отключена; — «Включен» — проверка доступности на устройстве включена
Элементы управления	
Поле поиска	Для ввода последовательности символов из искомой записи
Кнопка «Фильтр»	Для фильтрации списка ОЗ
Сохранить	При нажатии на кнопку введенные данные сохраняются
Отменить	При нажатии на кнопку введенные данные не сохраняются

Перечень сокращений

AES	–	Advanced Encryption Standard
DES	–	Data Encryption Standard
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
SHA	–	Secure Hash Algorithm
SNMP	–	Simple Network Management Protocol
SSH	–	Secure SHell
TELNET	–	TELEcommunication NETwork
TSP	–	Time Stamp Protocol
UDP	–	User Datagram Protocol
VC	–	Vulnerability Control
БД	–	База данных
МЭ	–	Межсетевой экран
ОЗ	–	Объект защиты
ОС	–	Операционная система
ПК	–	Программный комплекс
ПО	–	Программное обеспечение