ГАЗИНФОРМ СЕРВИС

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

Часть 1

Администрирование

Санкт–Петербург, 2023

Аннотация

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

Руководство содержит сведения, необходимые для настройки доступа пользователей ПК «Efros DO» к сетевым ресурсам и функциям, а также контроля работы с использованием веб-интерфейса.

Руководство состоит из следующих частей:

- часть 1 содержит описание работы общих разделов по администрированию комплекса;
- часть 2 предназначена для настройки и конфигурирования функций контроля устройств;
- часть 3 предназначена для настройки и конфигурирования функций контроля доступа.

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

Знаки, расположенные на полях руководства, указывают на примечания.

Степени важности примечаний:

Важная информация
Указания, требующие особого внимания.

Дополнительная информация
Информация, позволяющая упростить работу с комплексом.

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

Содержание

1 Назначение и основные функции ПК «Efros DO» 5
1.1 Назначение 5
1.2 Функциональные возможности программы 10
1.3 Роли пользователей 17
2 Условия выполнения ПК «Efros DO» 18
3 Работа с ПК «Efros DO» 20
3.1 Запуск веб–приложения ПК «Efros DO» 20
4 Раздел «Мониторинг» 24
4.1 Добавление новой вкладки и виджета 25
4.2 Редактирование виджета 30
5 Раздел «Объекты сети» 31
5.1 Объекты защиты 31
5.2 База знаний 50
5.3 Конечные точки 53
5.4 Карта сети 61
5.5 Векторы атак 75
5.6 Сканирование 85
6 Раздел «Отчеты» 90
6.1 Создание шаблона отчета 92
6.2 Редактирование шаблона отчета 95
7 Раздел «Центр задач» 96
7.1 Вкладка «Заявки» 96
7.2 Вкладка «Типы заявок» 102
7.3 Вкладка «Маршруты» 106
7.4 Вкладка «Группы пользователей» 110
7.5 Вкладка «Настройки» 113
8 Раздел «События» 114
8.1 Центр задач 114
8.2 Объекты защиты 115
8.3 Аудит 117

8.4 Доступ в сеть 118
8.5 Доступ на оборудование 119
8.6 Системные события 120
8.7 Фильтрация событий 123
8.8 Экспорт журналов в формате CSV и XLSX 123
9 Раздел «Администрирование» 125
9.1 Пользователи 125
9.2 Лицензия 140
9.3 Сертификаты 142
9.4 Планировщик 156
10 Раздел «Настройки» 167
10.1 TACACS+ и RADIUS 167
10.2 Доступ в сеть 170
10.3 Источники данных 179
10.4 Модули 190
10.5 База уязвимостей 197
10.6 Хранение данных 199
10.7 Почтовые серверы 202
10.8 Импорт данных 204
10.9 База знаний 208
11 Сообщения об ошибках пользователю 210
11.1 Ошибки при идентификации 210
11.2 Ошибки при создании/редактировании сущности 211
11.3 Ошибки, связанные с лицензией на ПК «Efros DO» 212
12 Завершение работы ПК «Efros DO» 213
13 Перечень сокращений 214
14 Приложение А 217

1 Назначение и основные функции ПК «Efros DO»

1.1 Назначение

Главной целью ПК «Efros DO» является решение следующих задач в области информационной безопасности:

- контроль конфигураций и топологии сети;
- оптимизация и настройка межсетевых экранов (далее — МЭ);
- контроль целостности и проверки соответствия хостов и конечных точек;
- анализ уязвимостей и построение векторов атак;
- сбор и отображение статистики по потокам данных в сети;
- централизованная сетевая идентификация администраторов и управление доступом на сетевых устройствах, у которых на клиентском уровне поддерживаются протоколы TACACS+ и (или) RADIUS;
- автоматизация управления МЭ.

Расшифровка названий и краткое описание видов лицензий приведены в таблице 1.

Таблица 1 – Расшифровка названия лицензии и краткое описание

Лицензия		Описание
NETWORK ASSURANCE	NA	Модуль контроля конфигураций и топологии сети
FIREWALL ASSURANCE	FA	Модуль оптимизации и настройки межсетевых экранов
CHANGE MANAGER	CM	Модуль анализа и управления объектами защиты в разделе "Центр задач"
VULNERABILITY CONTROL	VC	Модуль анализа уязвимостей и построения векторов атак
NETWORK FLOW ANALYSIS	NFA	Модуль сбора статистики по потокам данных в сети
INTEGRITY CHECK COMPLIANCE	ICC	Модуль контроля целостности и проверки соответствия хостов и конечных точек
NETWORK ACCESS CONTROL	NAC	Модуль разграничения и контроля доступа в сеть

Каждая лицензия обладает определенными количественными характеристиками. Количественные характеристики – это количество доступных лицензий на оборудование и условия их выдачи:

- модули «Efros NA», «Efros FA», «Efros ICC» и «Efros VC»: доступно 100 лицензий на оборудование для каждого модуля. Условие выдачи лицензии: если объекту защиты (далее – ОЗ) назначается возможность «Контроль устройств», то для ОЗ выделяется одна лицензия. Количественный показатель лицензии уменьшается;
- модуль «Efros NAC»: доступно 100 лицензий. Условие выдачи лицензии: если ОЗ назначается возможность «Контроль доступа», то для ОЗ выделяется одна лицензия:
  - для сетевого оборудования и конечных точек– количество выдаваемых лицензий зависит от количества активных сессий (IP-адрес – одна лицензия, диапазон адресов – лицензия выдается на количество адресов в диапазоне). Сессия заканчивается или прерывается – лицензия отзывается.
- модуль «Efros NFA»: доступно 100 лицензий. Условия выдачи лицензии: по источникам. Количество триггеров не ограничивается.

Подсчет лицензий для конечных точек ведется по сессиям, чья длительность не превышает значение параметра «Длительность активной сессии».

Доступность функциональных возможностей ПК «Efros DO», в зависимости от приобретенной лицензии, приведена в таблице 2.

Таблица 2 – Функциональные возможности в зависимости от лицензии

Раздел веб–интерфейса	**Вкладка меню**	**Efros DO***	**Лицензии на функциональные модули**						
			Efros NA	**Efros FA**	**Efros ICC**	**Efros VC**	**Efros NFA**	**Efros NAC**	**Efros CM**
Мониторинг		+							
Объекты сети		+							
	Объекты защиты (дерево устройств)	+							
	Объекты защиты (возможность «Контроль устройств»)		+	+	+	+			
	Объекты защиты (возможность «Контроль							+	

Раздел веб–интерфейса	Вкладка меню	Efros DO*	Лицензии на функциональные модули						
			Efros NA	Efros FA	Efros ICC	Efros VC	Efros NFA	Efros NAC	Efros CM
	доступа»)								
	Объекты защиты (возможность «Потоки»)						+		
	База знаний	+	+		+		+	+	
	Конечные точки							+	
	Карта сети	+							
	Векторы атак					+			
	Сканирование	+							
Контроль устройств			+	+	+	+			
	Устройства		+	+	+	+			
	Проверки безопасности		+	+	+	+			
	Проверки МЭ			+					
	Профили отчетов		+	+	+	+			
	Обработчики событий		+	+	+	+			
	Профили аутентификации		+	+	+	+			
	SNMP профили		+	+	+	+			
	Доступность устройств		+	+	+	+			
Контроль доступа								+	
	Сетевое оборудование							+	
	Сетевые пользователи							+	
	Наборы политик							+	
	Профили оборудования							+	
	Профили авторизации							+	
	Загружаемые ACL							+	
	Наборы команд							+	

Раздел веб–интерфейса	Вкладка меню	Efros DO*	Лицензии на функциональные модули						
			Efros NA	Efros FA	Efros ICC	Efros VC	Efros NFA	Efros NAC	Efros CM
	Разрешенные протоколы							+	
	Разрешенные MAC-адреса							+	
	Словари							+	
	Гостевые порталы							+	
Отчеты		+							
	Общие	+							
	Личные	+							
Центр задач		+							
События		+							
	Центр задач	+							
	Объекты защиты		+	+	+	+	+	+	
	Аудит		+	+	+	+	+	+	+
	Доступ в сеть								
	Доступ на оборудование							+	
	Системные события		+	+	+	+		+	
Администрирова-ние	Пользователи	+							
	Лицензии	+							
	Сертификаты							+	
	Планировщик	+							
Настройки		+							
	TACACS+ и RADIUS							+	
	Доступ в сеть							+	
	Источники данных							+	
	Модули		+	+	+	+			
	Модули (Сетевые)		+	+	+	+			
	Модули (Виртуализация)		+	+	+	+			
	Модули (Сервисные)		+	+	+	+			

Раздел веб–интерфейса	Вкладка меню	Efros DO*	Лицензии на функциональные модули						
			Efros NA	Efros FA	Efros ICC	Efros VC	Efros NFA	Efros NAC	Efros CM
	Модули (Приложения)		+	+	+	+			
	Модули (Пользовательские)		+	+	+	+			
	База уязвимостей					+			
	Хранение данных	+							
	Хранение данных (Контроль устройств)		+	+	+	+			
	Хранение данных (Контроль доступа)							+	
	Хранение данных (Потоки)						+		
	Хранение данных (Общее)	+							
	Почтовые сервера	+							
	Импорт данных							+	
	База знаний	+							

* отмеченные знаком «+» разделы и функциональные возможности всегда доступны, независимо от наличия лицензии на тот или иной функциональный модуль

1.2 Функциональные возможности программы

ПК «Efros DO» реализует следующие функциональные возможности:

- единая точка доступа к функциям системы и модулям интеграции;
- получение, обработка, интеграция и хранение данных, полученных из событий по ОЗ в ПК «Efros DO»;
- инвентаризация и ведение единого списка ОЗ;
- топология сети;
- мониторинг уведомлений о событиях контроля и об ошибках с ОЗ;
- мониторинг состояния ОЗ, подключенных к системе, в графическом и текстовом виде;
- формирование отчетов событий по ОЗ для модулей интеграции;
- ведение журнала системных событий;
- администрирование и настройка ПК «Efros DO»;
- идентификация и аутентификация пользователей комплекса на сервере ПК «Efros DO» с использованием идентификаторов и паролей;
- ведение списка пользователей комплекса с возможностью управления пользователями (добавление пользователей, групп пользователей, блокировка, активация, деактивация, удаление учетной записи пользователя, смена пароля пользователя);
- ролевое и дискреционное разграничение доступа пользователей комплекса к серверу ПК «Efros DO», к списку контролируемых на сервере ОЗ;
- управление ролями пользователей комплекса;
- создание, классификация и диспетчеризация заявок;
- функции модуля контроля конфигураций и топологии сети «Efros Network Assurance»;
- функции модуля оптимизации и настройки межсетевых экранов «Efros Firewall Assurance»;
- функции модуля контроля целостности и проверки соответствия хостов и конечных точек «Efros Integrity Check Compliance»;
- функции модуля анализа уязвимостей и построения векторов атак «Efros Vulnerability Control»;
- функции модуля сбора статистики по потокам данных в сети «Efros Network Flow Analysis»;

— функции модуля разграничения и контроля доступа в сети «Efros Network Access Control»;
— функции модуля анализа и управления объектами защиты в разделе «Центр задач»
«Efros Change Manager».

Модули ПК "Efros DO" интегрируются в систему с учетом особенностей функционирования. Комплекс обеспечивает работу общих сервисов, техническое взаимодействие между ними и совместное функционирование процессов.
Единый веб-интерфейс ПК «Efros DO» позволяет пользователям с ролью администратора получить доступ к следующим возможностям:

1) Управление объектами сети:
— просмотр ОЗ;
— инвентаризация параметров сети и управление не сконфигурированными ОЗ (добавление/удаление ОЗ);
— просмотр карты сети ОЗ;
— база знаний по ОЗ;
— векторы атак;
— ведение списка контролируемого клиентского оборудования (конечных точек сети и их групп);
— сканирование сети.
2) Контроль устройств:
— настройка доступа к объектам сети/группам объектов сети;
— проверка безопасности;
— проверка МЭ;
— настройка профилей подключения;
— просмотр отчетов о событиях;
— настройка обработчиков событий;
— настройка профилей аутентификации;
— настройка SNMP профилей;
— настройка проверки доступности устройств.
3) Контроль доступа в сеть и к оборудованию:
— управление устройствами/группами устройств;
— управление сетевыми пользователями/группами сетевых пользователей, имеющих доступ к активному сетевому оборудованию (АСО);
— настройка политик доступа;
— настройка условий доступа;
— настройка профилей авторизации;
— настройка профилей оборудования;
— редактирование разрешенных протоколов аутентификации;

— редактирование набора команд;
— настройка подключения к сервисам протоколов TACACS+ и/или RADIUS;
— загрузка ACL;
— словари атрибутов;
— создание и управление гостевыми порталами.

4) Администрирование:
— управление пользователями/группами пользователей;
— управление лицензиями на подключаемые модули;
— просмотр системных событий;
— настройка планировщика задач и событий;
— ведение списка корневых, серверных и клиентских сертификатов, создание запросов на сертификаты.

5) Управление настройками ПК «Efros DO»:
— настройка домена Active Directory (AD);
— управление триггерами Flow;
— управление гостевым порталом;
— аутентификация ACO.

6) Мониторинг:
— визуализация процессов, обеспечивающих информационную безопасность, с помощью встроенных и гибко настраиваемых схем в графическом виде с текстовым пояснением.

В ПК «Efros DO»:

1) Реализована поддержка протоколов для аутентификации, авторизации и учета действий пользователя на сетевых устройствах:
— протоколы TACACS+ и/или RADIUS.

2) Установлены внешние модули, отвечающие за активный аудит сетевого оборудования, серверных и клиентских операционных систем (далее — ОС):
— модуль взаимодействия с сетевыми устройствами (использует протоколы SSH/Telnet);
— модуль управления устройствами, модуль взаимодействия с устройствами Континент, Dionis, Docker (использует протоколы SCP, SFTP);
— модуль взаимодействия с CheckPoint (использует протоколы CPMI и LEA);
— модуль отправки писем по протоколу SMTP (использует протокол SMTP);
— модуль отправки syslog-сообщений и syslog-сервера (использует протокол Syslog);
— модуль отправки сообщений через MS Exchange (использует Microsoft Exchange Web Services Managed API);
— сканер сети для последующего добавления найденных устройств в список устройств (использует протокол SNMP);
— модуль взаимодействия с MS SQL (использует протокол Microsoft TDS);

— модуль взаимодействия с Oracle (использует протокол Oracle.Net);
— модуль взаимодействия с PostgreSQL, Jatoba (использует протокол PostgreSQL Protocol);
— модуль взаимодействия с MySQL (использует протокол MySQL);
— модуль взаимодействия с Firebird (использует протокол Firebird Wire Protocol);
— модуль взаимодействия с UserGate (использует протокол XML-RPC);
— Windows–агент (использует проприетарный протокол на базе HTTPS);
— модуль взаимодействия с устройствами по протоколу REST.

3) Созданы правила доступа путем сопоставления пользователя и сетевого устройства, и назначения пользователю списка доступных команд:
— обновления в настройках доступа применяются сразу после изменения параметров пользователя/групп пользователей и устройства/групп устройств.

1.2.1 Модуль контроля конфигураций и топологии сети «Efros Network Assurance»

Модуль «Efros NA» реализует следующие функциональные возможности «ПК «Efros DO»:

— контроль изменения конфигураций сетевого оборудования;
— контроль изменения конфигураций МЭ;
— проверки соответствия безопасности сетевого оборудования;
— проверки соответствия безопасности МЭ;
— моделирование трафика на основе маршрутов и правил МЭ.

Данные возможности доступны только при наличии лицензии на использование функционального модуля «Efros NA».

1.2.2 Модуль оптимизации и настройки межсетевых экранов «Efros Firewall Assurance»

Модуль «Efros FA» реализует следующие функциональные возможности ПК «Efros DO»:

— формирование отчетов по оптимизации правил, выявление теневых, избыточных, неиспользуемых правил;
— проверка правил МЭ на соответствие требованиям запрета или разрешения транзитного трафика между зонами;
— проверка правил МЭ на соответствие требованиям настройки;
— зонный анализ;

— формирование стандартов МЭ.

Данные возможности доступны только при наличии лицензии на использование функционального модуля «Efros FA».

1.2.3 Модуль контроля целостности и проверки соответствия хостов и конечных точек «Efros Integrity Check Compliance»

Модуль «Efros ICC» реализует следующие функциональные возможности ПК «Efros DO»:

— контроль изменения конфигураций ОС, виртуализации и прикладного программного обеспечения (далее – ППО);

— контроль целостности файлов ОС, виртуализации и ППО;

— проверки соответствия безопасности ОС, виртуализации и ППО.

Данные возможности доступны только при наличии лицензии на использование функционального модуля «Efros ICC».

1.2.4 Модуль анализа уязвимостей и построения векторов атак «Efros Vulnerability Control»

Модуль «Efros VC» реализует следующие функциональные возможности ПК «Efros DO»:

— выявление известных уязвимостей на основе версии ОС;

— синхронизация списков уязвимостей с собственной базой данных по уязвимостям;

— синхронизация с активными сканерами уязвимостей для получения информации об ОЗ;

— построение векторов атак.

Данные возможности доступны только при наличии лицензии на использование функционального модуля «Efros VC».

1.2.5 Модуль сбора статистики по потокам данных в сети «Efros Netflow Analyzer»

Модуль «Efros NFA» реализует следующие функциональные возможности ПК «Efros DO»:

— предоставление информации по соединениям, с параметрами скорости,

длительности и принадлежности к адресам;

- сбор статистики использования сетевого трафика по соединениям и анализ активности;
- контроль изменений IP и MAC-адресов;
- работа с протоколами NetFlow, sFlow, IPFIX и NetStream.

Данные возможности доступны только при наличии лицензии на использование функционального модуля «Efros NFA».

1.2.6 Модуль разграничения и контроля доступа в сеть «Efros Network Access Control»

Модуль «Efros NAC» реализует следующие функциональные возможности ПК «Efros DO»:

- управление доступом в сетевые сегменты с применением расширенных политик доступа в сеть, управление административным доступом к АСО;
- формирование расширенных политик управления доступом на основе собранной статистики и создание графического конструктора, позволяющего создавать наборы политик;
- профилирование конечных устройств (конечных точек);
- создание новых правил авторизации на основе уже существующих;
- регистрация и учет попыток подключения конечных точек и пользователей;
- синхронизация пользователей с источником LDAP;
- взаимодействие со службами каталогов LDAP (MS Active Directory, FreeIPA, OpenLDAP, ALD Pro);
- трассировка сессий RADIUS аутентификации;
- проверка значений RADIUS-атрибутов на основе регулярных выражений;
- отправка уведомлений в RADIUS о событиях на конечных точках (CoA, Disconnect);
- загрузка RADIUS-атрибутов производителей;
- использование политик TACACS+ для доступа на сетевое оборудование;
- трассировка сессий TACACS+ аутентификации;
- доступ на оборудование по протоколу TACACS+;
- гостевые порталы.

Данные возможности доступны только при наличии лицензии на использование функционального модуля «Efros NAC».

1.2.7 Модуль анализа и управления объектами защиты в разделе «Центр задач» «Efros Change Manager»

Модуль «Efros CM» реализует следующие функциональные возможности ПК «Efros DO»:

— автоматизация управления жизненным циклом правил МЭ.

1.3 Роли пользователей

Пользователями ПК «Efros DO» являются:

- пользователи (администраторы) ПК «Efros DO»;
- пользователи (администраторы) ОЗ;
- пользователи сервисов (сетевые пользователи), предоставляемых ОЗ (контролируемыми устройствами) и гостевыми порталами.

Возможности пользователя в ПК «Efros DO» зависят от назначенной роли и определяются настройкой выбранных привилегий. Для пользователя ОЗ определяется список доступных ОЗ и права доступа на них.

Сетевые пользователи не имеют доступа к веб-приложению ПК «Efros DO», но имеют доступ к назначенным в комплексе сетевым устройствам или ресурсам.

После установки и настройки ПК «Efros DO» в БД автоматически создается учетная запись пользователя с ролью встроенного системного администратора «GlobalAdministrator» и логином «SuperAdmin».

2 Условия выполнения ПК «Efros DO»

Минимальный состав технических средств электронно-вычислительной машины (далее — ЭВМ)[1] для установки серверной части и внешних модулей ПК «Efros DO» рассчитывается на основе данных, приведенных в таблице 3.

Таблица 3 – Минимальные требования к производительности сервера ПК

Поле	Параметры		
Количество объектов защиты (ОЗ)	До 500	До 1000	До 2000*
Требования к программному обеспечению			
ОС	Astra Linux Special Edition (v. 1.6, v.1.7), сертификат соответствия № 2557 (выдан ФСТЭК России 27 января 2012 г.); Astra Linux Common Edition (v.2.12); Альт 10 Server; РЕД ОС 7.3 Муром, сертификат соответствия № 4060 (выдан ФСТЭК России 12.01.2019 г.)		
Поддерживаемые системы управления базами данных (СУБД)	СУБД PostgreSQL 13; СУБД «Jatoba»		
Прикладное ПО	Docker 18.03.0 и выше; Docker-compose v2.9.0; Confluent Kafka 5.5.0		
Требования к аппаратному обеспечению			
Процессор	12 ядер (от 2 ГГц)	16 ядер (от 2 ГГц)	16 ядер (от 2 ГГц)
Оперативная память, не менее Гб	от 16 Гб	от 32 Гб	от 64 Гб
Жесткий диск, Гб (ПК + СУБД)	от 600 Гб	от 1200 Гб	от 2400 Гб
Сервер ПК, Гб	от 200 Гб	от 200 Гб	от 200 Гб
Сервер СУБД, Гб	от 400 Гб	от 1000 Гб	от 2200 Гб
Сетевая карта	1 Гбит/с	1 Гбит/с	1 Гбит/с
Требования для функционирования модуля «Efros NAC»			
TACACS+	порт 49		
RADIUS	порты 1812, 1813		
Требования для функционирования модуля «Efros NFA»			
Netflow v9+, IPFIX	порт 2056		
sFlow	порт 6343		
Netflow v5	порт 2055		

[1] Под ЭВМ понимается электронно–вычислительная машина, совместимая с архитектурой Intel x86 (x86_64)

Поле	Параметры
Требования для функционирования модулей «Efros NA», «Efros FA», «Efros ICC», «Efros VC», «Efros CM»	
Для подключения Windows–агента	порт 20002
syslog	порт 514
SNMP Trap / Inform	порт 162
Windows-агент	
ОС	Windows**
Процессор	1,6 ГГц
Оперативная память	1 Гб
Жесткий диск	100 Мб
Единый интерактивный веб–интерфейс обеспечивает доступ пользователей к функциональности ПК «Efros DO» с использованием браузера, который работает на основе проекта с открытым кодом Chromium	
*От 2000 ОЗ – параметры рассчитываются индивидуально. Необходимо обратиться в техподдержку по почте support@gaz-is.ru **ОС серии Windows: Windows Server 2008R2 Foundation Edition SP1 (64-разрядная); Windows Server 2008R2 Standard Edition SP1 (64-разрядная); Windows Server 2008R2 Enterprise Edition SP1 (64-разрядная); Windows Server 2008R2 Datacenter Edition SP1 (64-разрядная); Windows Server 2012/2012R2 Foundation (64-разрядная); Windows Server 2012/2012R2 Essentials (64-разрядная); Windows Server 2012/2012R2 Standard (64-разрядная); Windows Server 2012/2012R2 Datacenter (64-разрядная); Windows Server 2016 Standard (64-разрядная); Windows Server 2016 Datacenter (64-разрядная); Windows Server 2016 Essentials (64-разрядная); Windows Server 2019 Standard (64-разрядная); Windows Server 2019 Datacenter (64-разрядная); Windows Server 2019 Essentials (64-разрядная); Windows 7 Professional SP1 (32-разрядная/64-разрядная); Windows 7 Enterprise SP1 (32-разрядная/64-разрядная); Windows 7 Ultimate SP1 (32-разрядная/64-разрядная); Windows 8.1 Core (32-разрядная/64-разрядная); Windows 8.1 Professional (32-разрядная/64-разрядная); Windows 8.1 Enterprise (32-разрядная/64-разрядная); Windows 10 Home (32-разрядная/64-разрядная); Windows 10 Pro (32-разрядная/64-разрядная); Windows 10 Enterprise (32-разрядная/64-разрядная)	

Для эксплуатации и эффективного применения ПК «Efros DO» необходимо использование на ЭВМ лицензионного системного программного обеспечения.

3 Работа с ПК «Efros DO»

3.1 Запуск веб-приложения ПК «Efros DO»

3.1.1 Аутентификация пользователя

Для запуска веб-приложения ПК «Efros DO» пользователю необходимо:

1) Запустить веб-браузер.
2) Ввести в адресной строке открывшегося окна сетевой адрес приложения. Сетевой адрес приложения пользователю должен сообщить администратор, занимающийся обслуживанием ПК «Efros DO».
3) Нажать клавишу «Enter» на клавиатуре. На экране монитора откроется страница авторизации пользователя (рис. 1).
4) Ввести в поле «Логин» имя учетной записи пользователя.
5) Ввести в поле «Пароль» пароль пользователя.
6) Нажать кнопку «Подключиться».

В случае некорректного ввода данных появится сообщение об ошибке под кнопкой «Подключиться».

Рисунок 1 – Страница авторизации пользователя

При первой авторизации ПК «Efros DO» предложит сменить текущий пароль, установленный при создании пользователя, на новый. После смены пароля для работы в комплексе необходимо выполнить повторную авторизацию.

В случае успешной аутентификации откроется страница «Мониторинг» (рис. 2). Если в течение 10 минут[2] пользователь будет неактивен, то есть не будет взаимодействовать с веб-интерфейсом комплекса, сессия пользователя будет заблокирована до его повторной авторизации (рис. 3).

В этом случае пользователю необходимо либо завершить работу с интерфейсом ПК «Efros DO», закрыв соответствующую вкладку веб–браузера, либо выполнить повторный вход.

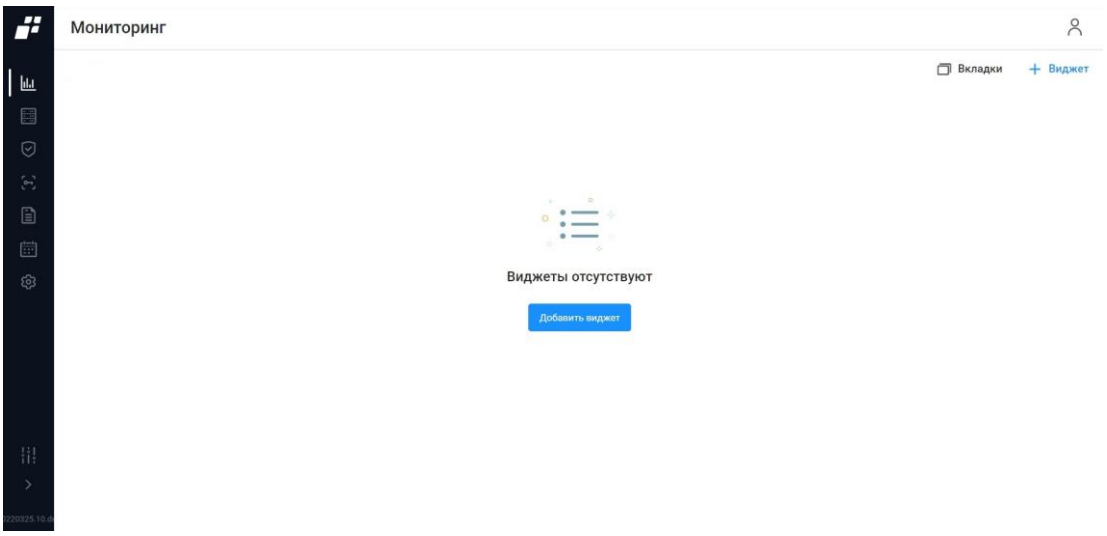


Рисунок 2 – Раздел «Мониторинг»

Рисунок 3 – Окно перехода к повторной аутентификации в ПК «Efros DO»

[2] Данный параметр можно изменить (Администрирование → Пользователи → Настройки безопасности → Прерывание сессии пользователя)

3.1.2 Настройка учетной записи пользователя ПК «Efros DO»

Графический интерфейс приложения ПК «Efros DO» представляет собой набор веб–страниц. При работе с приложением все функции меню веб–браузера остаются полностью доступными.

Типовая информационная структура страницы приложения ПК «Efros DO» включает:

1) Заголовок страницы, содержащий:
— логотип (пиктограмму) ПК «Efros DO»;
— название страницы (название раздела приложения);
— кнопку «Аккаунт» ( ), при выборе которой открывается следующее меню (рис. 4):
а) логин текущего пользователя (доступен только для просмотра);
б) блок «Оформление» – для выбора цветового решения интерфейса приложения (тема) и анимации интерфейса, используемого текущим пользователем. Выбор осуществляется активированием переключателя. Выбранная тема и анимация применяются сразу без перезапуска приложения;

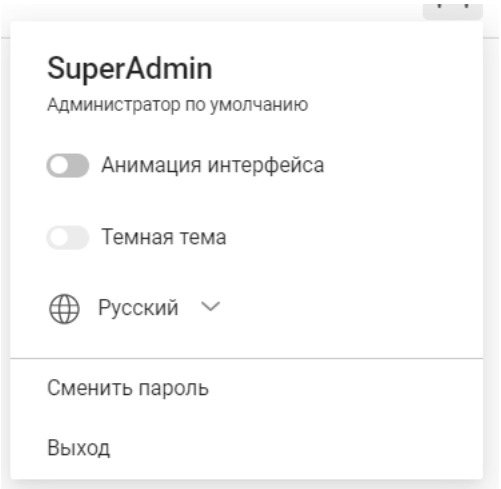


Рисунок 4 – Меню «Аккаунт»

в) поле «Язык приложения». По умолчанию задан русский язык;
г) кнопка «Сменить пароль»;
д) кнопка «Выход», при нажатии на которую происходит выход из веб–приложения и открывается страница авторизации пользователя (см. рис. 1);

2) Панель главного меню содержит:
— различные разделы для работы с комплексом;
— строку управления отображением панели главного меню. В развернутом состоянии панели строка имеет вид в соответствии с рис. 5, в свернутом отображаются пиктограммы, обозначающие разделы. Выбор пиктограммы позволяет перейти на страницу соответствующего раздела и раскрыть меню без

разворачивания панели главного меню.

3) Рабочая область страницы содержит блоки с данными выбранного раздела/подраздела приложения и версию продукта. Версия продукта является ссылкой, при нажатии на которую появляется окно с информацией о версии и доступности сервисов комплекса.

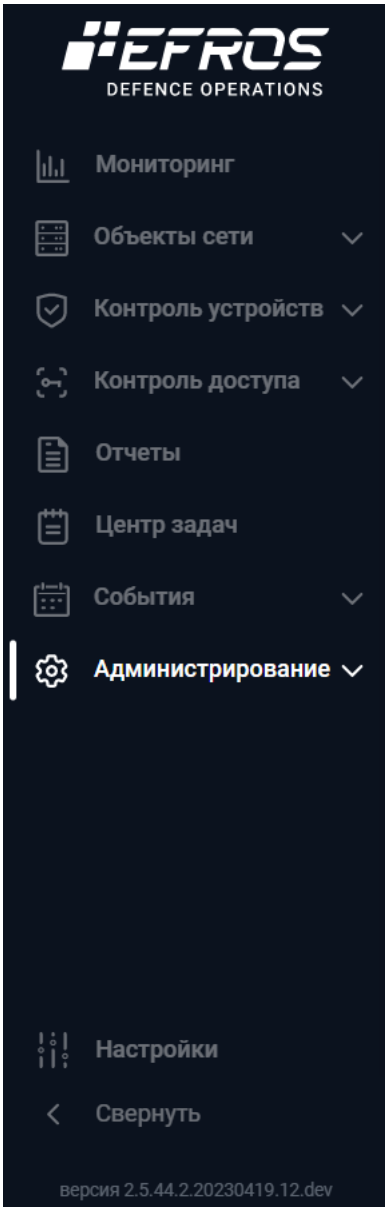


Рисунок 5 – Меню в развернутом виде

4 Раздел «Мониторинг»

Раздел представляет собой вкладки, состоящие из интерактивных отчетов (виджетов) в реальном времени по всем параметрам комплекса.

Для перехода в раздел необходимо выбрать в главном меню раздел «Мониторинг», или, если панель меню свернута, нажать на пиктограмму «», панель автоматически раскроется и отобразятся все разделы.

Отображаемые данные и доступная функциональность в разделе «Мониторинг» зависит от наличия хотя бы одной лицензии на функциональные модули.

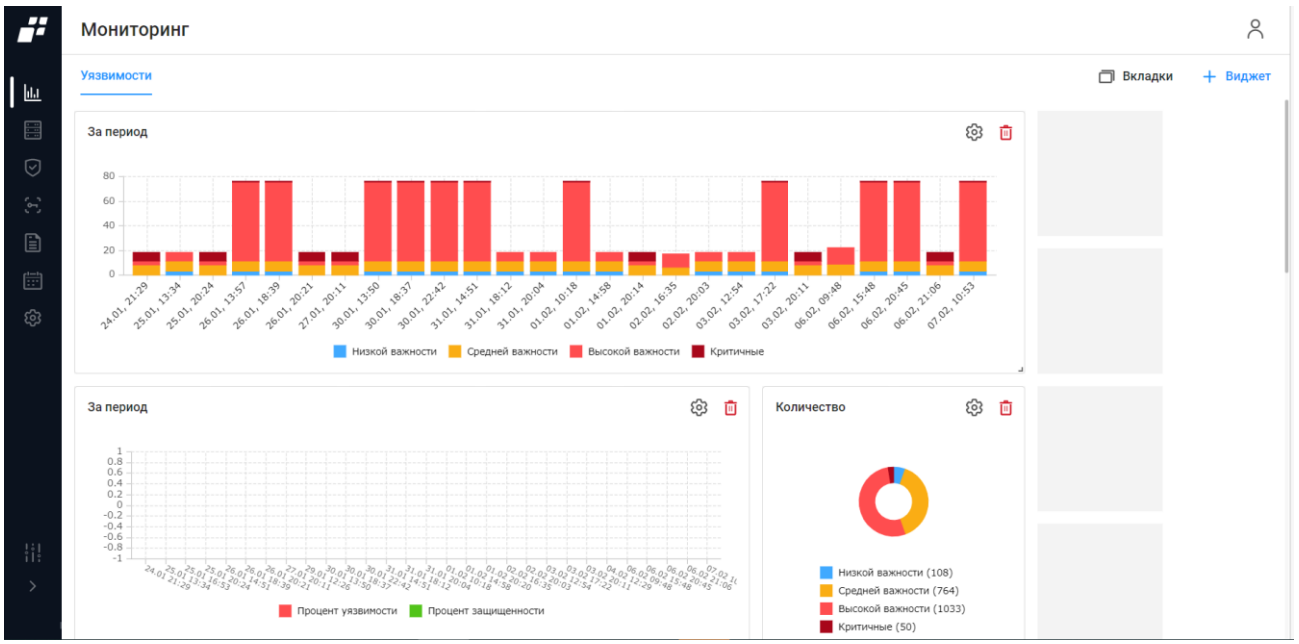


Рисунок 6 – Раздел «Мониторинг»

После установки комплекса раздел «Мониторинг» не содержит ни одной вкладки, на странице отображается сообщение *«Вкладки отсутствуют. Вам необходимо добавить хотя бы одну вкладку, чтобы добавить виджеты»* и кнопка «Добавить вкладку» для перехода в окно создания новой вкладки.

На странице отображаются следующие данные:

- вкладки (количество вкладок не ограничено);
- кнопка «Вкладки» (Вкладки) для добавления новой вкладки;
- кнопка «Виджет» (+ Виджет) для добавления нового виджета.

4.1 Добавление новой вкладки и виджета

Для добавления вкладки необходимо выполнить следующие действия:

1) Нажать кнопку «Вкладки» (Вкладки).
2) Откроется окно «Вкладки» (рис. 7). Необходимо указать название вкладки и нажать кнопку «Сохранить». При необходимости добавления нескольких вкладок пользователю нужно нажать на « + », при необходимости удалить вкладку нажать на « 🗑 ».

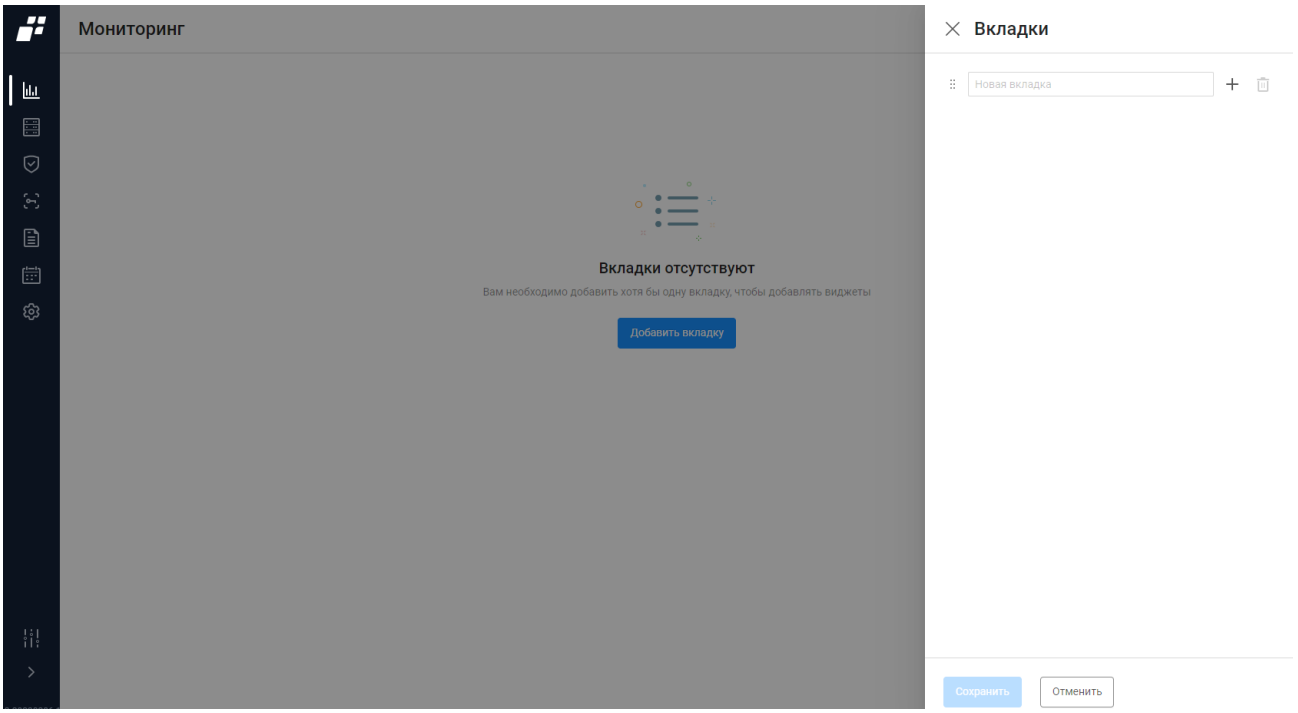


Рисунок 7 – Окно «Вкладки»

Для добавления нового виджета необходимо:

1) В созданной вкладке нажать на кнопку «Виджет» (+ Виджет).
2) Откроется окно «Библиотека виджетов» (рис. 8). Состав и описание виджетов приведены в таблице 4.

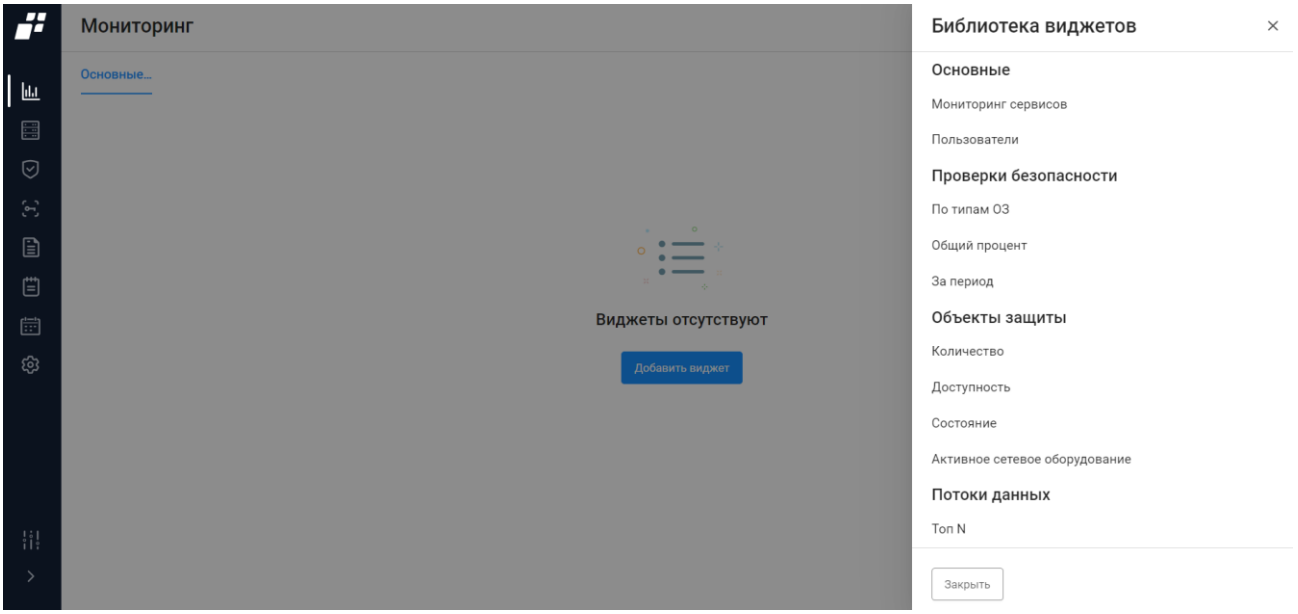


Рисунок 8 – Окно «Библиотека виджетов»

Таблица 4 – Состав и описание виджетов раздела «Мониторинг»

Поле	Описание
Группа виджетов «Основные»	
Мониторинг сервисов	Показывает состояние сервисов ПК «Efros DO». Позволяет быстро остановить, перезапустить или запустить сервисы
Пользователи	Показывает: — суммарное количество пользователей комплекса; — суммарное количество заблокированных пользователей комплекса; — суммарное количество активных пользователей комплекса
Группа виджетов «Уязвимости»	
Количество	Показывает данные по уязвимостям на текущий момент. Происходит динамическое обновление данных по выявленным уязвимостям
За период	Показывает график изменения количества ОЗ (вендоров) с выявленными уязвимостями за период – приводятся сведения о количестве ОЗ для каждой степени критичности уязвимостей за определенный шаг
Группа виджетов «Проверка безопасности»	
По типам ОЗ	Показывает данные последней проверки всех ОЗ каждого типа на текущий момент времени
Общий процент	Показывает данные последней проверки на текущий момент: — всего правил по всем возможностям, назначенным ОЗ; — количество выполненных правил;

Поле	Описание
	— процентное отношение выполненных правил к назначенным
За период	Показывает данные последней проверки в заданный промежуток времени: — всего правил по всем ОЗ в каждой точке заданного интервала; — количество выполненных правил в каждой точке заданного интервала; — процентное отношение выполненных правил к назначенным в каждой точке заданного интервала
Группа виджетов «Объекты защиты»	
Количество	Показывает данные о количестве ОЗ на текущий момент, сгруппированные по назначенным возможностям «Контроль доступа», «Контроль устройств», «Контроль трафика (Потоки)». Показывает количество несконфигурированных ОЗ[3]
Доступность	Показывает данные по доступности устройств на текущий момент
Состояние	Содержит графическое представление информации о количестве контролируемых ОЗ и результатах их проверок на уязвимости
Активное сетевое оборудование	Показывает ОЗ с назначенной возможностью «Контроль доступа» и сгруппированные по наличию протокола RADIUS/TACACS+ с указанием количества каждой группы к общему количеству ОЗ типа АСО: — «TACACS+»; — «RADIUS»; — «TACACS+ и RADIUS»
Группа виджетов «Потоки данных»	
Топ N	Три вида графиков в зависимости от параметра в поле «Тип»: — «Отправители» – представляет собой диаграмму из списка отправителей (IP-адрес источника), отсортированных по убыванию объема информации, которая была отправлена за последние несколько минут; — «Получатели» – представляет собой диаграмму из списка получателей (IP-адрес получателя), отсортированных по убыванию объема информации за последние несколько минут; — «Сервисы» – представляет собой диаграмму из списка

[3] Несконфигурированный ОЗ или устройство – это устройство, добавленное в базу данных комплекса через подразделы «Объекты защиты» и «Сканирование сети», через разделы «Контроль устройств» и «Контроль доступа», или автоматически.

Поле	Описание
	сервисов, отсортированных по убыванию объема информации за последние несколько минут
Объем трафика во времени	График объема передаваемого и/или полученного трафика в единицу времени за период через контролируемые источники (интерфейсы)

Возможность добавления виджета и информация, отображаемая на ней, зависит от типа установленной лицензии.

Доступность информации на виджетах приведена в таблице 5.

Таблица 5 – Доступность информации на виджетах в зависимости от типа лицензии

Лицензия / Наименование	«Efros DO»	«Efros VC»	«Efros ICC»	«Efros NA»	«Efros FA»	«Efros NFA»	«Efros NAC»
Группа виджетов «Основные»	**+**						**+**
Мониторинг сервисов	+						
Пользователи системы	+						
Сетевые пользователи							+
Группа виджетов «Уязвимости»		**+**					
Статистика уязвимости		+					
Статистика за период		+					
Группа виджетов «Проверки безопасности»			**+**	**+**			
По типам ОЗ			+	+			
Общий процент			+	+			
За период			+	+			
Группа виджетов «Объекты защиты»	**+**	**+**	**+**	**+**	**+**	**+**	**+**
Количество ОЗ	+	+	+	+	+	+	+
Доступность		+	+	+	+		
Состояние		+	+	+	+		
Активное сетевое	+						+

Лицензия / Наименование	«Efros DO»	«Efros VC»	«Efros ICC»	«Efros NA»	«Efros FA»	«Efros NFA»	«Efros NAC»
оборудование							
Группа виджетов «Потоки данных»						+	
Топ N						+	
Объем трафика во времени						+	

3) Из библиотеки необходимо выбрать требуемые виджеты (рис. 9).

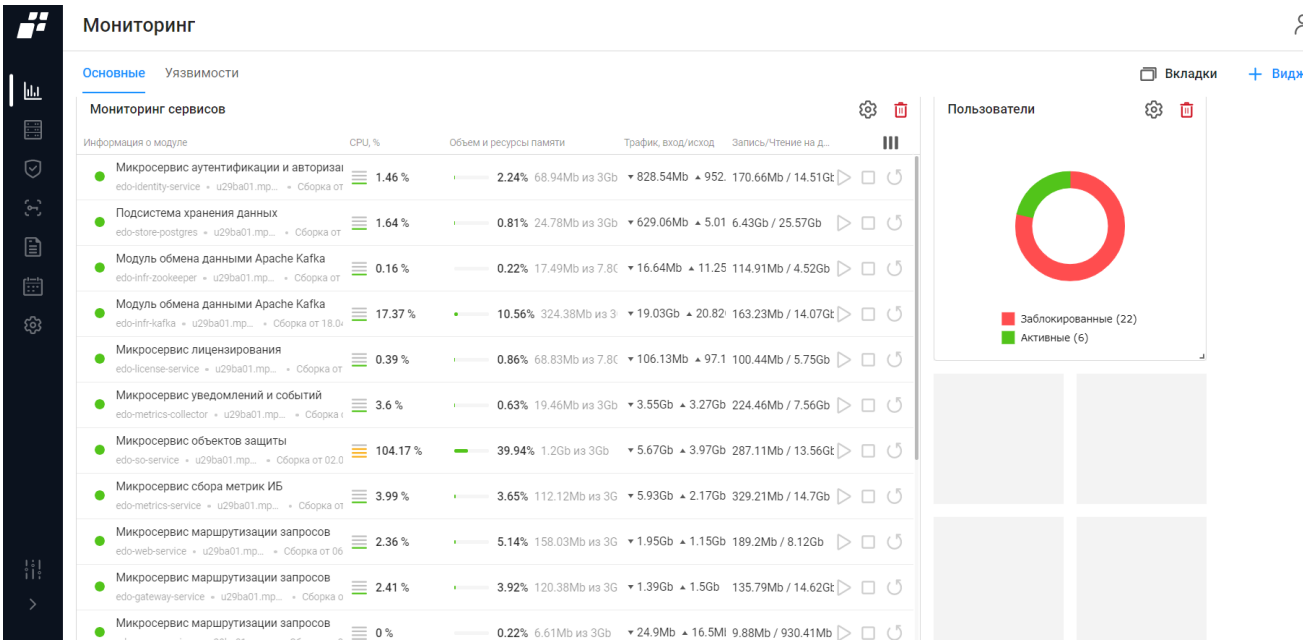


Рисунок 9 – Раздел «Мониторинг» с выбранными виджетами

В поле с виджетом располагаются:

— кнопка «Настройка» ( ) для настройки виджета;

— кнопка «Удалить» ( ) для удаления виджета;

— кнопка «Колонки» ( ) для изменения отображения колонок на виджете «Мониторинг сервисов».

4.2 Редактирование виджета

Редактирование виджета выполняется следующим образом:

1) Выбрать необходимый виджет.
2) Нажать на кнопку «Настройки» ( ).
3) Откроется окно редактирования виджета (рис. 10).

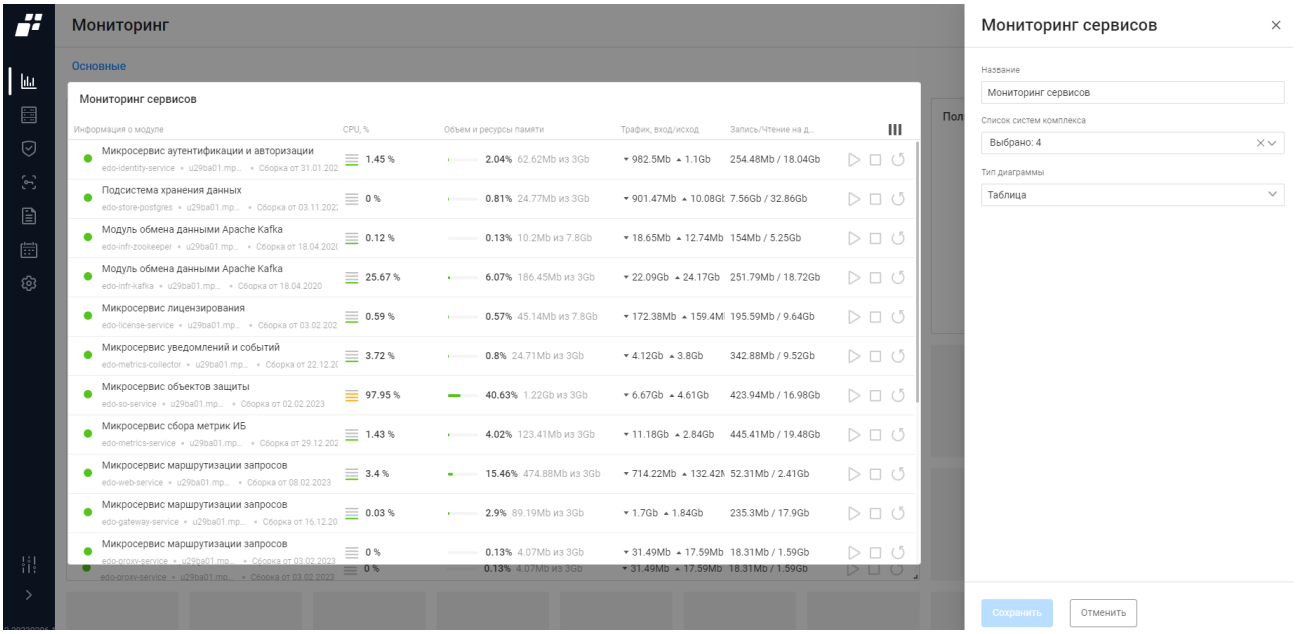


Рисунок 10 – Окно редактирования виджета «Мониторинг сервисов»

Состав окна редактирования зависит от выбранного виджета.

4) Внести требуемые изменения и нажать кнопку «Сохранить».

Для перемещения виджета по полю вкладки необходимо использовать курсор. Для изменения масштаба виджета необходимо переместить курсор в правый нижний угол виджета и растянуть/уменьшить поле с виджетом.

5 Раздел «Объекты сети»

Данный раздел представляет собой агрегированную информацию, характеризующую объект сети со стороны конфигурирования, авторизации и аутентификации.

5.1 Объекты защиты

Отображаемые данные и доступная функциональность в подразделе «Объекты защиты» зависит от наличия хотя бы одной лицензии на функциональные модули.

Данный подраздел представляет собой иерархический список сконфигурированных ОЗ. Сконфигурированный ОЗ – это объект сети, представленный в комплексе как сущность, сформированная на основе возможностей модулей интеграции или содержащая в себе ОЗ с назначенными возможностями модулей интеграции (например, возможность «Контроль доступа» или «Потоки данных»). Возможности модулей интеграции − это совокупность характеристик объекта сети в одном из модулей интеграции, созданная по определенным правилам, установленным в этом модуле, и обеспечивающая выполнение функциональности модуля интеграции. Несконфигурированный ОЗ – это устройство без назначенных возможностей модулей интеграции.

Для просмотра подраздела «Объекты защиты» пользователю необходимо выбрать в панели главного меню раздел «Объекты сети», или, если панель свернута, нажать на пиктограмму «  », панель автоматически раскроется и отобразятся все разделы.

Подраздел «Объекты защиты» (рис. 11), позволяет выполнять следующие действия с ОЗ:

- просмотр/изменение списка ОЗ;
- просмотр/изменение свойств групп ОЗ и отдельных ОЗ;
- конфигурирование ОЗ;
- настройка доступа к ОЗ.

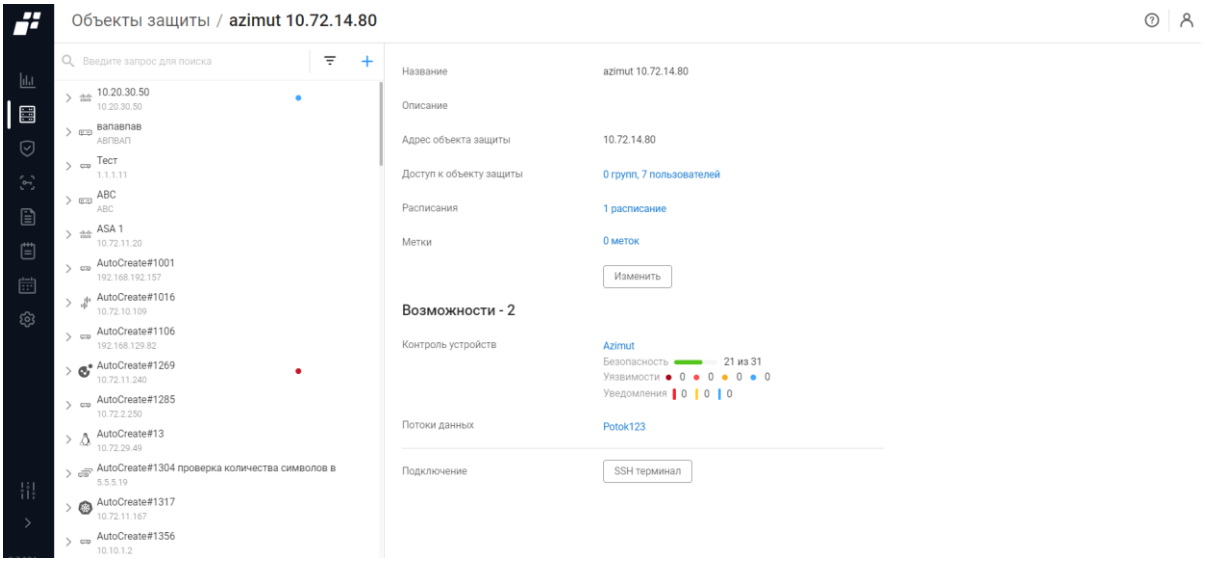


Рисунок 11 – Подраздел «Объекты защиты»

Страница содержит следующие элементы:

- дерево ОЗ – иерархический список сконфигурированных ОЗ, контролируемый ПК «Efros DO»;
- поле с информацией об ОЗ;
- поле «Возможности». Отображается при наличии хотя бы одной лицензии на функциональные модули «Efros NAC», «Efros NFA», «Efros NA», «Efros FA», «Efros VC» или «Efros ICC»;
- кнопка «SSH терминал» (SSH терминал) для подключения к ОЗ.

5.1.1 Дерево объектов защиты

Над деревом ОЗ располагаются:

- поле «Поиск» (Введите запрос для поиска) для поиска искомой записи в списке;
- кнопка «Фильтр» ( ) для фильтрации списка ОЗ;
- кнопка «Добавить» ( ) для создания нового объекта защиты.

При наведении курсора на ОЗ в дереве ОЗ появится кнопка «Контекстное меню» ( ), которая позволяет выполнить следующие действия:

- «Изменить» – внести изменения в параметры ОЗ;
- Добавить возможность «Контроль устройств»;
- Добавить возможность «Контроль доступа»;
- Добавить возможность «Потоки данных»;

— Добавить вложенный ОЗ;
— «Удалить».

При раскрытии ОЗ с помощью кнопки « › » может отображаться:

— иконка « », обозначающая возможность «Контроль устройств», которую назначили ОЗ;
— иконка « », обозначающая возможность «Контроль доступа», которую назначили ОЗ;
— иконка « », обозначающая возможность «Потоки данных», которую назначили ОЗ.

Цвет подсветки строки с ОЗ обозначает следующее (рис. 12):

— зеленый – выполнение операции;
— желтый – обнаружено событие контроля (например, не пройдена проверка устройства);
— красный:
  - при выполнении операции на устройстве возникла ошибка;
  - последняя выполняемая с возможностью операция закончилась ошибкой;
  - на текущий момент устройство не доступно;
  - последняя операция с возможностью закончилась ошибкой аутентификации – для устройства указаны неверные логин/пароль.
— оранжевый – ОЗ переведен в сервисный режим, при этом расписания и триггеры (автоматические опросы и действия) на нем не выполняются, но можно обратиться к нему по запросу пользователя, например, обновить отчеты/конфигурации;
— серый – нет связи;
— отсутствие подсветки – состояние ОЗ стабильно.

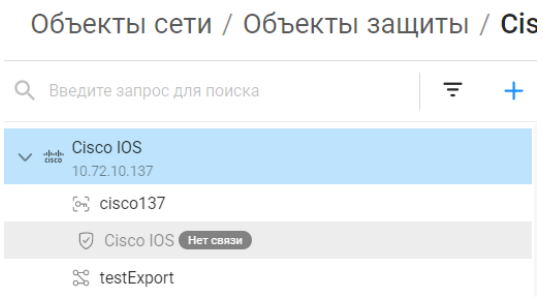


Рисунок 12 – Пример подсветки строки с ОЗ

Контекстное меню устройства с назначенной возможностью «Контроль устройств» позволяет выполнить следующие действия с устройством:

- изменить;
- загрузить конфигурации;
- принять все изменения;
- конфигурировать;
- включить сервисный режим;
- удалить.

Контекстное меню устройства с назначенной возможностью «Контроль доступа» позволяет выполнить следующие действия с устройством:

- изменить;
- удалить.

Контекстное меню устройства с назначенной возможностью «Потоки данных» позволяет выполнить следующие действия с устройством:

- изменить;
- создать копию;
- удалить.

При выборе устройства с назначенной возможностью «Контроль устройств» отображаются следующие вкладки[4]:

- «Статус»;
- «Отчеты»;
- «События»;
- «Архив».

При выборе устройства с назначенной возможностью «Контроль доступа» отображается описание ОЗ.

При выборе устройства с назначенной возможностью «Потоки данных» отображаются следующие вкладки:

- «Настройки»;
- «Срабатывания».

Добавление ОЗ осуществляется следующими способами:

- в разделе «Объекты защиты» через дерево ОЗ;
- в разделе «Контроль устройств» (более подробно см. документ «Руководство

[4] Более подробно данные вкладки описаны в документе «Руководство пользователя. Часть 2. Контроль устройств»

пользователя. Часть 2. Контроль устройств»);

— в разделе «Контроль доступа» (более подробно см. документ «Руководство пользователя. Часть 3. Контроль доступа»);

— автоматически при получении данных по устройствам из модуля «Efros NFA»;

— в подразделе «Сканирование сети».

5.1.1.1 Добавление ОЗ через дерево ОЗ

Для добавления нового ОЗ вручную необходимо выполнить следующие действия:

1) В дереве ОЗ нажать кнопку «Добавить» (+).
2) Откроется окно «Создание объекта защиты» (рис. 13). Состав и описание полей окна приведены в таблице 6.

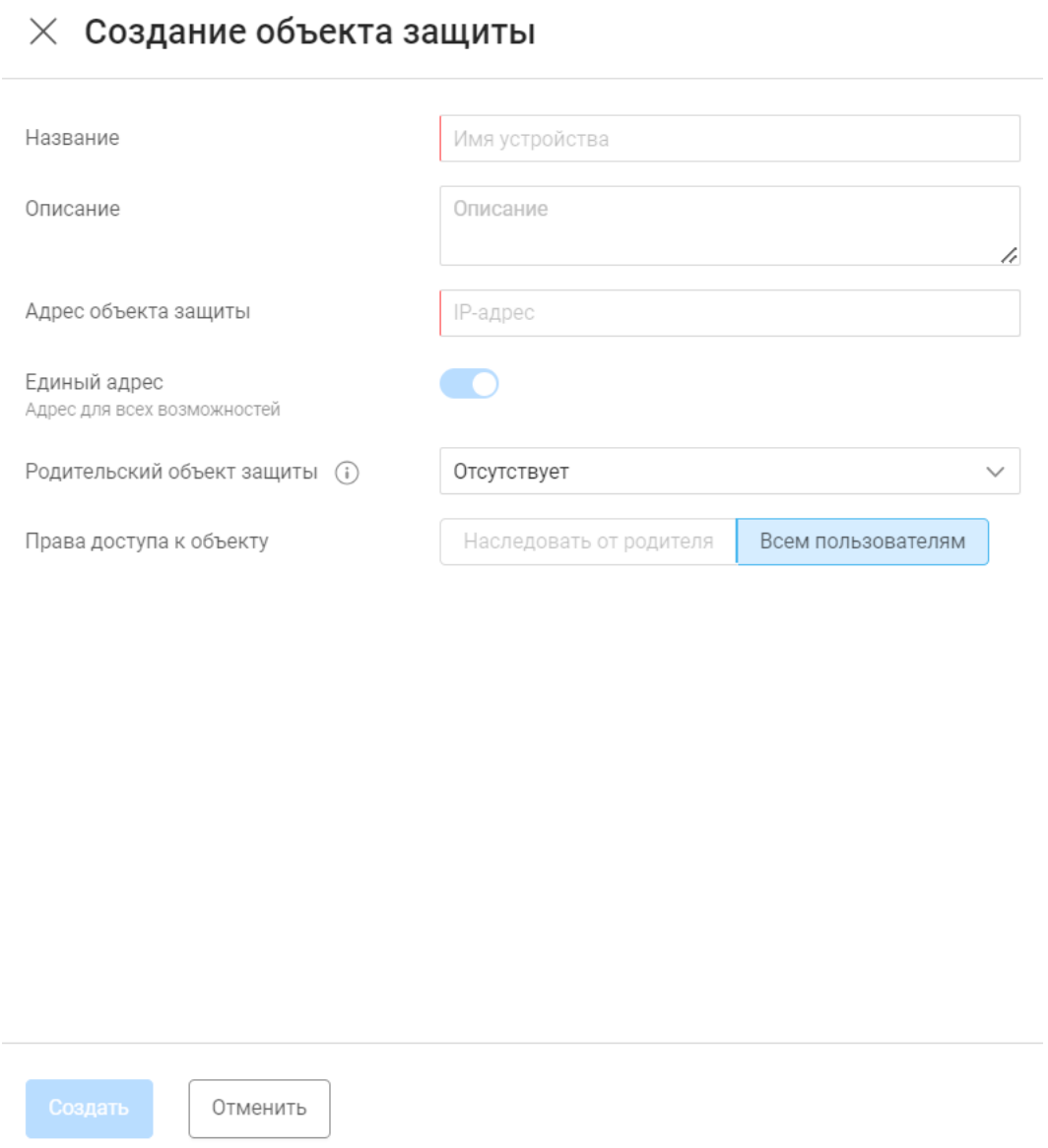


Рисунок 13 – Окно «Создание объекта защиты»

Таблица 6 – Состав и описание полей окна добавления ОЗ

Поле	Описание
Поле «Название»	Текстовое поле для ввода названия оборудования. Параметры ввода текста: от 1 до 50 любых символов
Поле «Описание»	Текстовое поле для ввода описания оборудования. Параметры ввода текста: от 1 до 250 любых символов
Поле «Адрес объекта защиты»	Текстовое поле для ввода IP-адреса ОЗ
Поле «Единый адрес»	Не доступно для редактирования, по умолчанию вкл.
Поле «Родительский ОЗ»	Заполняется автоматически значением ОЗ, которое было выбрано в дереве ОЗ
Поле «Права доступа к ОЗ»	Поле с выбором прав: — «Наследовать от родителя» – ОЗ доступен текущему пользователю; — «Всем пользователям» – ОЗ доступен всем пользователям комплекса
Поле «Доступ к ОЗ»*	Поле позволяет редактировать уровень доступа к ОЗ пользователей и групп пользователей: — Доступ отсутствует – данный ОЗ недоступен пользователю/группе пользователей; — Чтение – пользователь/группа пользователей видит данный ОЗ, но не имеет прав вносить какие–либо изменения; — Полный доступ – пользователь/группа пользователей может менять конфигурацию ОЗ
Поле «Метки»*	Назначение метки для ОЗ позволяет пользователю уточнить фильтрацию в дереве ОЗ
Элементы управления	
Создать	При нажатии на кнопку введенные данные сохраняются
Отменить	При нажатии на кнопку введенные данные не сохраняются
*данные поля появляются при редактировании уже созданного ОЗ	

3) Заполнить поля необходимыми параметрами.
4) Нажать кнопку «Создать».

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

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

5.1.1.2 Добавление вложенного ОЗ

Для добавления вложенного ОЗ необходимо выполнить следующие действия:

1) В дереве ОЗ выбрать ОЗ. Выбранный ОЗ будет родительским.
2) Нажать на кнопку «Контекстное меню» (•••). Выбрать «Добавить вложенный ОЗ».
3) Откроется окно «Создание объекта защиты», приведенное на рис. 13. Состав и описание полей окна приведены в таблице 6.
4) Заполнить поля необходимыми параметрами.
5) Нажать кнопку «Создать».

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

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

5.1.1.3 Добавление возможности «Контроль доступа»

Данная возможность доступна только при наличии лицензии на модуль «Efros NAC»

Для добавления возможности «Контроль доступа» ОЗ необходимо выполнить следующие действия:

1) Выбрать ОЗ в дереве ОЗ.
2) Из контекстного меню выбрать возможность «Контроль доступа».
3) Откроется страница «Создание возможности “Контроль доступа”» (рис. 14).

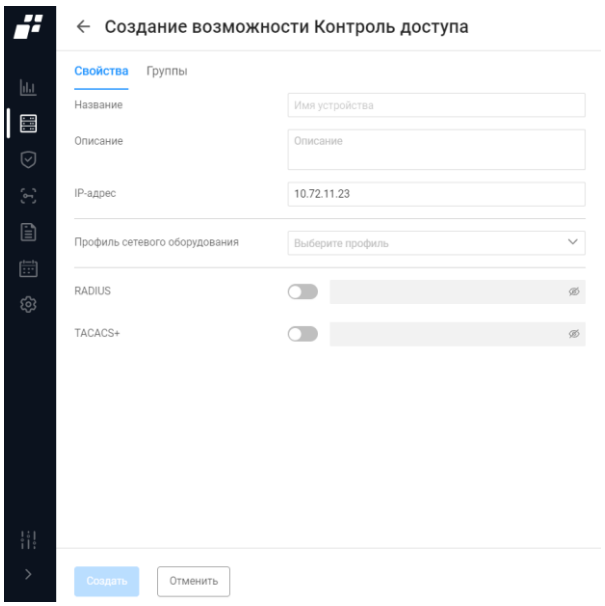


Рисунок 14 – Страница «Создание возможности “Контроль доступа”»

Страница состоит из следующих вкладок:

— «Свойства» – вкладка активна по умолчанию;

— «Группы».

Состав и описание полей вкладки «Свойства» приведены в таблице 7.

Таблица 7 – Состав и описание полей вкладки «Свойства»

Поле	Описание
Поле «Название»	Текстовое поле для ввода имени ОЗ
Поле «Описание»	Текстовое поле для ввода описания ОЗ
Поле «IP-адрес»	Текстовое поле для ввода IP-адреса ОЗ
Поле «Профиль сетевого оборудования»	Раскрывающийся список заранее созданных профилей сетевого оборудования (более подробно см. документ «Руководство пользователя. Часть 3. Контроль доступа»)
Поле «Тип протокола»	Переключатели: — «RADIUS»; — «TACACS+». Активация переключателя означает, что устройство работает с использованием соответствующего протокола. Для активированного протокола необходимо ввести заданный на устройстве разделяемый ключ. При вводе символы ключа заменяются знаком «•». Для просмотра введенного значения необходимо нажать в поле ввода кнопку «Просмотр» ( )
Элементы управления	
Создать	При нажатии кнопки создается возможность «Контроль доступа» у ОЗ
Отменить	При нажатии кнопки выполняется переход на страницу ОЗ без сохранения внесенных данных

4) Заполнить поля вкладки соответствующими параметрами.
5) Перейти на вкладку «Группы» (рис. 15). Состав и описание полей вкладки «Группы» приведены в таблице 8.

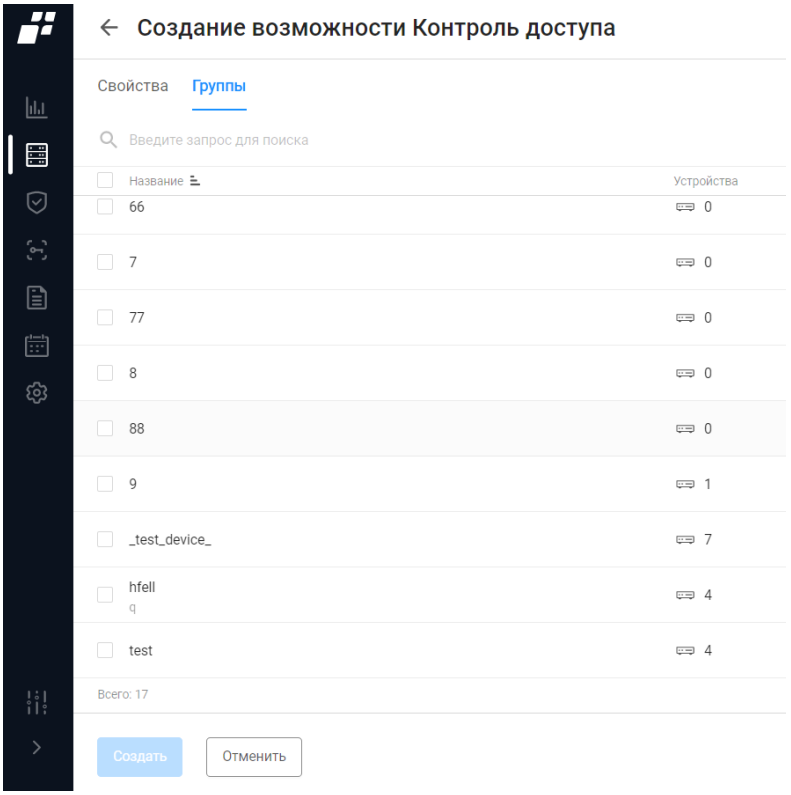


Рисунок 15 – Вкладка «Группы»

Таблица 8 – Состав и описание полей вкладки «Группы»

Поле	Описание
Поле для флага	Выбор определенной группы устройств
Поле «Название»	Содержит следующую информацию: — «Название группы устройств»; — «Описание»
Поле «Устройства»	Содержит информацию о количестве устройств в группе
Элементы управления	
Поле «Поиск»	Ввод последовательности символов из искомой записи
Создать	При нажатии кнопки создается возможность «Контроль доступа»
Отменить	При нажатии кнопки выполняется переход на страницу «Объекты сети», вкладка «Объекты защиты» без сохранения внесенных изменений

6) Добавить, при необходимости, ОЗ в группу устройств, установив флаг в нужной строке.
7) Нажать кнопку «Создать».

Автоматически запускается процесс проверки заполнения всех обязательных полей и уникальности добавляемой возможности.

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

5.1.1.4 Добавление возможности «Контроль устройств»

Данная возможность доступна только при наличии лицензии на функциональные модули «Efros NA», «Efros FA», «Efros ICC» или «Efros VC».

Для добавления возможности «Контроль устройств» ОЗ необходимо выполнить следующие действия:

1) Выбрать ОЗ в дереве ОЗ.
2) Из контекстного меню выбрать возможность «Контроль устройств».
3) Откроется страница «Создание возможности “Контроль устройств”» (рис. 16).

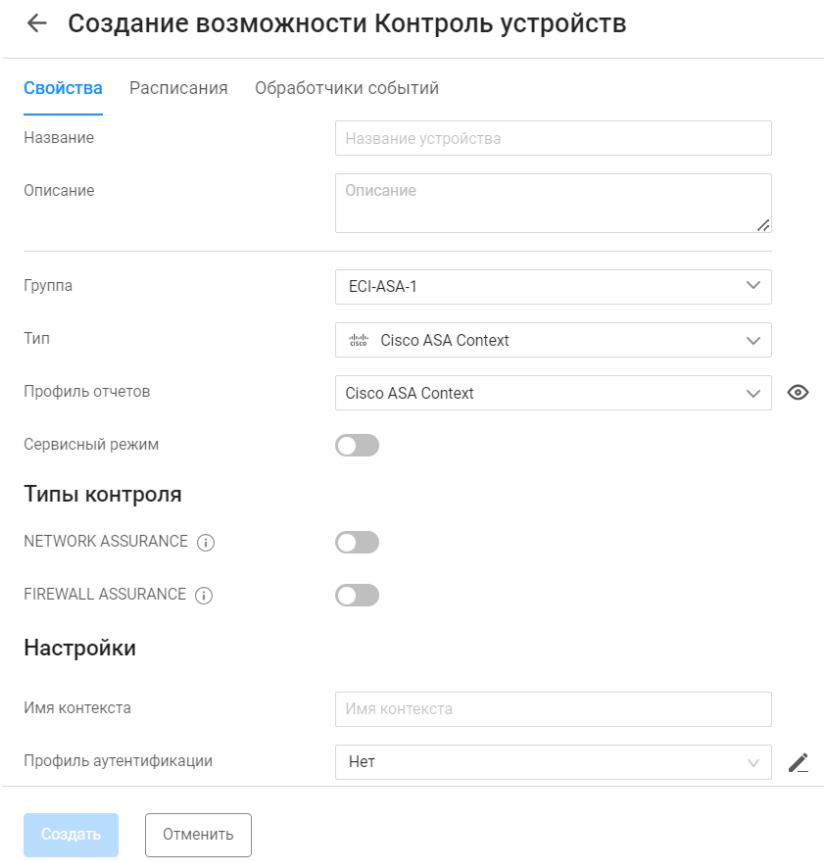


Рисунок 16 – Страница «Создание возможности “Контроль устройств»

Страница состоит из следующих вкладок:

- «Свойства» – вкладка активна по умолчанию;
- «Расписания»;
- «Обработчики событий».

Состав и описание полей вкладки «Свойства» приведены в таблице 9.

Таблица 9 – Состав и описание полей вкладки «Свойства»

Поле	Описание
Поле «Название»	Текстовое поле для ввода названия добавляемого ОЗ
Поле «Описание»	Текстовое поле для ввода краткого описания ОЗ. Например, место размещения оборудования, инвентарный/серийный номер и т.д.
Поле «Группа»	Раскрывающийся список доступных для выбора групп
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 параметров контроля устройств. Поле становится доступно после выбора типа устройства
Поле «Сервисный режим»	Переключатель: включение/отключение сервисного режима для устройства. В сервисном режиме устройство не опрашивается по заданному расписанию. Его доступность не проверяется в автоматическом режиме. Обновление данных выполняется только по запросу пользователя
Группа полей «Типы контроля»	Переключатель. Количество переключателей зависит от наличия лицензий и типа устройства. Переключатель отображается – при наличии лицензии на модуль и доступности типа контроля на устройстве. Переключатель не отображается – лицензия на модуль недоступна. Переключатель отображается, но нет возможности поменять статус – достигнут или превышен лимит лицензий по количеству устройств
Дополнительные параметры подключения зависят от выбранного типа устройства в поле «Тип»	
Элементы управления	
Создать	При нажатии кнопки создается возможность «Контроль устройств» у ОЗ
Отменить	При нажатии кнопки выполняется переход на страницу ОЗ без сохранения внесенных данных

4) Заполнить поля вкладки соответствующими параметрами.
5) Перейти на вкладку «Расписания» (рис. 17). Состав и описание полей вкладки «Расписания» приведены в таблице 10.

На вкладке «Расписания» отображаются только те расписания, у которых выбран статус использования «Вкл.», более подробно описано в п. 5.1.2.

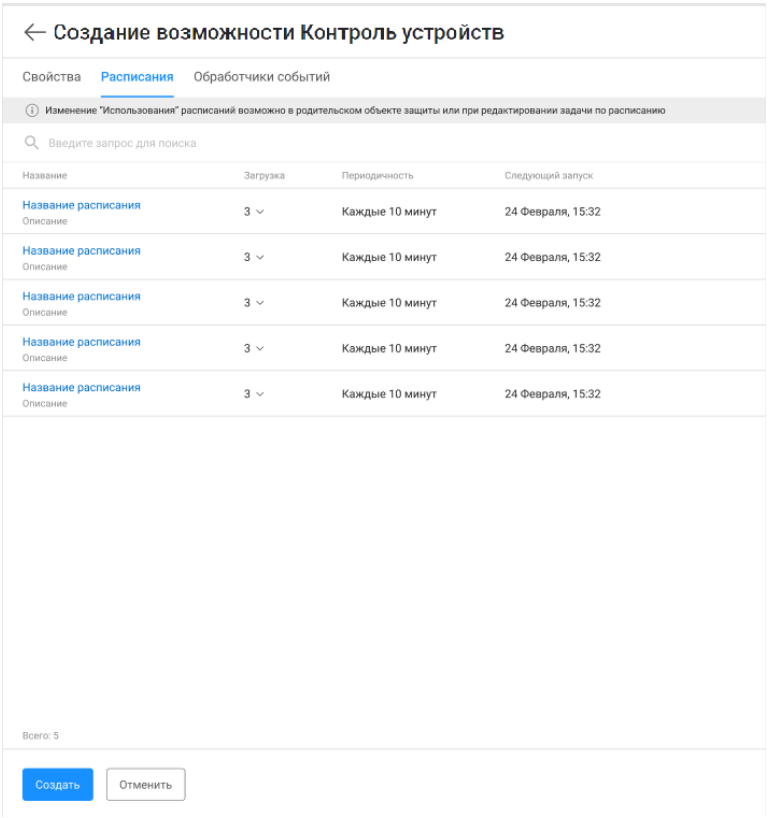


Рисунок 17 – Вкладка «Расписания»

Таблица 10 – Состав и описание полей вкладки «Расписания»

Поле	Описание
Поле «Название»	Название расписания
Поле «Загрузка»	Раскрывающийся список загружаемых отчетов: — «Конфигурации»; — «Проверки безопасности»; — «Уязвимости»
Поле «Периодичность»	Период срабатывания расписания
Поле «Следующий запуск»	Дата и время последнего срабатывания расписания
Элементы управления	
Создать	При нажатии кнопки окно возможности закрывается, возможность отображается у ОЗ

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

6) Перейти на вкладку «Обработчики событий» (рис. 18). Состав и описание полей вкладки «Обработчики событий» приведены в таблице 11.
7) В поле «Использование» выбрать режим срабатывания обработчика событий (на вкладке отображаются только активные обработчики событий).

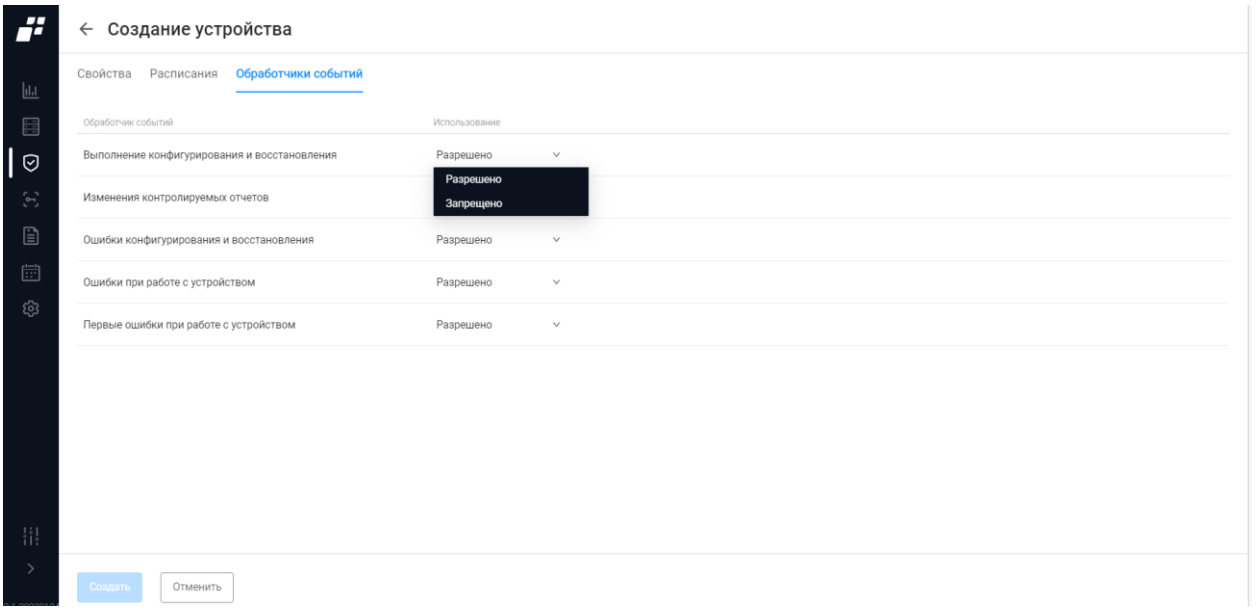


Рисунок 18 – Вкладка «Обработчики событий»

Таблица 11 – 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

8) Нажать кнопку «Создать».

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

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

5.1.1.5 Добавление возможности «Потоки данных»

Данная возможность доступна только при наличии лицензии на функциональный модуль «Efros NFA»

Для добавления возможности «Потоки данных» ОЗ пользователю необходимо выполнить следующие действия:

1) Выбрать ОЗ в дереве ОЗ.
2) Из контекстного меню выбрать возможность «Потоки данных».
3) Откроется страница «Создание возможности “Триггер потока данных”» (рис. 19).

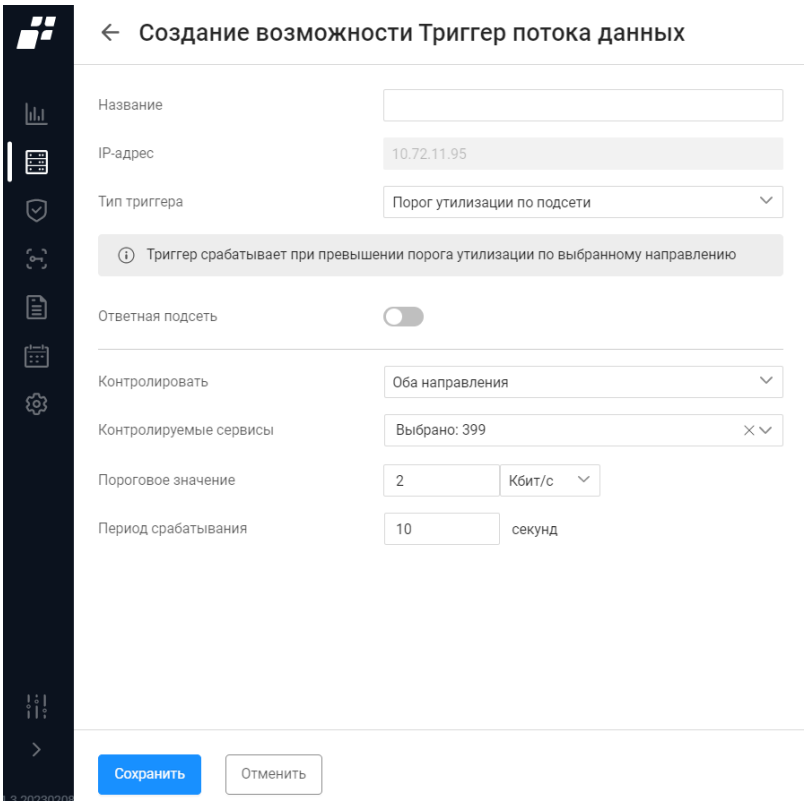


Рисунок 19 – Страница «Создание возможности “Триггер потока данных”»

Состав и описание полей страницы приведены в таблице 12.

Таблица 12 – Состав и описание полей страницы «Создание возможности “Триггер потока данных”»

Поле	Описание
Поле «Название»	Текстовое поле для ввода имени ОЗ
Поле «IP-адрес»	IP-адрес, наследуемый от ОЗ, которому добавляется

	возможность. Поле недоступно для редактирования
Поле «Тип триггера»	Поле с раскрывающимся списком триггеров: — «Порог утилизации по подсети»; — «Порог утилизации по интерфейсу»; — «Переключение каналов»
Дополнительные параметры настройки возможности зависят от выбранного типа триггера в поле «Тип триггера»	
Создать	При нажатии кнопки создается возможность «Триггер потока данных» у ОЗ
Отменить	При нажатии кнопки выполняется переход на страницу ОЗ без сохранения внесенных данных

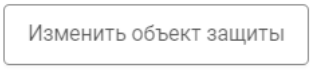
4) Заполнить поля вкладки соответствующими параметрами.
5) Нажать кнопку «Создать».

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

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

5.1.1.6 Изменение параметров ОЗ

Для изменения параметров ОЗ пользователю необходимо выполнить следующие действия:

1) В дереве ОЗ выделить необходимый ОЗ, раскрыть контекстное меню и выбрать в нем пункт «Изменить».
2) В открывшемся окне при необходимости внести изменения в поле «Возможности», отредактировать доступ к ОЗ и метки.
3) Для редактирования параметров ОЗ (название, IP-адрес и др.) необходимо нажать на кнопку « 

».
4) В открывшемся окне редактирования внести требуемые изменения.
5) Нажать кнопку «Сохранить».

Автоматически запустится процесс проверки заполнения всех обязательных полей и уникальности редактируемого ОЗ.

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

5.1.1.7 Фильтрация в дереве ОЗ

Для фильтрации в дереве ОЗ необходимо нажать кнопку «Фильтр» ( ). Откроется окно фильтрации (рис. 20). Состав полей окна и правила их заполнения приведены в таблице 13.

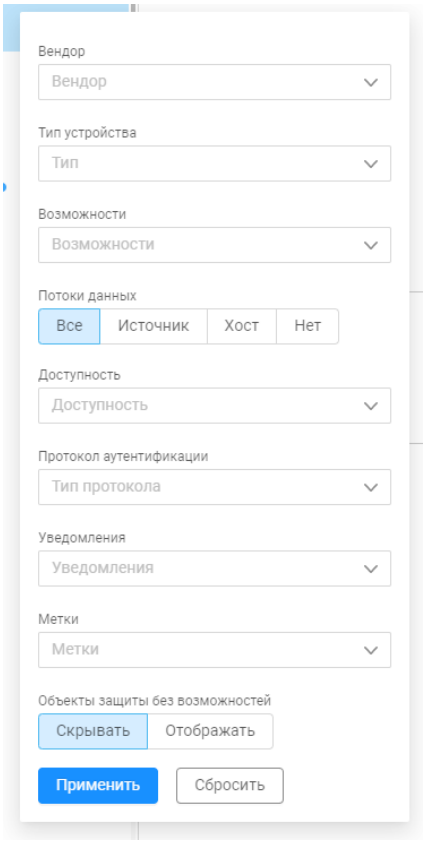


Рисунок 20 – Окно фильтрации ОЗ в дереве ОЗ

Таблица 13 – Состав и описание полей окна фильтрации ОЗ в дереве ОЗ

Поле	Описание
Поле «Вендор»	Раскрывающийся список типов устройств
Поле «Тип устройства»	Раскрывающийся список содержит типы устройств, с которыми работает комплекс: — «Сетевые устройства»; — «Виртуализация»; — «Операционные системы»; — «Прикладное ПО»; — «Сервисы»
Поле «Возможности»	Раскрывающийся список поля содержит перечень возможностей, которые можно назначить ОЗ: — «Контроль устройств»; — «Контроль доступа»;

Поле	Описание
	— «Потоки»
Поле «Потоки данных»	Выбор отображения ОЗ по потокам данных: — «Все»; — «Источник»; — «Хост»; — «Нет»
Поле «Доступность»	Раскрывающийся список содержит информацию о текущем статусе ОЗ в комплексе: — «Доступен»; — «Не доступен»; — «Нет данных»
Поле «Протокол аутентификации»	Раскрывающийся список содержит информацию о протоколах аутентификации сетевых устройств: — «TACACS+»; — «RADIUS»; — «Нет данных»
Поле «Уведомления»	Раскрывающийся список содержит информацию о типе уведомлений о событиях, произошедших на ОЗ: — «Важные»; — «Критичные;» — «Информационные»; — «Нет данных»; — «Нет уведомлений»
Поле «Метки»	Дополнительный параметр фильтрации, создаваемый пользователем при редактировании ОЗ
Поле «Объекты защиты без возможностей»	Выбор отображения ОЗ без возможностей: — «Скрывать»; — «Отображать»
Элементы управления	
Применить	При нажатии кнопки окно фильтрации закрывается, введенные настройки фильтрации применяются
Сбросить	При нажатии кнопки окно фильтрации закрывается без применения введенных настроек

Далее необходимо заполнить поля. После чего окно фильтрации закроется, а в дереве отобразятся ОЗ, соответствующие заданным параметрам фильтрации.

Для отмены заданных правил фильтрации и отображения в дереве ОЗ всех записей необходимо нажать кнопку «Отменить».

5.1.2 Блок «Информация об ОЗ»

Блок с описанием ОЗ (рис. 21) содержит следующую информацию:

- название устройства;
- описание устройства;
- адрес устройства;
- доступ к объекту защиты. Является ссылкой. При переходе пользователь может посмотреть в какие группы входит ОЗ, кто из пользователей комплекса имеет доступ к ОЗ. При наличии особых привилегий пользователь может редактировать доступ у группы пользователей и у каждого пользователя индивидуально;
- расписания, назначенные ОЗ. При переходе по ссылке позволяет пользователю поменять статус использования расписания: вкл./выкл.;
- метки. Является ссылкой. При переходе позволяет пользователю создать собственные метки для фильтрации ОЗ в дереве;
- кнопка «Изменить» (Изменить). Позволяет пользователю перейти в окно редактирования ОЗ и внести требуемые изменения.

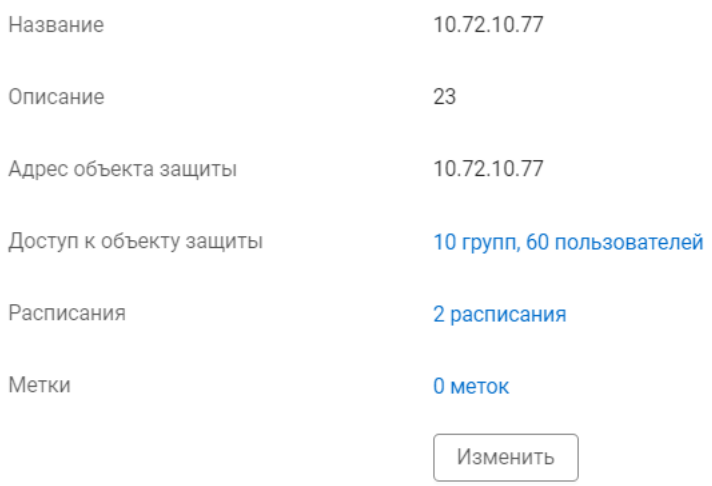


Рисунок 21 – Блок «Информация об ОЗ»

5.1.3 Блок «Возможности»

Блок «Возможности» содержит информацию о назначенных возможностях ОЗ (рис. 22). Назначить возможности ОЗ в данном блоке невозможно. При переходе по ссылке-названию устройства появляется доступ для просмотра и редактирования возможности.

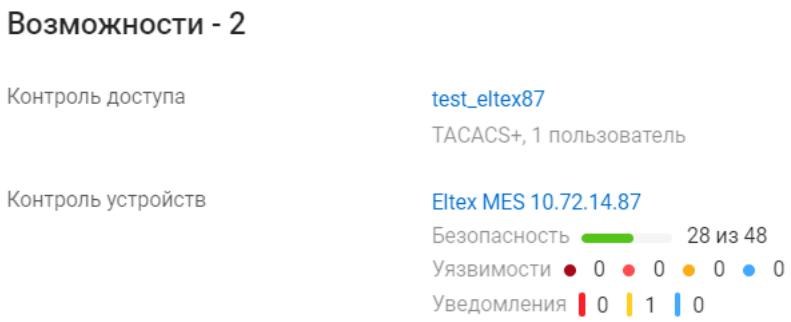


Рисунок 22 – Блок «Возможности»

5.2 База знаний

Отображаемые данные и доступная функциональность в подразделе «База знаний» зависит от наличия хотя бы одной лицензии на функциональные модули.

В ПК «Efros DO» в подразделе «База знаний» реализована возможность систематического сбора сведений об ОЗ (устройствах) на основе активного и пассивного сканирования. Для этого используется ряд протоколов и утилит. Полученные данные хранятся в БД комплекса в виде результатов обработки данных в структурированной форме и используются для решения задач ИБ (рис. 23).

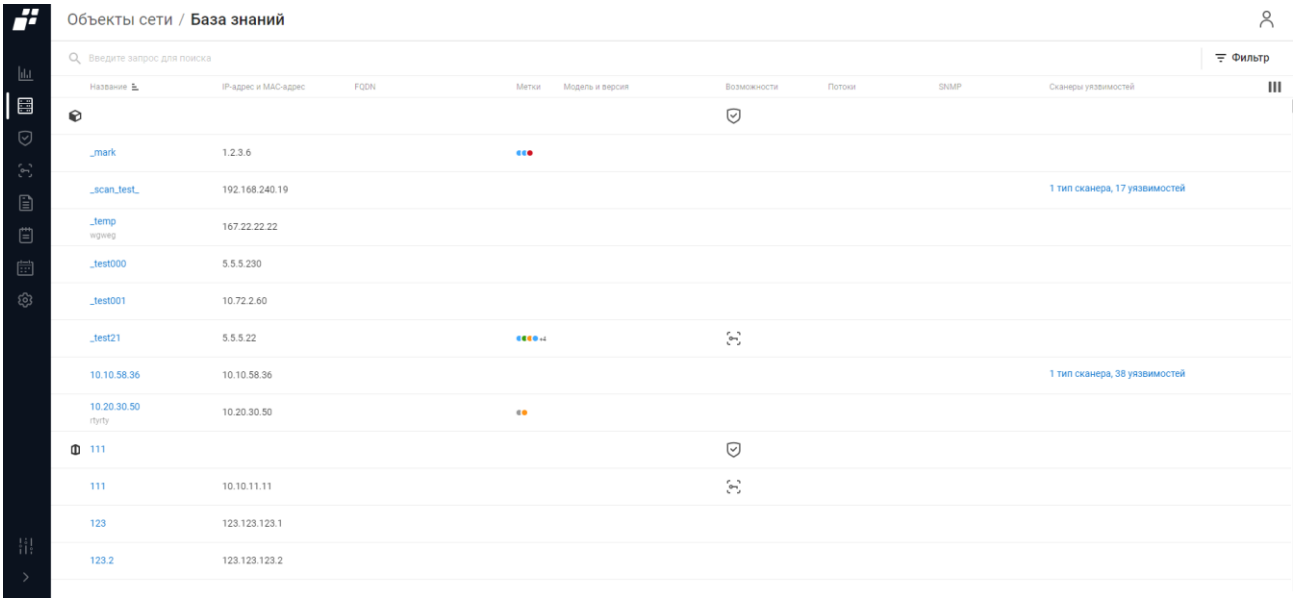


Рисунок 23 – Подраздел «База знаний»

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

- иконка производителя;
- название ОЗ;
- IP-адрес и MAC-адрес устройства. Является ссылкой. При переходе открывается окно редактирования объекта защиты (более подробно см. п.п. 5.1.1.6);
- доменное имя (FQDN);
- метки;
- модель и версия устройства (если она есть);
- назначенные возможности (более подробно см. п. 5.1.1);
- информация о потоках (данные, полученные в результате пассивного сканирования NetFlow). Является ссылкой. При переходе открывается окно с описанием зафиксированных потоков данных;

— информация, полученная через SNMP (данные, полученные в результате SNMP сканирования). Является ссылкой. При переходе открывается окно с результатами сканирования;
— сканеры уязвимостей. Является ссылкой. При переходе открывается окно со сканером уязвимостей и перечнем обнаруженных уязвимостей.

Над списком объектов сети располагаются:

— кнопка «Поиск» (Введите запрос для поиска) для поиска искомой записи в списке;
— кнопка «Фильтр» (Фильтр) для фильтрации списка объектов сети;
— кнопка «Колонки» ( ) для изменения отображения колонок на странице.

При наведении курсора на строку с ОЗ, в правой части строки появляется кнопка «Удалить» ( ) для удаления настройки.

5.2.1 Фильтрация в Базе знаний

Для фильтрации ОЗ в подразделе «База знаний» необходимо нажать кнопку «Фильтр» ( ). Откроется окно фильтрации, приведенное на рис. 24. Состав полей окна и правила их заполнения приведены в таблице 14.

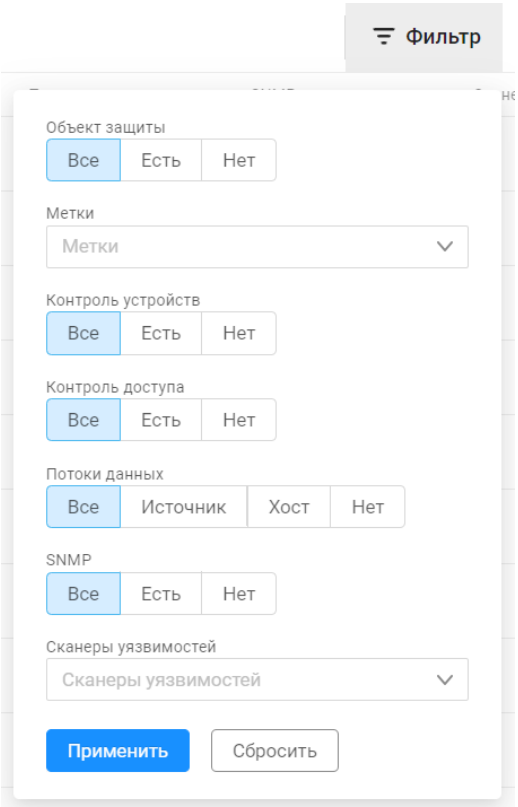


Рисунок 24 – Окно фильтрации списка ОЗ

Таблица 14 – Состав и описание полей окна фильтрации списка ОЗ

Поле	Описание
Поле «Объект защиты»	Поле с выбором типа ОЗ: — «Все»; — «Есть» (сконфигурирован); — «Нет» (не сконфигурирован)
Поле «Метки»	Раскрывающийся список меток, назначенных ОЗ пользователем
Поле «Контроль устройств»	Возможность «Контроль устройств» у ОЗ: — «Все»; — «Есть»; — «Нет»
Поле «Контроль доступа»	Возможность «Контроль доступа» у ОЗ: — «Все»; — «Есть»; — «Нет»
Поле «Потоки данных»	Возможность «Потоки данных» у ОЗ: — «Все»; — «Источник»; — «Хост»; — «Нет»
Поле «SNMP»	Проверка доступности по SNMP: — «Все»; — «Есть»; — «Нет»
Поле «Сканеры уязвимостей»	Раскрывающийся список для выбора сканера уязвимостей
Элементы управления	
Применить	При нажатии кнопки окно фильтрации закрывается, введенные настройки фильтрации применяются
Сбросить	При нажатии кнопки окно фильтрации закрывается без применения введенных настроек

Необходимо заполнить поля требуемыми параметрами. После чего в списке отобразятся ОЗ, соответствующие заданным параметрам фильтрации.

Для отмены заданных правил и отображения в списке ОЗ всех записей необходимо нажать кнопку «Отменить».

5.3 Конечные точки

Подраздел «Конечные точки» доступен пользователю для работы при наличии лицензии на функциональный модуль «Efros NAC».

В данном подразделе содержится список конечных точек (список клиентского оборудования), автоматически создаваемых при попытке получения доступа к сети с использованием протокола RADIUS и загружаемых в виде файла форматом CSV (подраздел «Импорт данных», более подробно см. подраздел 10.8). Кроме этого, пользователь может создавать собственные конечные точки/группы конечных точек, просматривать данные, полученные о конечных точках в результате профилирования, управлять аутентификацией устройств, подключаемых к сети по MAC-адресам (MAB).

Страница содержит отдельные вкладки списков конечных точек и групп конечных точек. По умолчанию активной является вкладка «Конечные точки» (рис. 25).

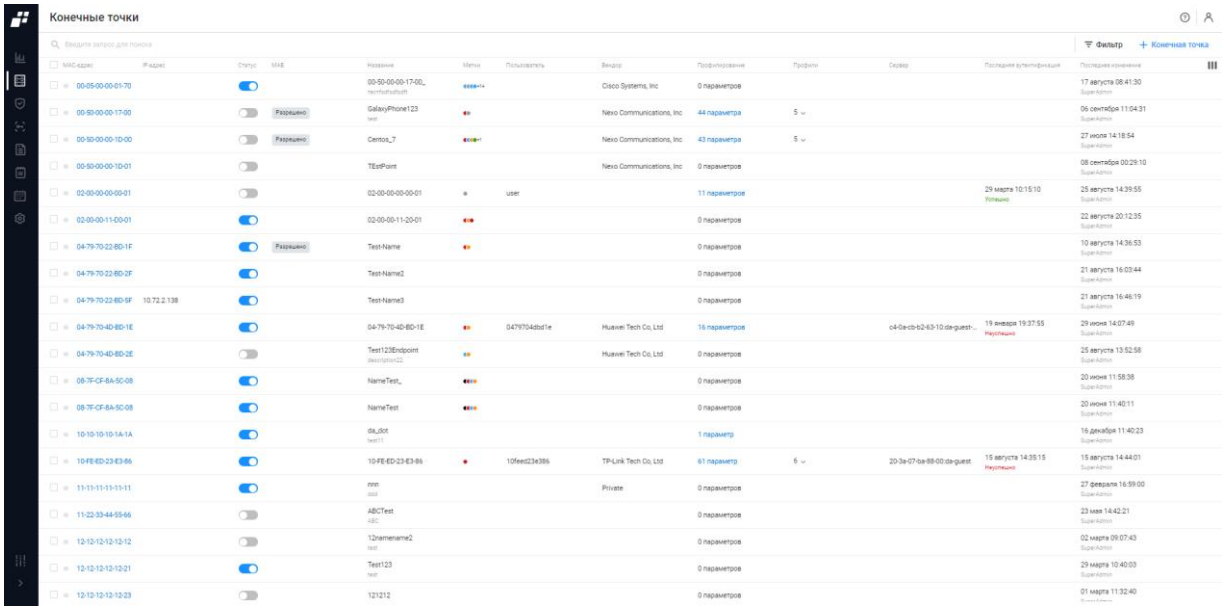


Рисунок 25 – Подраздел «Конечные точки»

Список конечных точек реализован в виде таблицы (см. рис. 25). Для каждой записи списка отображаются следующие данные:

- поле для флага – выбор конечной точки, чтобы создать копию, добавить в группу или удалить;
- MAC-адрес. Является ссылкой, при переходе открывается окно редактирования конечной точки;
- IP-адрес конечной точки;
- статус – показывает, подключена ли конечная точка к сети;

- MAB – отображает информацию: запрещена или разрешена аутентификация устройств, подключаемых к сети по MAC-адресам;
- название конечной точки;
- метки – это ключевые слова, которые используются для выделения объектов сети из общего списка, упрощения поиска объектов, объединения объектов в логические категории;
- пользователь – имя пользователя, содержащегося в запросе при попытке получения доступа к сети;
- вендор – производитель конечной точки согласно MAC-адресу;
- профилирование. Является ссылкой, при переходе открывается окно профиля конечной точки. Отображает динамически обновляемые данные о конечной точке, получаемые в процессе аутентификации/аудита с использованием протокола RADIUS;
- профили – перечень профилей, полученных в результате классификации конечных точек;
- сервер – MAC-адрес сетевого устройства, содержащийся в запросе при попытке получения доступа к сети (через разделитель может присутствовать имя беспроводной сети);
- дата, время и результат выполнения последней аутентификации;
- дата и время внесения последних изменений.

Профилирование — классификация конечных точек путем проверки значений атрибутов, отправляемых этими устройствами в сети. Профилирование устройств позволяет собирать информацию о производителе, типе устройства, операционной системе и пр.

Источники профилирования, поддерживаемые в комплексе:

- атрибуты, получаемые по протоколу RADIUS при взаимодействии конечной точки с комплексом;
- атрибуты, получаемые по протоколу DHCP при назначении IP-адреса конечной точке.

Для возможности получения данных атрибутов, необходимо настроить на оборудовании перенаправление трафика DHCP в комплекс путем использования dhcp-proxy. В случае использования оборудования производителя Cisco используется настройка ip helper-address.

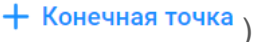
- атрибуты HTTP User-Agent, получаемые при открытии пользователем страницы

подключения к гостевому порталу.

Над списком с конечными точками располагаются:

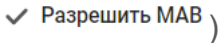
— поле поиска () для поиска искомой записи в списке;

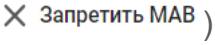
— кнопка «Фильтр» () для фильтрации списка конечных точек;

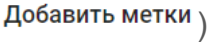
— кнопка «Конечная точка» () позволяет добавить новую конечную точку;

— кнопка «Колонки» () для изменения отображения колонок на странице.

При установке флага в строке с необходимой конечной точкой над списком появляются следующие кнопки:

— кнопка «Разрешить MAB» () разрешает аутентификацию устройств, подключаемых к сети по MAC-адресам;

— кнопка «Запретить MAB» () запрещает аутентификацию устройств, подключаемых к сети по MAC-адресам;

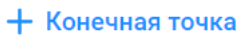
— кнопка «Добавить метки» () позволяет добавить пользовательские метки;

— кнопка «Удалить» () позволяет удалить выбранную конечную точку.

Кнопки «Создать копию» и «Удалить» также появляются в правой части экрана в строке с выбранной конечной точкой.

5.3.1 Добавление новой конечной точки вручную

Для ручного добавления в список новой конечной точки необходимо выполнить следующие действия:

1) Нажать на кнопку «Конечная точка» ().
2) Откроется страница «Создание конечной точки сети» (рис. 26). Страница состоит из следующих вкладок:

— «Основные» – вкладка активна по умолчанию;

— «Дополнительные атрибуты».

Состав и описание полей вкладки «Основные» приведены в таблице 15.

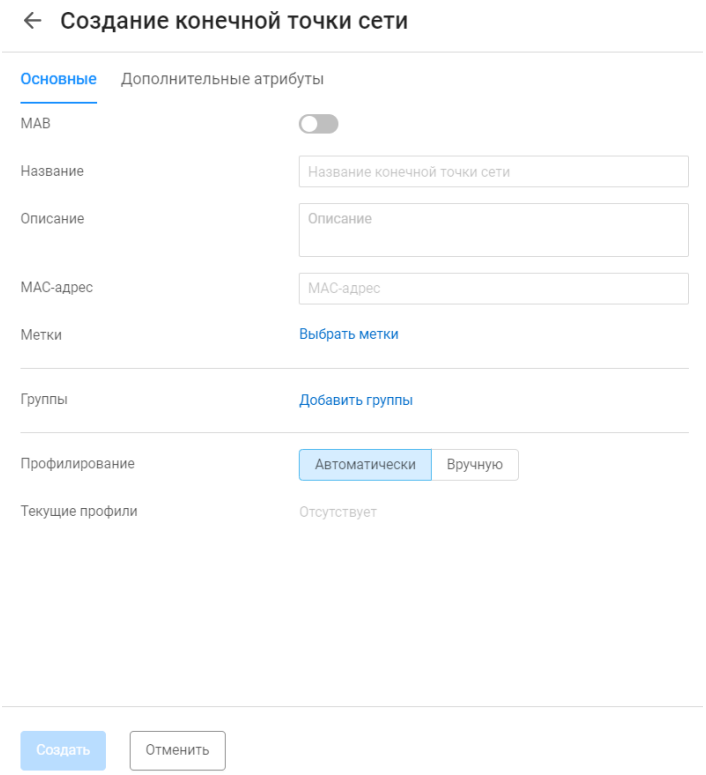


Рисунок 26 – Вкладка «Основные»

Таблица 15 – Состав и описание полей вкладки «Основные»

Поле	Описание
Поле «MAB»	Переключатель: — «Запретить MAB» ( ) – конечной точке запрещена аутентификация в сети по MAC-адресу; — «Разрешить MAB» ( ) – конечной точке разрешена аутентификация в сети по MAC-адресу. По умолчанию установлено положение «Запретить MAB»
Поле «Название»	Текстовое поле для ввода названия оборудования. Параметры ввода текста: от 1 до 50 символов. Допустимые символы: буквы латинского алфавита, цифры, «_», «–»
Поле «Описание»	Текстовое поле для ввода описания оборудования. Параметры ввода текста: от 1 до 250 любых символов
Поле «MAC-адрес»	Текстовое поле для ввода MAC-адреса конечной точки
Поле «Метки»	Параметр фильтрации, создаваемый пользователем. При нажатии на кнопку «Выбрать метки» появляется окно с метками, созданными пользователями комплекса. Метки разрешено создавать, редактировать и удалять
Поле «Группы»	По умолчанию поле содержит только кнопку «Добавить

Поле	Описание
	группы». При нажатии на кнопку «Добавить группы» открывается окно выбора групп, заведенных в ПК «Efros DO». Далее надо выбрать группу, в которую необходимо добавить конечную точку. После выбора группы необходимо нажать кнопку «Выбрать»
Поле «Профилирование»	Переключатель: — «Автоматически». При выборе автоматического профилирования профили конечной точки определяются и назначаются автоматически на основе атрибутов/значений, полученных от источников профилирования, в результате проверки правил политик профилирования. При получении новых атрибутов/значений от источников профилирования, профили конечной точки автоматически пересчитываются; — «Вручную». При выборе ручного профилирования профили конечной точки определяются и назначаются пользователем. Автоматическое профилирование конечной точки отключается, автоматически назначенные профили снимаются и не пересчитываются
Поле «Текущие профили»	Поле становится доступным для выбора профиля только после выбора в поле «Профилирование» положения «Вручную». Для выбора профиля необходимо нажать на ссылку «Выбрать профили» и из раскрывшегося списка выбрать требуемый профиль
Элементы управления	
Создать	При нажатии кнопки выполняется переход на страницу списка конечных точек с сохранением внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу списка конечных точек без сохранения внесенных данных

3) Заполнить поля вкладки «Основные» необходимыми параметрами.
4) На вкладке «Дополнительные атрибуты» отображается список источников профилирования и их параметров (атрибутов) в табличном виде. Данные на вкладке заполняются автоматически при выборе профиля и недоступны для редактирования (рис. 27).

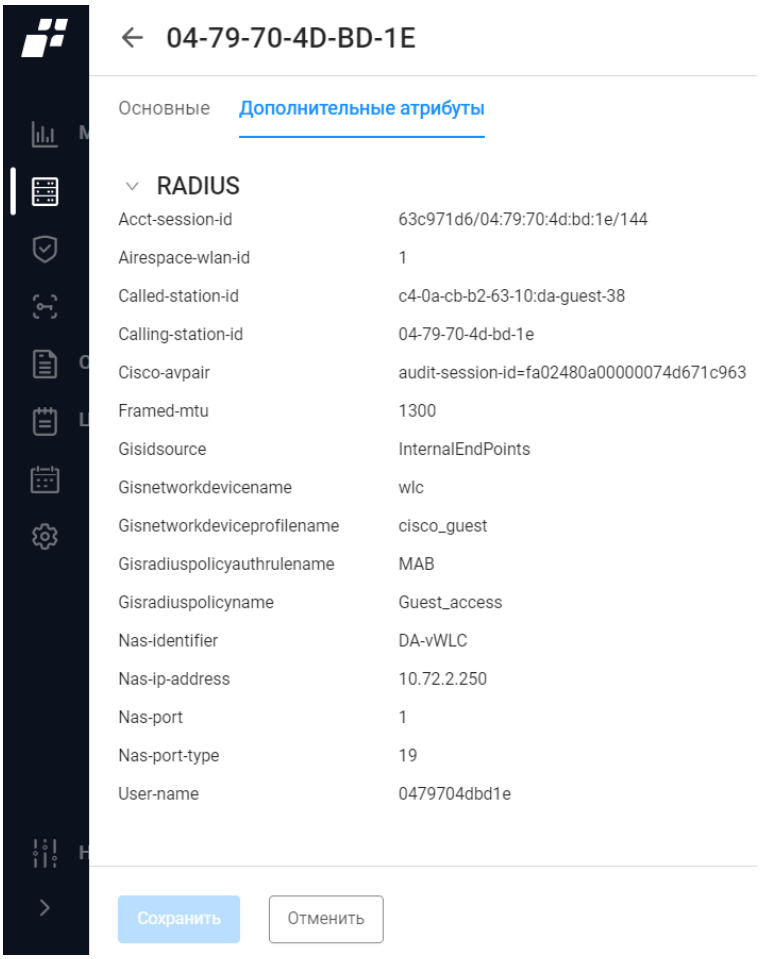


Рисунок 27 – Вкладка «Дополнительные атрибуты»

5) Нажать кнопку «Создать».

Автоматически запускается процесс проверки заполненности всех обязательных полей и уникальности добавляемой конечной точки 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 «Создать».

5.3.2 Фильтрация конечных точек

Для фильтрации в списке конечных точек необходимо нажать кнопку «Фильтр» (Фильтр). Откроется окно фильтрации (рис. 28). Состав полей окна и правила их заполнения приведены в таблице 16.

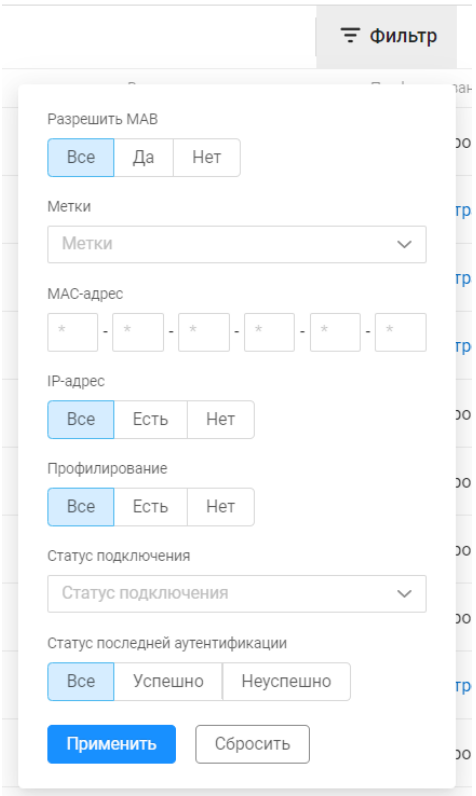


Рисунок 28 – Окно фильтрации списка конечных точек

Таблица 16 – Состав и описание полей окна фильтрации списка конечных точек

Поле	Описание
Поле «Разрешить MAB»	Переключатель: — «Все» – при выборе отображаются все конечные точки; — «Да» – при выборе отображаются конечные точки с разрешенным MAB; — «Нет» – при выборе отображаются конечные точки с запрещенным MAB
Поле «Метки»	Раскрывающийся список с пользовательскими метками, назначенными конечным точкам сети
Поле «MAC-адрес»	Поле из шести блоков для ввода MAC-адреса искомых конечных точек
Поле «IP-адрес»	Переключатель: — «Все» – при выборе отображаются все конечные точки; — «Да» – при выборе отображаются конечные точки с IP-адресом; — «Нет» – при выборе отображаются конечные точки без IP-адреса
Поле «Профилирование»	Переключатель: — «Все» – при выборе отображаются все конечные точки;

Поле	Описание
	— «Да» – при выборе отображаются конечные точки с профилированием; — «Нет» – при выборе отображаются конечные точки без профилирования
Поле «Статус подключения»	Раскрывающийся список: — «Активно»; — «Неактивно»; — «Нет информации»
Поле «Статус последней аутентификации»	Переключатель: — «Все» – при выборе отображаются все конечные точки; — «Успешно» – при выборе отображаются конечные точки, прошедшие процедуру аутентификации без ошибок; — «Неуспешно» – при выборе отображаются конечные точки, для которых процедура прохождения аутентификации завершилась с ошибкой
Элементы управления	
Сбросить	При нажатии кнопки окно фильтрации закрывается без применения введенных настроек
Применить	При нажатии кнопки окно фильтрации закрывается, введенные настройки фильтрации применяются

Далее необходимо заполнить поля. После чего окно фильтрации закроется, на странице отобразятся конечные точки, соответствующие заданным параметрам фильтрации.

Для отмены заданных правил фильтрации и отображения на странице всех записей необходимо нажать кнопку «Отменить».

5.4 Карта сети

Отображаемые данные и доступная функциональность в подразделе «Карта сети» зависят от наличия хотя бы одной лицензии на функциональный модуль.

Данный подраздел представляет собой визуализацию актуального состояния сети в виде графического представления физической и логической топологии соединений ОЗ (сконфигурированных и несконфигурированных) и подсетей. Карта сети является инструментом для диагностики поведения и прогнозирования поведения сети (рис. 29).

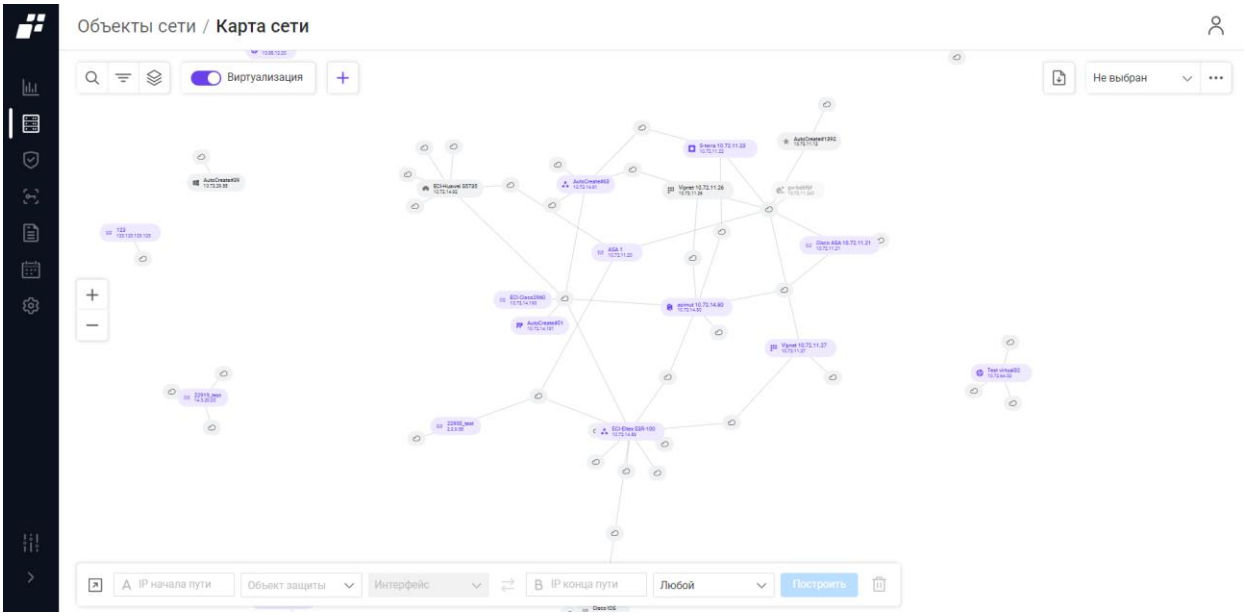


Рисунок 29 – Подраздел «Карта сети»

На странице отображаются ОЗ и их связи. Дополнительно на карте сети отображается следующие данные:

- наименование;
- IP-адрес;
- иконка производителя.

При наведении курсора на выбранный физический ОЗ (ОЗ выделен серым цветом) появляется окно со следующей информацией (рис. 30):

- статус ОЗ:
  - доступен « » – последняя операция с устройством выполнена успешно;
  - недоступен « » – при выполнении операции с ОЗ (загрузка отчетов, проверка связи) произошла ошибка аутентификации;
  - нет связи « » – последняя операция с ОЗ (загрузка отчетов, проверка связи) завершилась ошибкой.
- иконка производителя;

— название и IP-адрес ОЗ;
— уровень безопасности;
— количество и тип уязвимостей;
— модель, версия, если есть у ОЗ;
— время последнего обновления;
— протоколы TACACS+/RADIUS;
— кнопки «Начало пути», «Подробнее», «Обновить ( )».

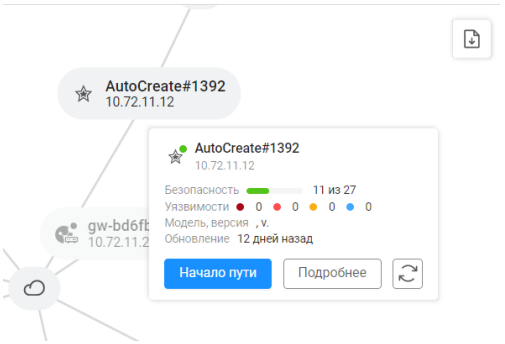
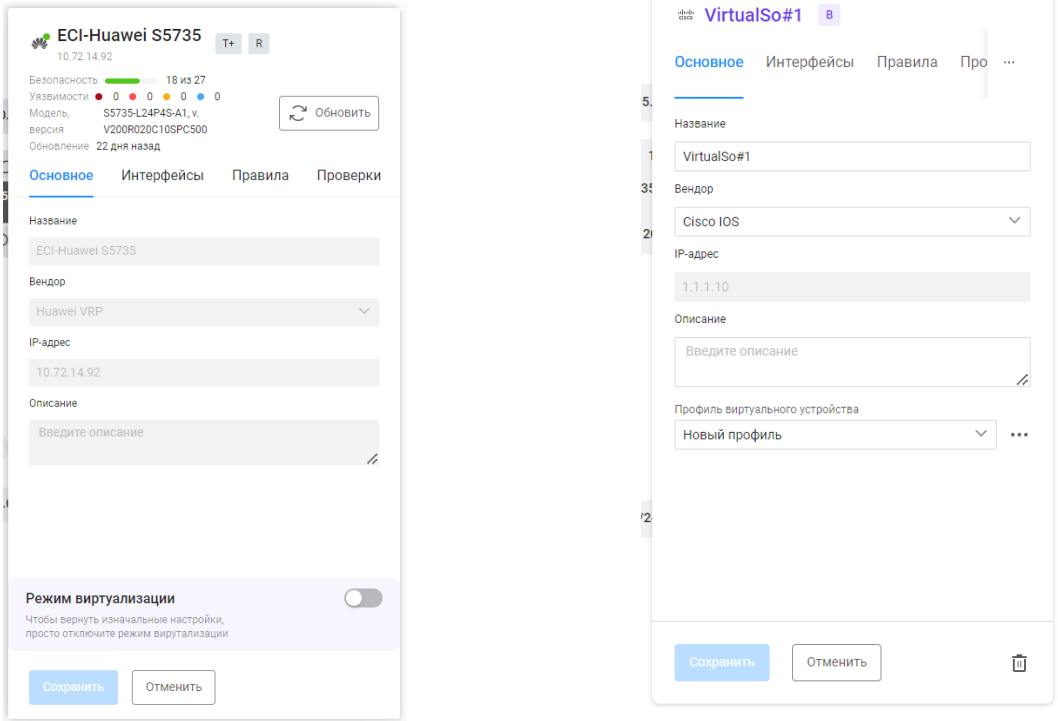


Рисунок 30 – Окно карточки физического ОЗ

При выделении ОЗ (как физического, так и виртуального) и нажатии кнопки «Подробнее», открывается окно со следующей информацией об ОЗ (рис. 31).



а) б)

Рисунок 31 – Окно карточки ОЗ из карты сети:

а) физический ОЗ; б) виртуальный ОЗ

Таблица 17 – Состав и описание полей окна физического ОЗ

Поле	Описание
Поле с описанием ОЗ	Содержит следующую информацию для физического ОЗ: — иконка вендора; — статус; — название ОЗ; — IP-адрес; — протоколы TACACS+/RADIUS; — уровень безопасности; — количество уязвимостей; — модель; — версия; — время последнего обновления
Вкладка «Основное»	
Поле «Название»*	Название ОЗ
Поле «Вендор»*	Поле с раскрывающимся списком установленных внешних модулей в комплексе (более подробно описано в подразделе 9.4)
Поле «IP-адрес»*	IP-адрес ОЗ
Поле «Описание»*	Краткое описание ОЗ
Вкладка «Интерфейсы»	Содержит список интерфейсов в табличной форме
	Содержит поле поиска
Вкладка «Правила»	Содержит список правил МЭ
	Содержит список правил маршрутизации
	Содержит поле поиска
Вкладка «Проверки»	Содержит следующие данные: — «Зонный анализ»; — «Оптимизация правил»
Элементы управления	
Обновить	Позволяет обновить информацию об ОЗ, которая представлена на карточке
Режим виртуализации	Переключатель в режим виртуализации. При наличии у ОЗ виртуального объекта, подгружается вся информация из первого доступного профиля виртуального объекта
Отменить	По нажатию кнопки окно физического устройства закрывается без применения введенных данных
Сохранить	По нажатию кнопки окно физического устройства закрывается, внесенные изменения сохраняются
*Поле недоступно для редактирования	

Таблица 18 – Состав и описание полей окна виртуального ОЗ

Поле	Описание
Поле с описанием ОЗ	Содержит следующую информацию: — иконка вендора; — название ОЗ; — IP-адрес ОЗ; — значок виртуального объекта
Вкладка «Основное»	
Поле «Название»	Название ОЗ
Поле «Вендор»	Производитель ОЗ Поле доступно только при создании виртуального объекта
Поле «IP-адрес»	IP-адрес ОЗ Поле доступно только при создании виртуального объекта
Поле «Описание»	Краткое описание ОЗ
Поле «Профиль виртуального устройства»	Раскрывающийся список профилей, каждый из которых содержит список параметров конкретного виртуального устройства. Поле появляется только при редактировании виртуального объекта
Кнопка «Режим виртуализации»	Отключение режима виртуализации и возвращение к изначальным настройкам ОЗ
Вкладка «Интерфейсы»	Содержит список интерфейсов
	Содержит поле поиска
	Содержит кнопки редактирования «✎» и удаления «🗑» интерфейсов
Вкладка «Правила»	Содержит список правил МЭ
	Содержит список правил маршрутизации
	Содержит поле поиска
	Содержит кнопки редактирования «✎» и удаления «🗑» правил
	Содержит кнопку «Добавить» при отсутствии правил
Вкладка «Проверки»	Содержит следующие данные: — «Зонный анализ»; — «Оптимизация правил»

Поле	Описание
Элементы управления	
Сохранить	При нажатии кнопки окно физического ОЗ закрывается, изменения сохраняются
Отменить	При нажатии кнопки окно физического ОЗ закрывается без изменений
Все вкладки, кроме поля с IP-адресом, доступны для редактирования	

На странице карты сети располагаются:

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

— кнопка «Фильтр» ( ) для фильтрации списка ОЗ;

— кнопка «Слои» ( ) – позволяет пользователю скрыть/отобразить такие атрибуты ОЗ и подсетей, как:

- «Вендор»;
- «Название»;
- «IP-адрес»;
- «VPN-туннели»;
- «Адрес подсети»;
- «Нетранзитные сети».

— кнопка экспорта « » для сохранения всей карты сети или ее части в необходимом формате;

— поле для выбора профиля карты сети (Не выбран). Позволяет выбрать сохраненные ранее профили карты сети;

— кнопка «Контекстное меню» ( ) рядом с полем для выбора профиля – для перехода в окно сохранения/удаления/изменения текущего профиля (рис. 32).

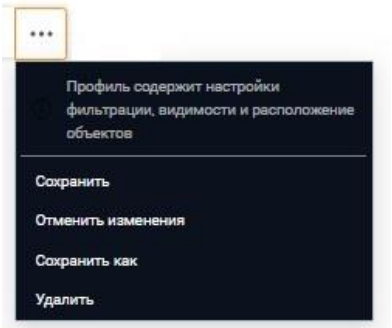


Рисунок 32 – Контекстное меню

— кнопка активации режима виртуализации. Позволяет показать скрытые

виртуальные ОЗ;

— кнопка « + » для создания виртуального объекта (отображается при активации режима виртуализации);
— кнопки изменения масштаба карты сети;
— панель построения маршрута для проверки прохождения трафика между устройствами.

5.4.1 Добавление виртуального ОЗ

Для добавления виртуального ОЗ необходимо выполнить следующие действия:

1) Включить режим «Виртуализация» на карте сети.
2) Нажать кнопку «Создать виртуальный объект» (+).
3) Откроется окно «Создание виртуального объекта», приведенное на рис. 34. Окно состоит из следующих вкладок:

— «Основное» - вкладка активна по умолчанию;
— «Интерфейсы»;
— «Правила»;
— «Проверки».

Состав и описание полей вкладки «Основное» приведены в таблице 19.

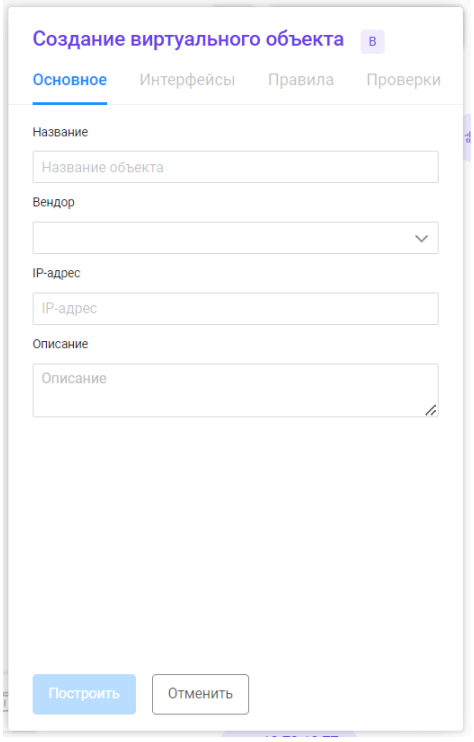


Рисунок 33 – Контекстное меню

Таблица 19 – Состав и описание полей вкладки «Основное»

Поле	Описание
Поле «Название»	Текстовое поле для ввода названия виртуального ОЗ. Параметры ввода текста: от 1 до 50 любых символов
Поле «Вендор»	Текстовое поле для ввода описания оборудования. Параметры ввода текста: от 1 до 250 любых символов
Поле «IP-адрес»	Поле для ввода IP-адреса виртуального объекта. При заполнении становятся доступны вкладки «Интерфейсы» и «Правила». Вкладка «Проверки» становится доступна после создания правил на вкладке «Правила». Параметры для ввода текста: от 1 до 50 символов, формат от 0.0.0.0 до 255.255.255.255, кроме 0.0.0.0 и 255.255.255.255
Поле «Описание»	Текстовое поле для ввода описания виртуального ОЗ. Параметры ввода текста: от 1 до 500 любых символов
Элементы управления	
Построить	При нажатии кнопки выполняется переход на страницу карты сети с сохранением внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу карты сети без сохранения внесенных данных

4) Заполнить поля вкладки «Основное» необходимыми параметрами. При создании нового виртуального объекта создается новый профиль устройства (профиль конфигураций). При создании виртуального объекта на основе физического устройства профиль виртуального объекта совпадает с профилем физического устройства.
5) Перейти на вкладку «Интерфейсы» (рис. 34). При создании нового виртуального объекта вкладка пустая. На вкладке отображается надпись: «Нет интерфейсов. Вам необходимо добавить хотя бы один» и кнопка «Добавить».

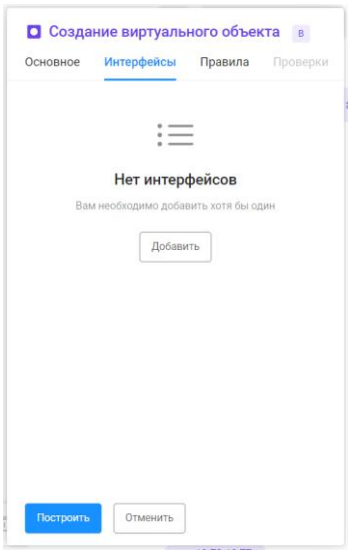


Рисунок 34 – Вкладка «Интерфейсы»

6) Нажать на кнопку «Добавить». Откроется окно «Создание интерфейса». Необходимо заполнить требуемые поля и нажать кнопку «Создать». Созданный интерфейс отобразится на вкладке «Интерфейсы».
7) Перейти на вкладку «Правила» (рис. 35). При создании нового виртуального объекта вкладка пустая. На вкладке отображаются следующие надписи:

— «Нет правил межсетевых экранов. Вам необходимо добавить хотя бы один набор» и кнопка «Добавить»;
— «Нет правил маршрутизации. Вам необходимо добавить хотя бы одно правило» и кнопка «Добавить».

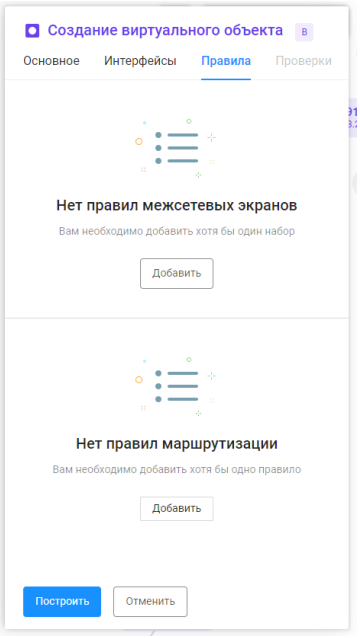


Рисунок 35 – Вкладка «Правила»

8) Нажать на кнопку «Добавить», добавить необходимые правила МЭ и правила маршрутизации.
9) Перейти на вкладку «Проверки» (рис. 36). На вкладке отображаются проверки МЭ: «Зонный анализ» и «Оптимизация правил». При переходе по ссылке «Зонный анализ» пользователь должен перейти в подраздел «Проверки МЭ», вкладка «Зонный анализ» и создать соответствующую проверку. Проверки «Оптимизация правил» срабатывают автоматически, как только назначаются на вкладке «Зонный анализ».

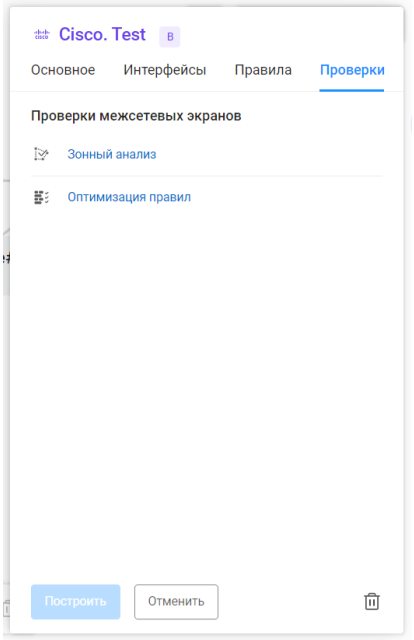


Рисунок 36 – Вкладка «Проверки»

10) Нажать кнопку «Построить». Созданный виртуальный ОЗ отобразится на карте сети.

Автоматически запускается процесс проверки заполненности всех обязательных полей и уникальности добавляемого виртуального объекта.

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

5.4.2 Построение маршрута в подразделе «Карта сети»

Построенный маршрут позволяет пользователю смоделировать прохождение трафика в сетевой структуре и произвести соответствующие настройки того или иного устройства.

Существует несколько способов построения маршрута.

Способ 1:

1) Нажать на кнопку « » в нижнем левом углу карты сети.

2) Откроется окно «Построение маршрута» (рис. 37). Состав и описание полей окна приведены в таблице 20.

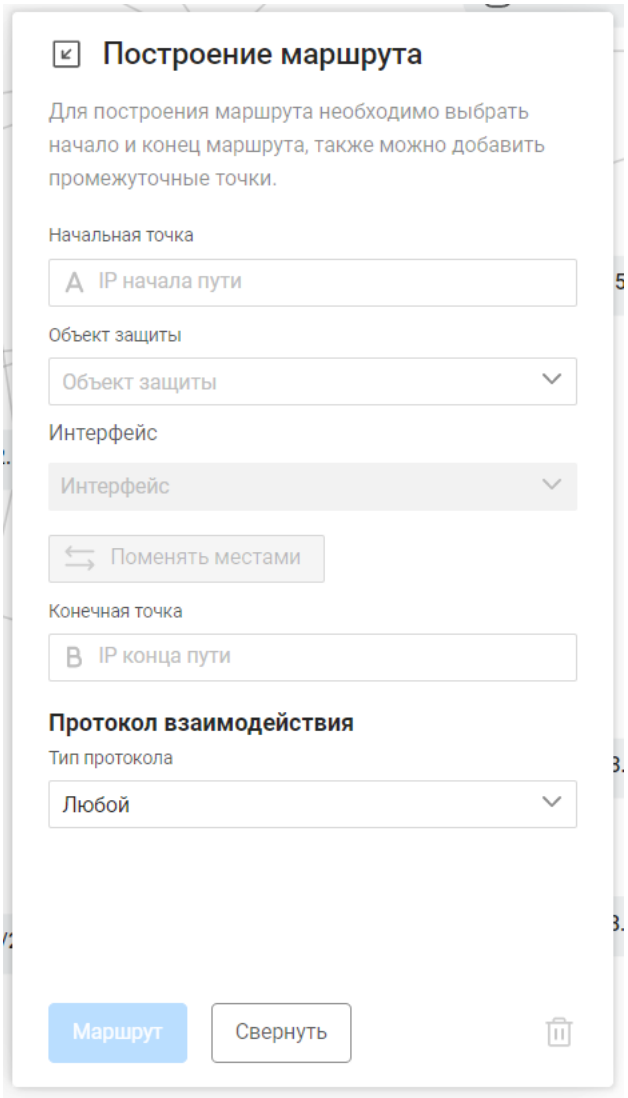


Рисунок 37 – Окно «Построение маршрута»

Таблица 20 – Состав и описание полей окна «Построение маршрута»

Поле	Описание
Поле «Начальная точка»	Поле для введения IP-адреса необходимого ОЗ
Поле «Объект защиты»	Раскрывающийся список всех ОЗ в комплексе
Поле «Интерфейс»	Заполняется автоматически после выбора ОЗ
Поле «Конечная точка»	Поле для введения IP-адреса
Группа полей «Протокол взаимодействия»	
Поле «Тип	Поле выбора протокола из списка:

Поле	Описание
протокола»	— «Любой»; — «TCP»; — «UDP»; — «TCP/UDP»; — «ICMP»; — «Другой»
Элементы управления	
Маршрут	При нажатии на кнопку окно фильтрации закрывается, введенные настройки фильтрации применяются
Свернуть	При нажатии на кнопку вертикальная форма маршрута меняется на горизонтальную, при этом поля остаются заполненными
Иконка «Удалить»	При нажатии на иконку очищаются все поля, при этом форма остается открытой
Поменять местами	Позволяет поменять местами выбранные ОЗ для построения маршрута. Кнопка становится активной после заполнения полей «Начальная точка», «Конечная точка»

3) Заполнить поля вкладки соответствующими параметрами.
4) Нажать кнопку «Маршрут». После чего будет построен маршрут в окне «Построение маршрута» (рис. 38).

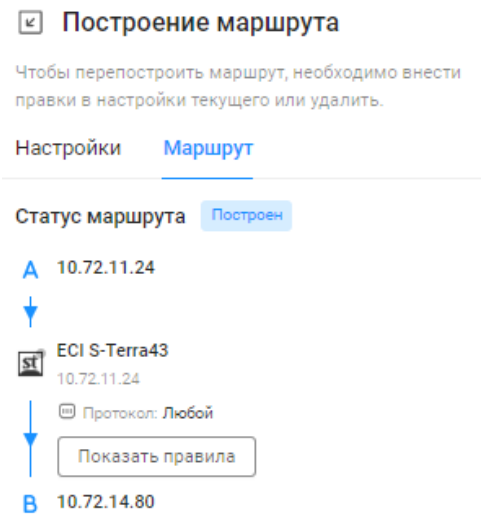


Рисунок 38 – Окно «Построение маршрута»

Поля вкладки «Настройки» соответствуют полям при построении маршрута.

Способ 2:

1) Заполнить параметры в поле «Маршрут» непосредственно на карте сети

(рис. 39). Состав и описание полей поля приведены в таблице 21.

Рисунок 39 – Поле «Маршрут»

Таблица 21 – Состав и описание полей поля «Маршрут»

Поле	Описание
Группа полей «A»	
Поле «IP начала пути»	IP-адрес ОЗ, который является начальной точкой маршрута
Поле «Объект защиты»	Поле представляет собой раскрывающийся список всех ОЗ в комплексе
Поле «Интерфейс»	Заполняется автоматически при выборе ОЗ
Группа полей «B»	
Поле «IP конца пути»	IP-адрес ОЗ, который является конечной точкой маршрута
Поле «Протокол»	Поле с раскрывающимся списком протоколов

Способ 3:

1) Навести курсор на необходимый ОЗ.
2) Нажать кнопку «Начало пути».
3) Навести курсор на второй ОЗ.
4) Нажать кнопку «Конец пути». Маршрут построен.

5.4.2.1 Статусы при неуспешном построении маршрута

Статусы при неуспешном построении маршрута:

- «Устройство не найдено» – неправильно настроена таблица маршрутизации на устройстве. Пользователю необходимо перенастроить устройство;
- «Блокировка правилами фильтрации» – маршрут заблокирован правилами ACL (информационное сообщение);
- «Маршрут зациклен» – маршрут построен через одно устройство дважды. Пользователю необходимо проверить параметры начальной и конечной точек маршрута (интерфейсы, правила и проверки);
- «Маршрутизация отсутствует» – таблица маршрутизации на устройстве пуста/не заполнены некоторые строки таблицы. Пользователю необходимо проверить таблицу маршрутизации на устройстве;
- «Маршрут прерван» – не удалось построить маршрут. Отсутствуют промежуточные объекты сети для построения маршрута. Пользователю

необходимо откорректировать параметры начальной и конечной точек маршрута;

— «Маршрут блокирован правилами маршрутизации» – пользователю необходимо проверить правила маршрутизации. Если устройство физическое – откорректировать маршруты на устройстве. Если устройство виртуальное, то пользователь может откорректировать правила непосредственно на карте сети.

5.4.3 Фильтрация на карте сети

Для фильтрации ОЗ необходимо нажать кнопку «Фильтр» ( ). Откроется окно фильтрации (рис. 40).

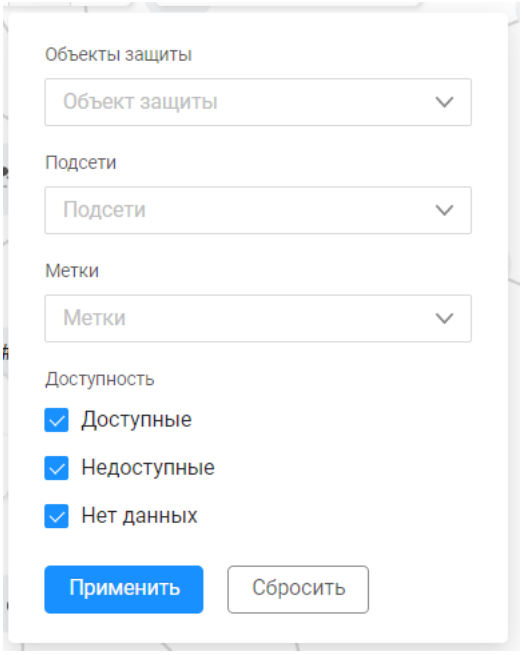


Рисунок 40 – Окно фильтрации ОЗ на карте сети

Состав и описание полей окна приведены в таблице 22.

Таблица 22 – Состав и описание полей окна фильтрации подраздела «Карта сети»

Поле	Описание
Поле «Объекты защиты»	Раскрывающийся список с ОЗ. Если режим виртуализации для карты сети выключен, то отображаются физические ОЗ. Если режим виртуализации для карты сети включен, то отображаются следующие ОЗ: — физические ОЗ, для которых нет связанных виртуальных объектов; — виртуальные ОЗ, связанные с физическими ОЗ; — виртуальные ОЗ, несвязанные с физическими ОЗ

Поле	Описание
Поле «Подсети»	Раскрывающийся список со всеми подсетями
Поле «Метки»	Раскрывающийся список с метками текущего пользователя
Поле «Доступность»	Поле с выбором статуса ОЗ в комплексе: — «Доступные»; — «Недоступные»; — «Нет данных»
Элементы управления	
Применить	При нажатии кнопки окно фильтрации закрывается, введенные настройки фильтрации применяются
Сбросить	При нажатии кнопки окно фильтрации закрывается без применения введенных настроек

Далее необходимо заполнить поля. После чего окно фильтрации закроется, на странице отобразятся данные, соответствующие заданным параметрам фильтрации.

Для отмены заданных правил фильтрации и отображения на странице всех данных необходимо нажать кнопку «Отменить».

5.5 Векторы атак

Вектор атаки – это последовательность определенных действий или средство для получения неавторизованного доступа к защищённой информационной системе или сети.

Построение векторов атак в комплексе позволяет показать возможные варианты использования уязвимостей, обнаруженных на устройствах сети (рис. 41).

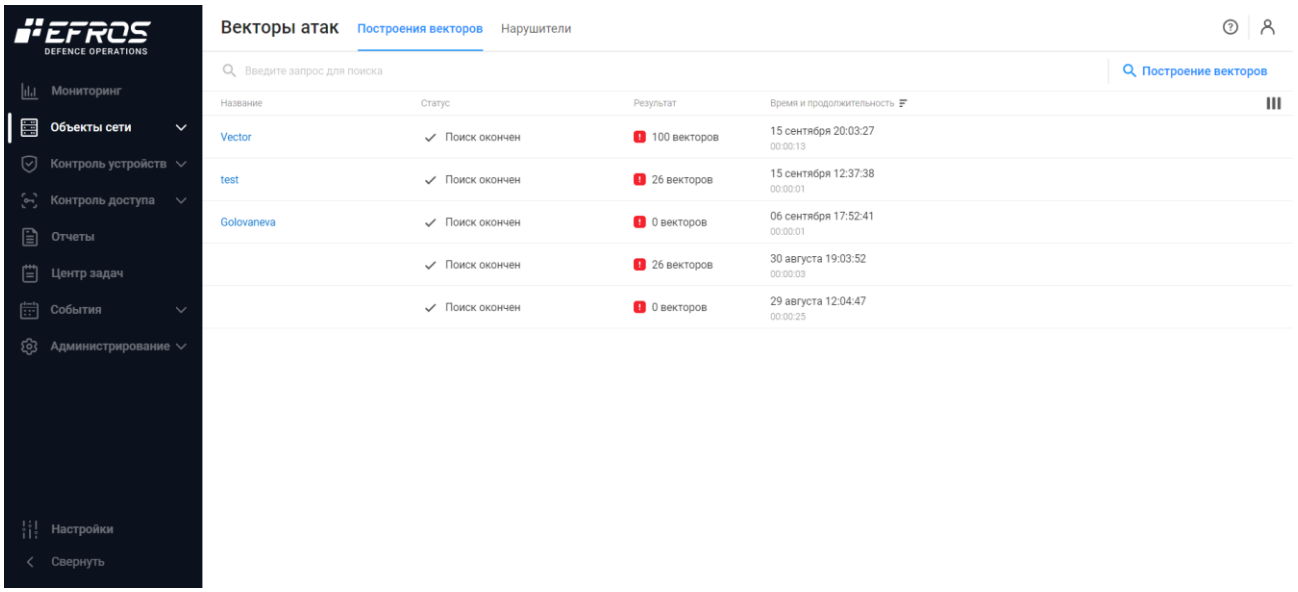


Рисунок 41 – Подраздел «Векторы атак»

Построение векторов атак осуществляется на основе следующих данных:

- средств защиты;
- топологии сети;
- объектов защиты;
- анализа уязвимостей и источников угроз.

В подразделе доступны следующие функции:

- задание параметров сканирования для построения векторов атак;
- расчет векторов атак в контексте сети;
- формирование и отображение списка найденных векторов по заданным параметрам;
- визуализация выбранного вектора атаки на карте сети.

После установки ПК «Efros DO» список векторов атак пуст, на странице отображается сообщение «*Список пуст. Вы можете выполнить новый поиск векторов*» и кнопка «*Построить вектора*» для перехода на страницу создания нового вектора атак.

Подраздел содержит следующие вкладки:

— «Построения векторов»;
— «Нарушители».

5.5.1 Вкладка «Построения векторов»

На вкладке отображаются построенные вектора атак (см. рис. 41). Список векторов атак реализован в виде таблицы. Для каждой записи таблицы отображаются следующие данные:

— название вектора;
— статус (поиск окончен/поиск ведется);
— результат построения векторов атак в виде количества найденных векторов атак;
— время и продолжительность построения.

Над списком заявок располагаются:

— поле поиска (Введите запрос для поиска) для поиска искомой записи в списке;
— кнопка «Построение векторов» (Построение векторов);
— кнопка «Колонки» ( ) для изменения отображения колонок на странице.

При выборе строки с необходимым вектором в правом углу строки появляются следующие кнопки:

— кнопка «Удалить» ( ) для удаления вектора атак;
— кнопка «Настройки» ( ) для настройки вектора атак.

5.5.1.1 Построение вектора атак

Для создания нового вектора атак необходимо выполнить следующие действия:

1) Нажать на кнопку в центре страницы «Построить вектора» (Построение векторов) или на кнопку «Построение векторов» (Построение векторов).
2) Откроется окно «Построение векторов атак» (рис. 42). Состав и описание полей страницы приведено в таблице 23.

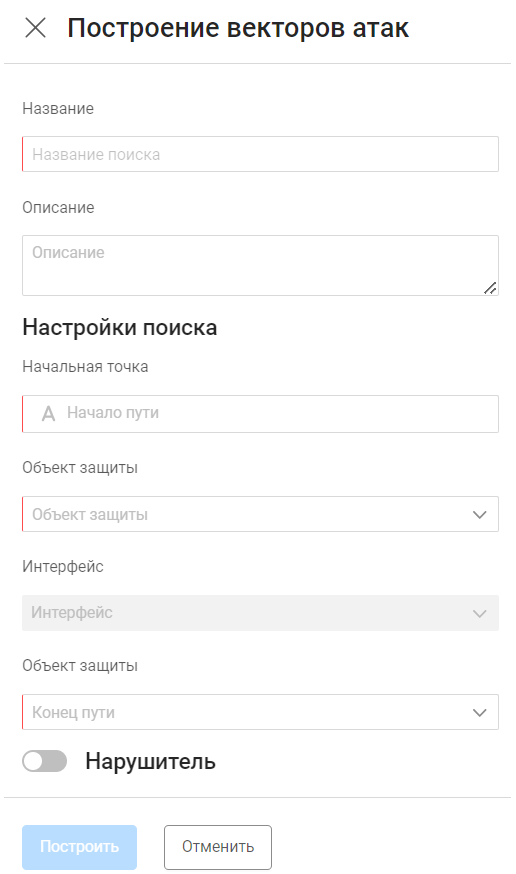


Рисунок 42 – Окно «Построение векторов атак»

Таблица 23 – Состав и описание полей окна «Построение векторов атак»

Поле	Описание
Поле «Название»	Текстовое поле для ввода названия вектора атаки. Параметры ввода текста: от 1 до 200 символов. Допустимые символы: буквы латинского алфавита, цифры, «_», «–»
Поле «Описание»	Текстовое поле для ввода описания вектора атаки. Параметры ввода текста: от 1 до 4000 любых символов
Группа полей «Настройки поиска»	
Поле «Начальная точка»	IP-адрес начала пути
Поле «Объект защиты»	Раскрывающийся список ОЗ
Поле «Интерфейс»	Раскрывающийся список интерфейсов. Зависит от выбранного ОЗ в поле «Объекты защиты». Поле становится активным только после выбора ОЗ в поле «Объекты защиты»
Поле «Объект защиты» (конечная	Раскрывающийся список ОЗ

Поле	Описание
точка)	
Группа полей «нарушитель»	
Кнопка «Нарушитель»	Переключатель. При активации появляются дополнительные поля
Поле «Нарушитель»	Раскрывающийся список нарушителей (более подробно см. п. 5.5.2)
Поле «Доступ»	Переключатель: — «Полный»; — «Отсутствует». При выборе переключателя «Полный» появляется дополнительное поле «Доступные объекты защиты»
Поле «Доступные объекты защиты»	Раскрывающийся список объектов защиты
Элементы управления	
Построить	При нажатии кнопки выполняется построение вектора атак
Отменить	При нажатии кнопки выполняется переход на страницу без сохранения внесенных данных

3) Заполнить поля окна необходимыми параметрами.
4) Нажать кнопку «Построить». Результат построения представлен на рис. 42.

5.5.1.2 Редактирование построенного вектора атак

Для редактирования построенного вектора атак необходимо выполнить следующие действия:

1) В списке построенных векторов атак выделить необходимый и перейти по ссылке на страницу редактирования (рис. 43)

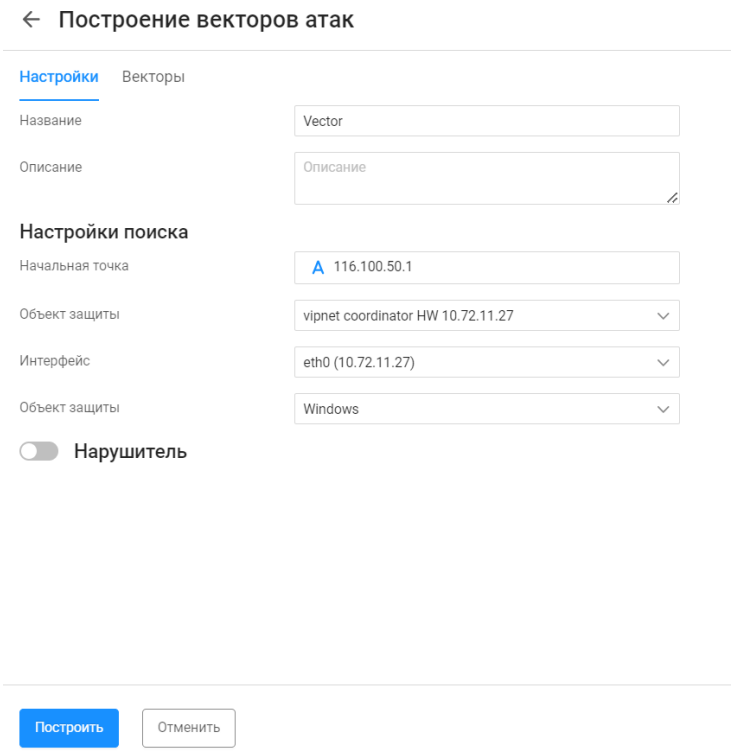


Рисунок 43 – Окно редактирования вектора

Окно состоит следующих вкладок:

- «Настройки»;
- «Векторы».

2) На вкладке «Настройки» выполнить изменение параметров построения.
3) Нажать кнопку «Построить». Автоматически запустится процесс построения нового вектора атак.

Вкладка «Векторы» содержит список построенных векторов атак в виде табличного списка (рис. 44) .

5.5.1.3 Визуализация вектора атак на карте сети

Для просмотра визуализации вектора атак на карте сети необходимо выполнить следующие действия:

1) Выбрать вектор атак на странице со списком векторов.
2) Откроется окно «Построение векторов атак».
3) Перейти на вкладку «Векторы» (см. рис. 44).

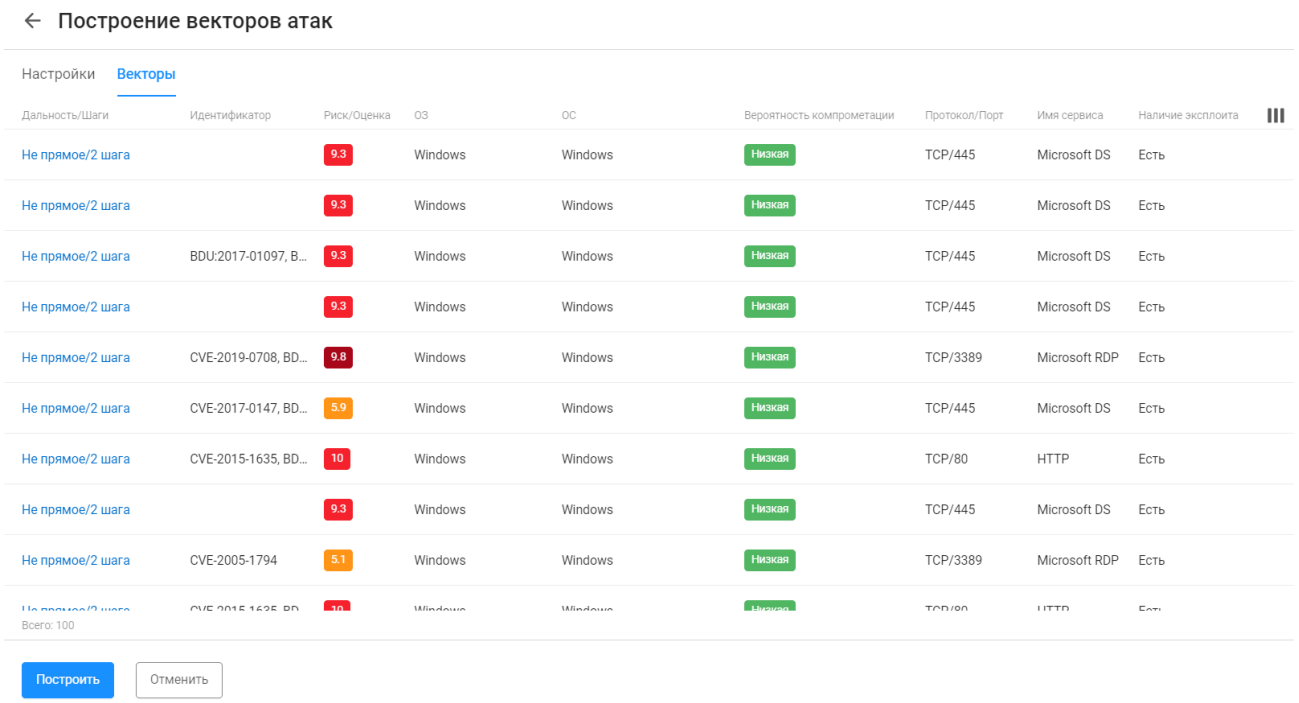


Рисунок 44 – Вкладка «Векторы»

Список векторов атак реализован в виде таблицы. Для каждой записи таблицы отображаются данные:

- дальность/шаги;
- идентификатор;
- риск/оценка;
- ОЗ;
- ОС;
- вероятность компрометации;
- протокол/порт;
- имя сервиса;
- наличие эксплоита.

4) Нажать на ссылку-дальность/шаги. Откроется страница с визуальным отображением вектора атак на карте сети (рис. 45)

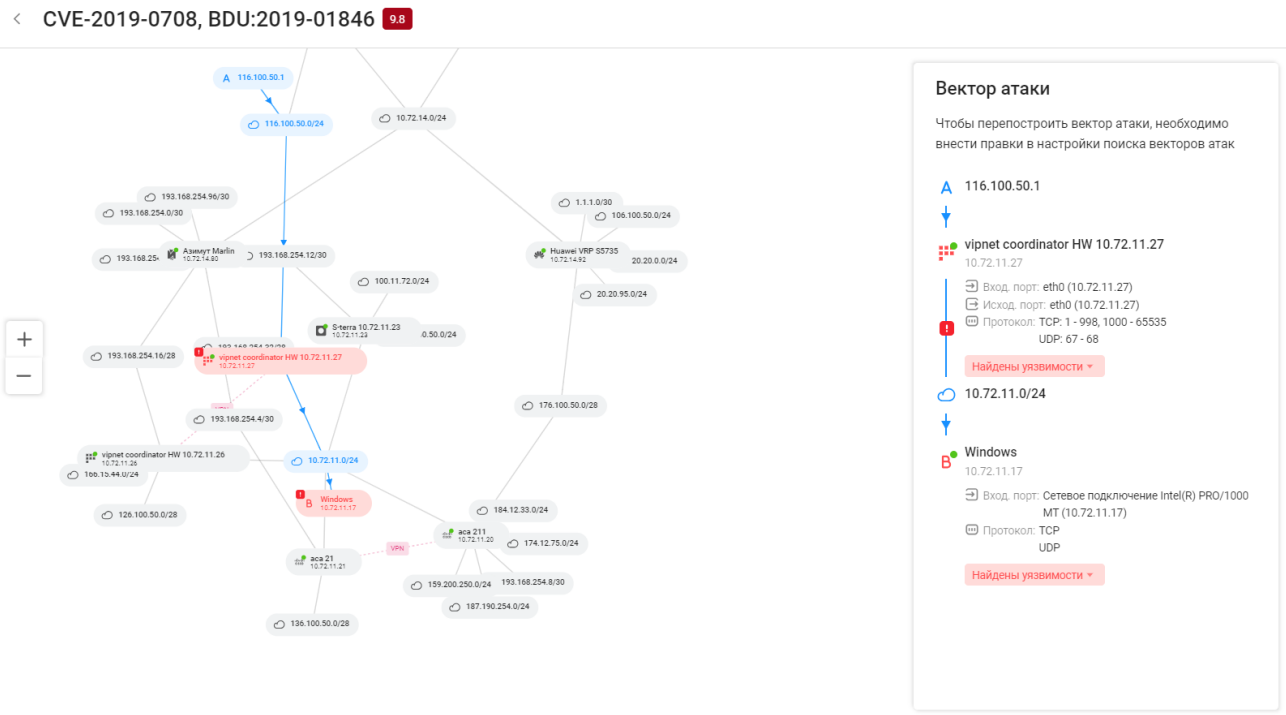


Рисунок 45 – Визуализация вектора атак на карте сети

На странице содержатся следующие данные:

- ОЗ, подсети и их связи;
- вертикальное представление прохождения вектора атаки от точки А до точки В;
- обнаруженные уязвимости.

5.5.2 Вкладка «Нарушители»

Нарушитель — это лицо или событие (явление), в результате действий (наступления, возникновения) которых возможно нарушение конфиденциальности, целостности или доступности информации, содержащейся в комплексе, и возникновение неприемлемых негативных последствий (ущерба).

Добавление нарушителя позволяет проверить безопасность системы. Построение векторов атак с использованием модели нарушителя позволяет оценить, насколько система устойчива к различным видам атак с использованием уязвимостей и обнаружить устройства с наибольшей вероятностью компрометации на основании потенциала нарушителя. Это позволяет пользователю внести, в первую очередь, соответствующие изменения и исправить выявленные проблемы на устройствах, наиболее подверженных компрометации. Впоследствии, заданную модель нарушителя можно использовать в механизме построения векторов атак, как дополнительную опцию. При её использовании, на карте сети формируется вектор, который визуализирует, какие узлы сети с использованием данной модели нарушителя могут быть скомпрометированы с высокой вероятностью и комплекс предоставляет

информацию о том, почему этот узел считается наиболее уязвимым при использовании этой сущности нарушителя.

Список нарушителей реализован в виде таблицы (рис. 46).

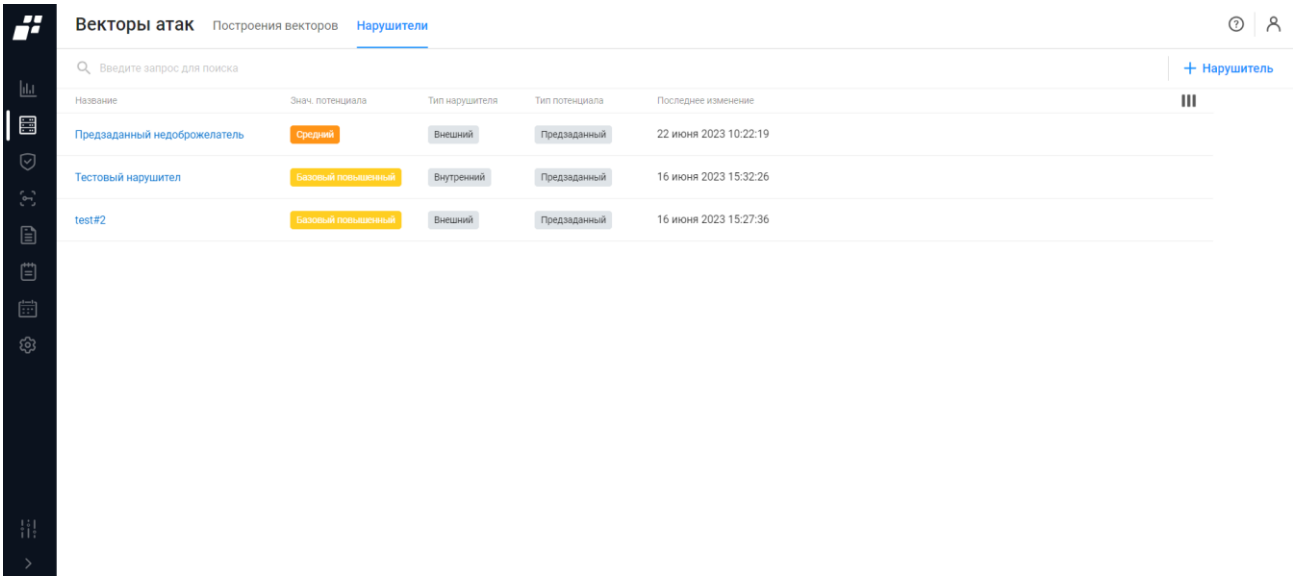


Рисунок 46 – Визуализация вектора атак на карте сети

Для каждой записи списка отображаются данные:

- название нарушителя. Является ссылкой, при переходе по которой открывается окно редактирования нарушителя;
- значение потенциала нарушителя (степень опасности);
- тип нарушителя;
- дата и время внесения изменений в настройки нарушителя.

Над списком нарушителей располагаются:

- поле поиска (Введите запрос для поиска) для поиска искомой записи в списке;
- кнопка «Нарушитель» (+ Нарушитель) для создания новой заявки;
- кнопка «Колонки» ( ) для изменения отображения колонок на странице.

При выборе строки с необходимой заявкой в правом углу строки появляются следующие кнопки:

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

5.5.2.1 Добавление нарушителя

Для добавления в список новой заявки пользователю необходимо:

1) Нажать на странице (см. рис. 46) кнопку «Нарушитель» (+ Нарушитель).

1) Откроется страница создания нового нарушителя (рис. 47). Состав и описание полей страницы приведены в таблице 24.

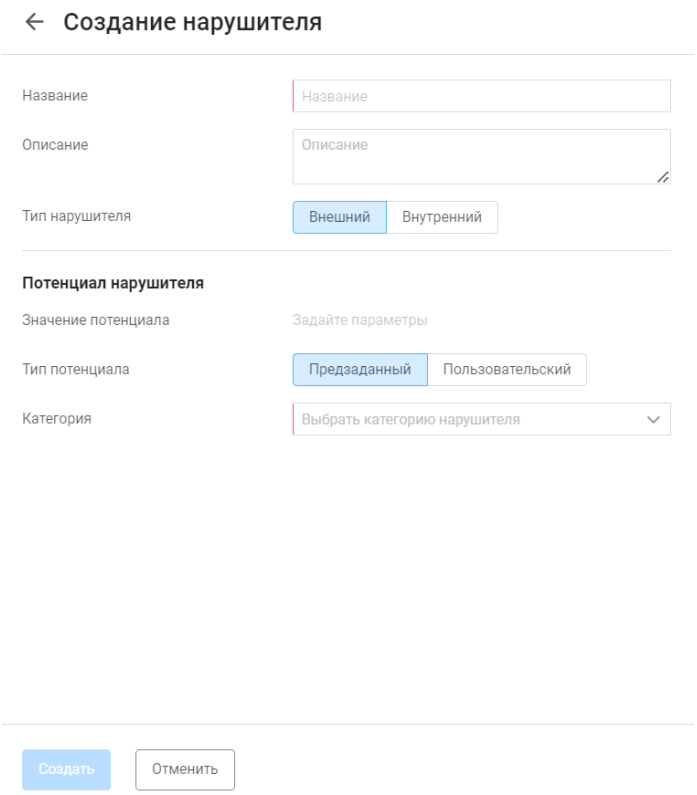


Рисунок 47 – Окно «Создание нарушителя»

Таблица 24 – Состав и описание полей окна создания нарушителя

Поле	Описание
Поле «Название»	Текстовое поле для ввода названия нарушителя. Параметры ввода текста: от 1 до 250 любых символов. Допустимые символы: латинские буквы, кириллица, цифры и символы "_", "-"
Поле «Описание»	Текстовое поле для ввода описания нарушителя. Параметры ввода текста: от 1 до 4000 любых символов
Поле «Тип нарушителя»	Переключатель: — «Внешний»; — «Внутренний»
Группа полей «Потенциал нарушителя»	
Поле «Значение потенциала»*	Поле недоступно для редактирования. Существуют следующие значения: — «Базовый»; — «Базовый повышенный»; — «Средний»;

Поле	Описание
	— «Высокий»
Поле «Тип потенциала»	Переключатель: — «Предзаданный»; — «Пользовательский». При выборе переключателя «Пользовательский» появляются дополнительные поля
Поле «Категория»	Раскрывающийся список с категориями
Поле «Затрачиваемое время»	Переключатель: — «<30 мин»; — «<1 дня»; — «<1 месяца»; — «>1 месяца»
Поле «Техническая компетентность»	Переключатель: — «Непрофессионал»; — «Специалист»; — «Профессионал»
Поле «Знание проекта и ИС»	Раскрывающийся список
Поле «Возможности доступа к ИС»	Раскрывающийся список
Поле «Оснащенность нарушителя»	Раскрывающийся список
Элементы управления	
Создать	При нажатии на кнопку окно создания заявки закрывается, заявка отображается в списке заявок
Отменить	При нажатии на кнопку окно создания заявки закрывается без сохранения данных
*Поле заполняется автоматически и зависит от параметров, указанных в группе полей «Потенциал нарушителя»	

2) Заполнить поля страницы соответствующими параметрами.
3) Нажать кнопку «Создать».

Автоматически запустится процесс проверки заполнения всех обязательных полей и уникальности создаваемой заявки.

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

5.6 Сканирование

Отображаемые данные и доступная функциональность в подразделе «Сканирование» зависят от наличия хотя бы одной лицензии на функциональный модуль.

В данном подразделе реализована автоматизированная возможность формирования списка подключенных к ПК «Efros DO» физических устройств в определенном диапазоне IP-адресов.

При первой авторизации в комплексе подраздел «Сканирование» не содержит ни одного устройства, на странице отображается сообщение «Список пуст. Вы можете выполнить новое сканирование» и кнопка «Сканировать» для перехода в окно настроек сканирования сети.

5.6.1 Запуск нового сканирования

Для запуска нового сканирования необходимо выполнить следующие действия:

1) Нажать кнопку в центре страницы « Сканировать » или кнопку « Сканировать » в правом верхнем углу страницы.
2) Откроется окно «Настройки сканирования» (рис. 48). Состав и описание полей окна приведены в таблице 25.

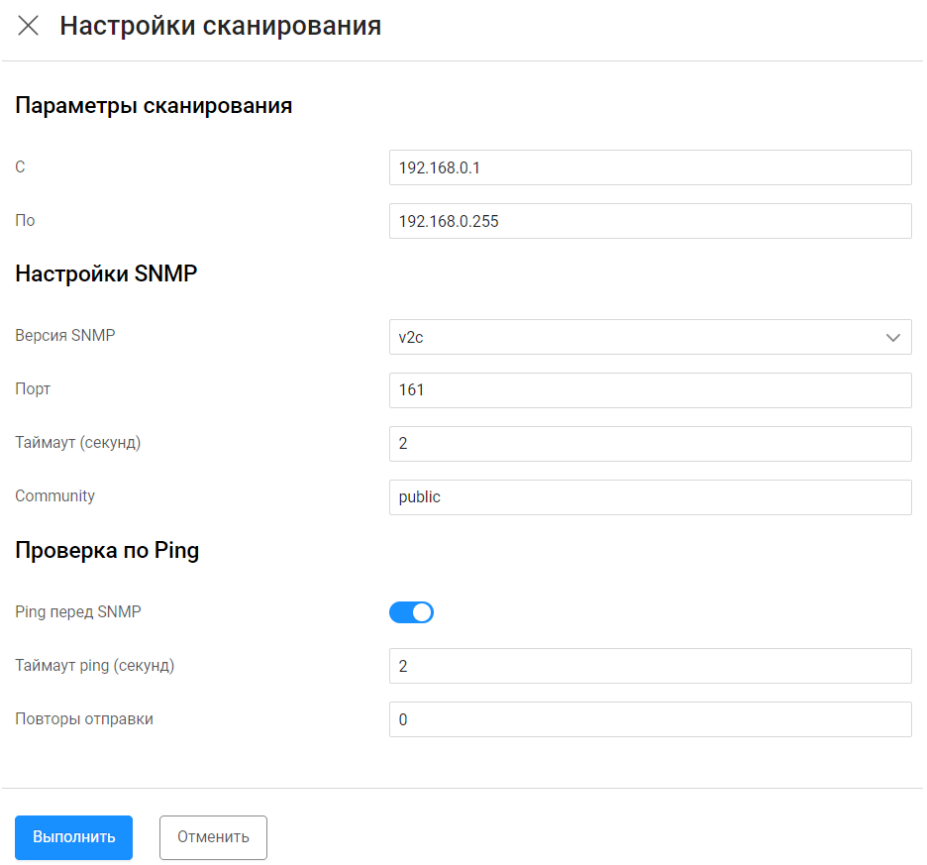


Рисунок 48 – Окно «Настройки сканирования»

Таблица 25 – Состав и описание полей окна «Настройки сканирования»

Поле	Описание
Группа полей «Параметры сканирования»	
Поле «С»	IP-адрес, с которого начинается сканирование
Поле «По»	IP-адрес, на котором заканчивается сканирование
Группа полей «Настройки SNMP»	
Поле «Версия SNMP»	Раскрывающийся список с версиями протокола SNMP. Количество полей для дальнейшей настройки зависит от выбранной версии протокола
Поле «Порт»	Порт на устройстве, на который будут отправляться SNMP-запросы
Поле «Таймаут»	Временной промежуток ожидания ответа от агента SNMP перед сканированием следующего IP-адреса
Поле «Community»	Идентификатор используемый для аутентификации на контролируемом устройстве при использовании протокола SNMPv.2c. Рекомендуемое значение «public». Поле обязательно к заполнению при использовании SNMPv2c
Поле «Имя	Имя (логин) учетной записи пользователя, которая будет

Поле	Описание
пользователя»	использоваться для авторизации на контролируемом устройстве по протоколу SNMPv.3. Поле обязательно к заполнению при использовании SNMPv.3
Поле «Пароль аутентификации»	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 «Пароль privacy»	Пароль для управления контролируемым устройством при использовании протокола SNMPv.3. Поле обязательно к заполнению при использовании SNMPv.3
Поле «Аутентификация»	Выбор алгоритма хеширования при аутентификации контролируемого устройства при использовании протокола SNMPv.3. Можно установить использование алгоритмов MD5 (Message Digest 5), SHA (Secure Hash Algorithm), либо отказаться от хеширования выбрав значение «None»
Поле «Алгоритм privacy»	Выбор алгоритма для подключения к контролируемому устройству при использовании протокола SNMPv.3. Возможные варианты для выбора: — «AES128 (Advanced Encryption Standard)»; — «DES (Data Encryption Standard)». Для отказа выбрать значение «None»
Группа полей «Проверка по Ping»	
Поле «Ping перед SNMP»	Переключатель: — «Включен»; — «Выключен». Включение проверки доступности устройства с помощью запроса ping перед началом сканирования по SNMP
Поле «Таймаут Ping» (секунд)	Временной промежуток ожидания ответа перед началом сканирования по SNMP
Поле «Повторы отправки»	Количество повторных попыток отправки ping-запроса к каждому из адресов диапазона
Элементы управления	
Выполнить	При нажатии кнопки выполняется сканирование сети
Отменить	При нажатии кнопки выполняется переход на страницу подраздела без сохранения внесенных данных

3) Заполнить параметры окна требуемыми значениями.
4) Нажать кнопку «Сохранить».

Автоматически запустится сканирование сети по указанным параметрам. Результат

сканирования сети приведен на рис. 49.

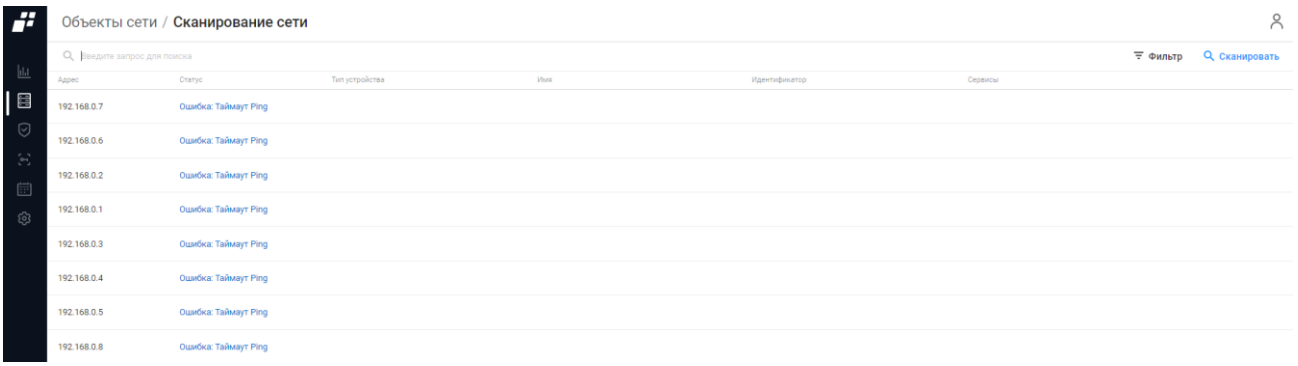


Рисунок 49 – Страница с результатом сканирования сети

Состав и описание полей страницы приведены в таблице 26.

Таблица 26 – Состав и описание страницы с результатом сканирования сети

Поле	Описание
Поле «Адрес»	IP-адрес обнаруженного устройства
Поле «Статус»	Статус выполнения операции поиска устройства по запросу к IP-адресу
Поле «Тип устройства»	Тип обнаруженного устройства
Поле «Имя»	Имя обнаруженного устройства
Поле «Идентификатор»	Идентификатор устройства
Поле «Сервисы»	Тип сервиса, через который обнаружено устройство

Обнаруженные физические ОЗ (устройства) являются несконфигурированными.

При выделении строки в списке обнаруженных ОЗ появляется окно с описанием устройства (рис. 50).

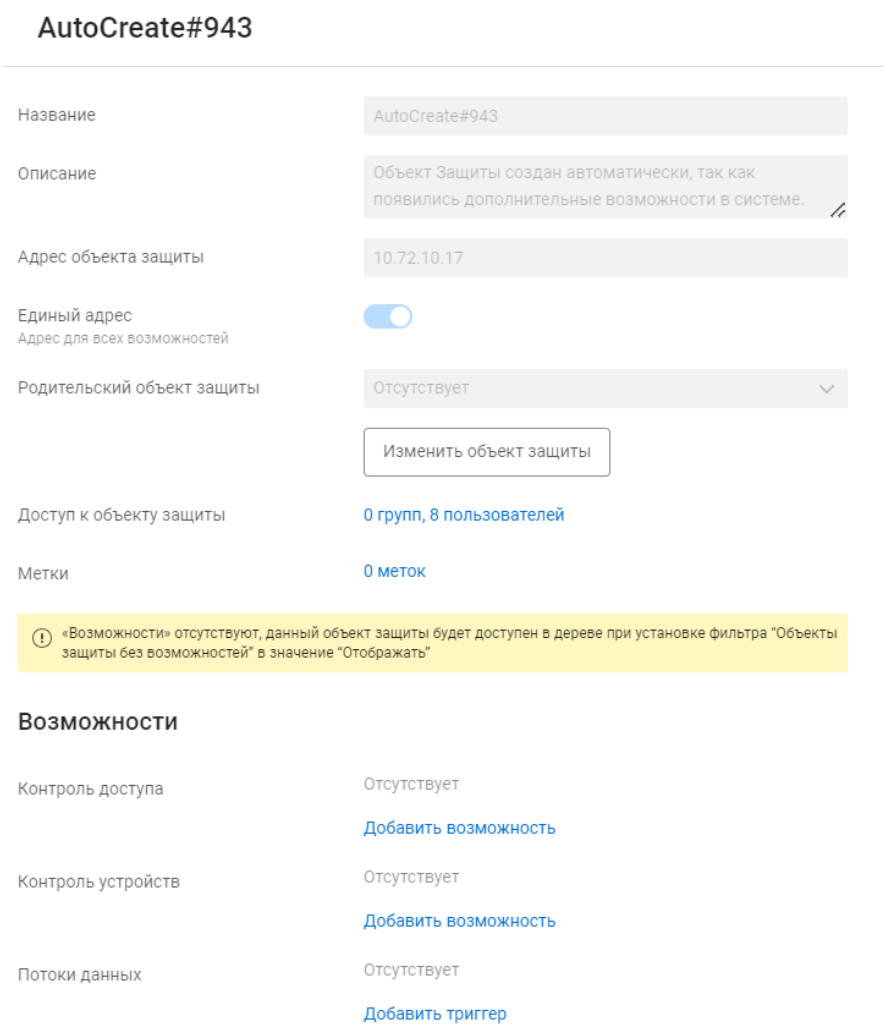


Рисунок 50 – Окно просмотра информации об ОЗ

Изменение параметров ОЗ описано в п.п. 5.1.1.6.

6 Раздел «Отчеты»

Отображаемые данные и доступная функциональность в разделе «Отчеты» зависят от наличия хотя бы одной лицензии на функциональный модуль.

В данном разделе пользователь может создавать шаблоны отчетов определенного типа по заданным параметрам. Данные, которые формируются по заданному шаблону отчета, динамично изменяются в процессе работы комплекса.

Раздел содержит отдельные вкладки: «Общие» (шаблоны отчетов могут видеть/изменять все пользователи с особыми привилегиями) и «Личные» (шаблоны отчетов доступны пользователю, который их создал). По умолчанию активной является вкладка «Общие», содержащая список общих шаблонов отчетов.

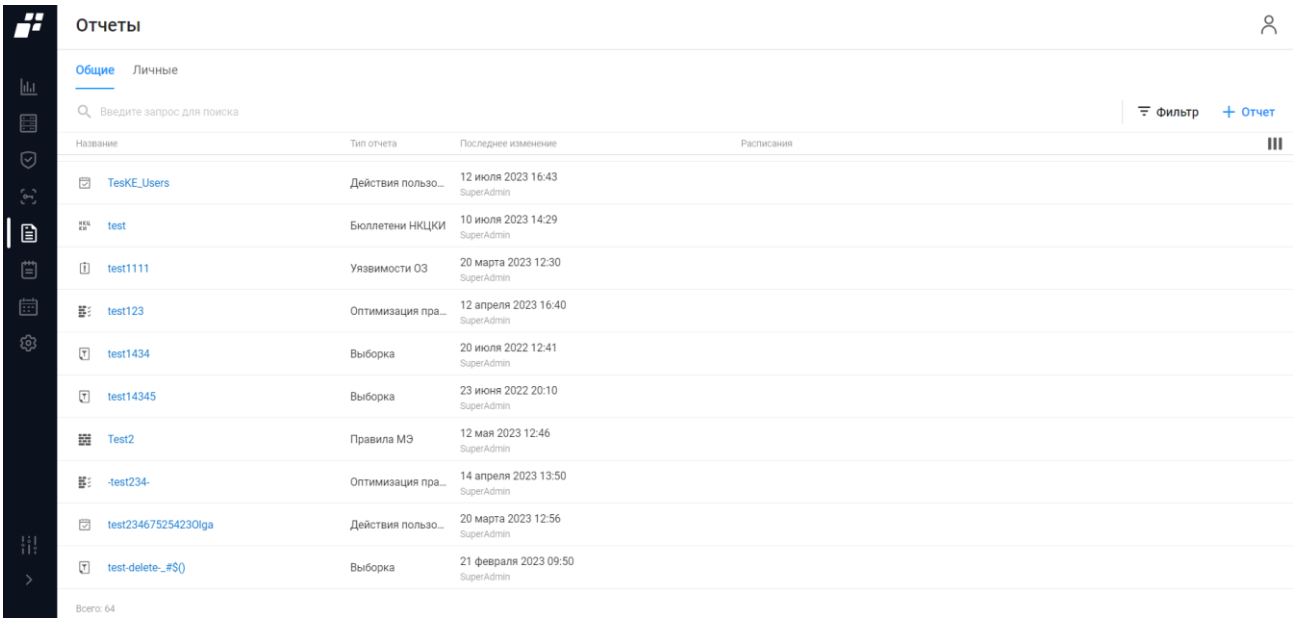


Рисунок 51 – Раздел «Отчеты»

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

- иконка с обозначением типа шаблона отчета;
- название шаблона отчета. Является ссылкой, при переходе по которой открывается окно редактирования (более подробно описано в подразделе 6.2);
- тип шаблона:
  - «Выборка» – представляет собой сводную информацию, содержащуюся в последних загруженных отчетах одного типа ОЗ, имеющих возможность «Контроль устройств». Отображается при наличии лицензии на функциональные модули «Efros NA» или «Efros ICC»;

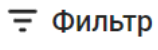
- «Действия пользователей» – представляет собой сводную информацию по действиям пользователей на ОЗ (по событиям протокола TACACS+: Аутентификация, Авторизация и Аудит). Отображается при наличии лицензии на функциональные модули «Efros NA», «Efros ICC», «Efros FA», «Efros VC» или «Efros NAC»;
- «Уязвимости ОЗ» – представляет собой сводный перечень отчетов, содержащий перечень уязвимостей для ОЗ с назначенной возможностью «Контроль устройств». Отображается при наличии лицензии на функциональный модуль «Efros VC»;
- «Бюллетени НКЦКИ» – представляет собой сводный перечень отчетов по бюллетеням НКЦКИ на ОЗ и бюллетеням из БДУ. Отображается при наличии лицензии на функциональный модуль «Efros VC»;
- «Оптимизация правил МЭ» – представляет собой сводную информацию из существующих отчетов по оптимизации правил МЭ. Отображается при наличии лицензии на функциональный модуль «Efros FA»;
- «Правила МЭ» – представляет собой сводные данные по всем правилам МЭ на ОЗ, отобранных пользователем по определенным критериям. Отображается при наличии лицензии на функциональный модуль «Efros FA».

— дата последнего изменения шаблона и логин пользователя, внесшего изменения;

— расписания, настроенные для шаблона.

Над списком шаблонов располагаются:

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

— кнопка «Фильтр» () для фильтрации списка шаблонов;

— кнопка «Добавить отчет» () для добавления шаблона отчета;

— кнопка «Колонки» () для изменения отображения колонок на странице.

При выборе строки с необходимым шаблоном в правом углу строки появляются следующие кнопки:

— кнопка «Удалить» () для удаления шаблона отчета;

— кнопка «Настройки» () для настройки шаблона отчета.

Содержание вкладки «Личные» аналогично содержанию вкладки «Общие», кроме колонки «Расписания».

6.1 Создание шаблона отчета

Для добавления в список нового шаблона пользователю необходимо выполнить следующие действия:

1) Нажать кнопку «Отчет» (+ Отчет) (см. рис. 51).
2) Из раскрывающегося списка выбрать необходимый шаблон.
3) Откроется страница создания шаблона отчета. Состав и описание полей страницы в зависимости от типа создаваемого шаблона приведены в таблице 27.

Таблица 27 – Состав и описание полей страницы создания шаблона отчета

Поле	Описание
Поля страницы «Создание отчета (Выборка)»	
Поле «Вендор»	Раскрывающийся список всех типов устройств, доступных в комплексе
Поле «Базовый отчет»	Раскрывающийся список базовых отчетов. Поле становится активно только после выбора типа устройства в поле «Вендор»
Поле «Объекты защиты»	Является ссылкой на форму выбора ОЗ, доступных в комплексе
Блок полей «Фильтр содержимого» в зависимости от типа базового отчета (текстовый или структурированный)	
Поля страницы «Создание отчета (Действия пользователей)»	
Поле «Пользователи»	Раскрывающийся список сетевых пользователей АСО
Поле «Объекты защиты»	Поле с формой выбора ОЗ, имеющих возможность «Контроль доступа»
Поле «Дата за»	Переключатель для выбора времени: — «Последние N дней» – пользователь указывает цифровое количество дней; — «Период» – пользователь задает временной промежуток
Поле «Количество дней»	Указывается, за какой период необходимо сформировать отчет по действиям пользователей
Поля страницы «Создание отчета (Уязвимости ОЗ)»	
Поле «Вендор»	Раскрывающийся список установленных модулей в комплексе (более подробно описано в подразделе 9.4)
Поле «Объекты защиты»	Раскрывающийся список ОЗ, имеющих возможность «Контроль устройств»
Поле «Критичность уязвимостей»	Раскрывающийся список видов критичности уязвимостей: — «Критичные»; — «Высокой важности»; — «Средней важности»; — «Низкой важности»

Поле	Описание
	Более подробно см. документ «Руководство пользователя. Часть 2. Контроль устройств»
Поля страницы «Создание отчета (Бюллетени НКЦКИ)»	
Поле «Пользователи»	Раскрывающийся список установленных модулей в комплексе (более подробно описано в подразделе 10.4)
Поле «Объекты защиты»	Раскрывающийся список ОЗ, имеющих возможность «Контроль устройств»
Поле «Дата за»	Переключатель для выбора времени: — «Последние N дней» – пользователь указывает цифровое количество дней; — «Период» – пользователь задает временной промежуток
Поле «Количество дней»	Указывается, за какой период необходимо сформировать отчет по бюллетеням
Поле «Критичность бюллетеней»	Раскрывающийся список видов критичности бюллетеней: — «Критичные»; — «Высокой важности»; — «Средней важности»; — «Низкой важности»
Поля страницы «Оптимизация правил МЭ»	
Поле «Вендор»	Раскрывающийся список с типами устройств, которые поддерживает комплекс
Поле «Объекты защиты»	Раскрывающийся список объектов защиты. Количество ОЗ зависит от выбранного вендора
Поле «Типы оптимизации»	Раскрывающийся список со следующими значениями: — «Все значения»; — «Теневые»; — «Избыточные»; — «Нулевые Hit Count»
Поля страницы «Создание отчета (Правила МЭ)»	
Поле «Вендор»	Раскрывающийся список вендоров. Для выбора вендора необходимо проставить флаг в необходимой строке
Поле «Объекты защиты»	Раскрывающийся список объектов защиты. Количество ОЗ зависит от выбранного вендора
Поле «Действие»	Переключатель: — «Все» – в отчет попадают правила независимо от значения действия правила; — «Permit» – в отчет попадают правила, в которых в качестве действия указано Permit; — «Deny» – в отчет попадают правила, в которых в

Поле	Описание
	качестве действия указано Deny
Поле «Протоколы/порты»	Переключатель: — «Не учитывать» – в отчет попадают правила независимо от значения протоколов/портов правила; — «Any» – в отчет попадают правила, если протокол правила имеет значение Any; — «Значение» – в отчет попадают правила, содержащие указанные в проверке значения для протокола и портов. При выборе переключателя «Значение» появляется дополнительное поле для выбора протокола и порта
Поле «Адреса источника»	Переключатель: — «Не учитывать» – в отчет попадают правила независимо от значения адреса источника; — «Any» – в отчет попадают правила, если адрес источника правила имеет значение Any; — «Значение» – в отчет попадают правила, содержащие все указанные в проверке значения для адресов источников. При выборе переключателя «Значение» появляется дополнительное поле для ввода адресов источников, указанных во включаемом в отчет правиле
Поле «Адреса назначения»	Переключатель: — «Не учитывать» – в отчет попадают правила независимо от значения адреса назначения; — «Any» – в отчет попадают правила, если адрес назначения правила имеет значение Any; — «Значение» – в отчет попадают правила, содержащие все указанные в проверке значения для адресов назначения. При выборе переключателя «Значение» появляется дополнительное поле для ввода адресов назначения, указанных во включаемом в отчет правиле
Поле «Статус правила»	Переключатель: — «Все статусы» – в отчет попадают правила в любом статусе; — «Активные» – в отчет попадают активные правила; — «Отключенные» – в отчет попадают отключенные правила
Поле	Переключатель:

Поле	Описание
«Комментарий»	— «Не учитывать» – в отчет попадают правила независимо от того есть комментарий или нет; — «Есть» – в отчет попадают только правила с комментариями; — «Нет» – в отчет попадают только правила без комментариев
Элементы управления	
Выполнить	При нажатии на кнопку окно создания отчета закрывается, отображается сформированный отчет
Отменить	При нажатии на кнопку окно создания отчета закрывается без применения введенных данных

4) Заполнить поля страницы соответствующими параметрами.
5) Нажать кнопку «Выполнить».

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

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

Формирование данных в шаблоне происходит динамически при открытии шаблона. При закрытии шаблона прежняя информация в нем не сохраняется.

6.2 Редактирование шаблона отчета

Для редактирования данных шаблона отчета пользователю необходимо нажать кнопку «Настройки» справа от названия отчета, откроется страница редактирования шаблона отчета. Далее пользователю необходимо внести требуемые изменения и нажать кнопку «Сохранить».

Автоматически запустится процесс проверки заполнения всех обязательных полей и уникальности редактируемого шаблона.

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

7 Раздел «Центр задач»

Данный раздел позволяет пользователю выполнять следующие действия (рис. 52):

- создавать заявки на выполнение определенных действий;
- автоматически контролировать статусы выполнения заявок;
- контролировать процесс выполнения заявок;
- назначать сроки исполнения заявки
- назначать исполнителя;
- назначать согласующих и утверждающих лиц.

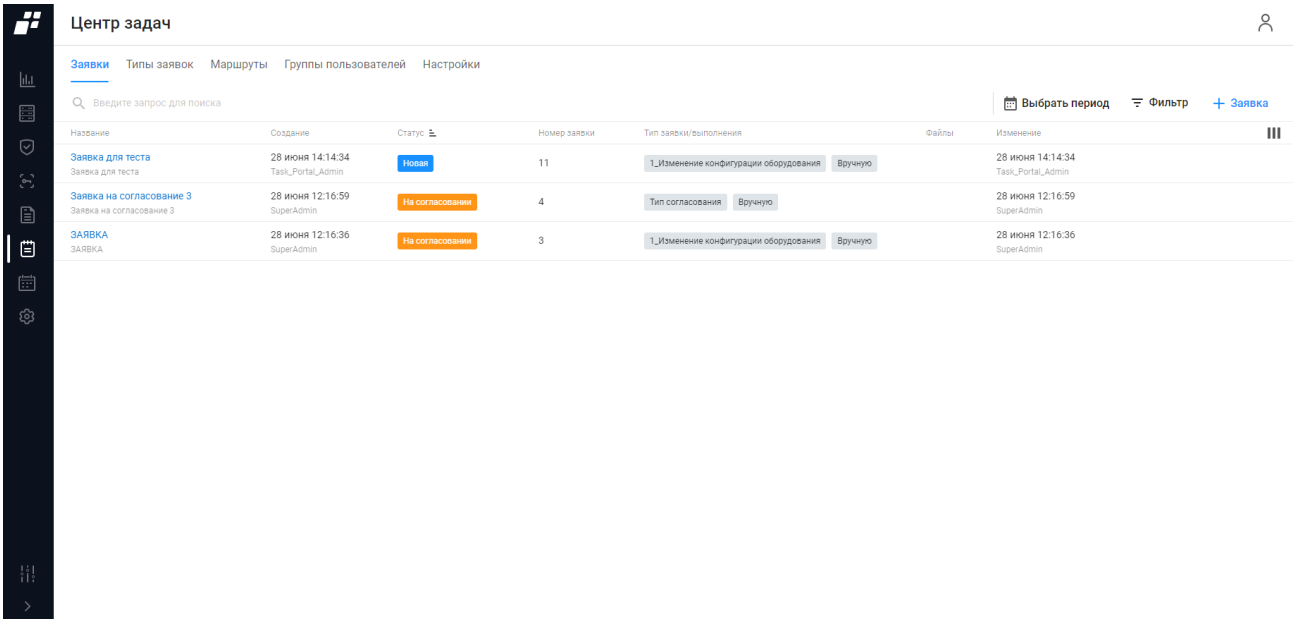


Рисунок 52 – Раздел «Центр задач»

Раздел содержит следующие вкладки:

- «Заявки» – вкладка активна по умолчанию;
- «Типы заявок»;
- «Маршруты»;
- «Группы пользователей»;
- «Настройки».

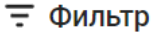
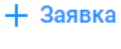
7.1 Вкладка «Заявки»

На вкладке отображаются: заявки пользователя-автора и заявки пользователя-участника в маршруте.

Список заявок реализован в виде таблицы (рис. 52). Для каждой записи списка отображаются данные:

- название заявки. Является ссылкой, при переходе по которой открывается страница управления заявкой (более подробно описано в п. 7.1.2);
- дата создания заявки и логин пользователя, создавшего заявку;
- статус заявки. Статус заявки подсвечен определенным цветом:
  - «Новая» – зеленый цвет;
  - «В работе» – голубой цвет;
  - «Проверка» – фиолетовый цвет;
  - «Закрыта» – синий цвет;
  - «На согласовании» – оранжевый цвет;
  - «На утверждении» – оранжевый цвет;
  - «На корректировке» – оранжевый цвет;
  - «Не согласована» – серый цвет;
  - «Не утверждена» – серый цвет;
  - «Срок согласования истек» – серый цвет;
  - «Срок утверждения истек» – серый цвет;
  - «Срок выполнения истек» – серый цвет;
  - «Срок проверки истек» – серый цвет;
  - «Срок корректировки истек» – серый цвет.
- номер заявки;
- тип заявки и способ выполнения заявки;
- файлы, прикрепленные к заявке в виде раскрывающегося списка с возможностью скачивания;
- дата изменения заявки и логин пользователя, внесшего изменение.

Над списком заявок располагаются:

- поле поиска () для поиска искомой записи в списке;
- кнопка «Выбрать период» () позволяет задать период для отображения заявок за определенный промежуток времени;
- кнопка «Фильтр» () для фильтрации списка заявок;
- кнопка «Заявка» () для создания новой заявки;
- кнопка «Колонки» () для изменения отображения колонок на странице.

При выборе строки с необходимой заявкой в правом углу строки появляются следующие кнопки:

- кнопка «Удалить» () для удаления заявки;

— кнопка «Создать копию» () для создания копии заявки.

7.1.1 Создание заявки

Необходимо предварительно создать группу пользователей (для работы с заявкой) на вкладке «Группы пользователей» и маршрут следования заявки на вкладке «Маршруты».

Для добавления в список новой заявки пользователю необходимо:

6) Нажать на странице (см. рис. 52) кнопку «Заявка» ().
7) Откроется страница создания новой заявки. Состав и описание полей страницы приведены в таблице 28.

Таблица 28 – Состав и описание полей страницы создания заявки

Поле	Описание
Поле «Название»	Текстовое поле для ввода названия заявки. Параметры ввода текста: от 1 до 250 любых символов
Поле «Содержание»	Текстовое поле для ввода описания заявки. Параметры ввода текста: от 1 до 4000 любых символов
Поле «Тип заявки»	Раскрывающийся список для выбора типа заявки (стандартного или пользовательского)
Поле «Файлы»	Поле для загрузки файла
Элементы управления	
Создать	При нажатии на кнопку окно создания заявки закрывается, заявка отображается в списке заявок
Отменить	При нажатии на кнопку окно создания заявки закрывается без сохранения данных

8) Заполнить поля страницы соответствующими параметрами.
9) Нажать кнопку «Создать».

Автоматически запустится процесс проверки заполнения всех обязательных полей и уникальности создаваемой заявки.

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

7.1.2 Управление заявкой

После создания заявки пользователю необходимо отправить заявку в работу:

1) Нажать на название созданной заявки. Откроется страница управления заявкой

(рис. 53)

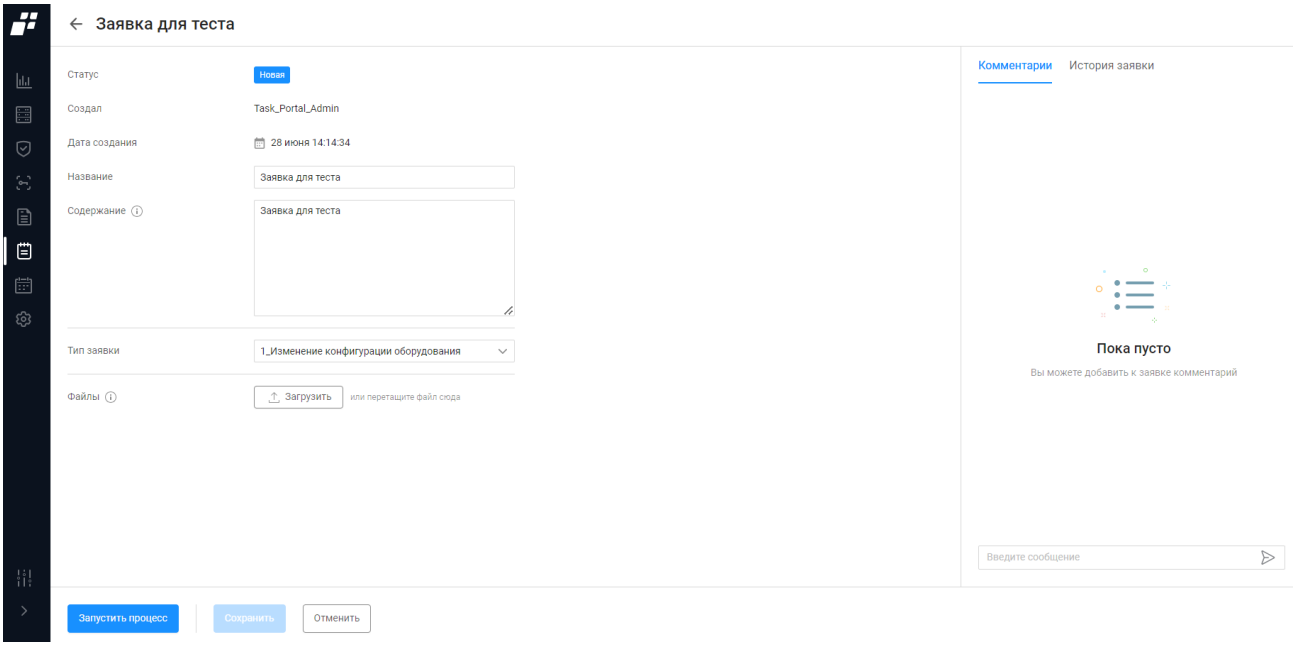


Рисунок 53 – Страница управления заявкой

2) На данной странице пользователь может выполнить следующие действия:

— отредактировать название и содержание заявки (поле доступно до стадии «На согласовании»);
— поменять тип заявки (поле доступно до стадии «На согласовании»);
— загрузить файл с расширением .docx, .csv, .xls или .xlsx, содержащий уточняющую информацию (поле доступно до стадии «На согласовании»);
— добавить комментарий на любой стадии заявки;
— просмотреть историю заявки от начала ее создания до закрытия;
— отправить заявку в работу, нажав на кнопку «Запустить процесс» (Запустить процесс);
— согласовать заявку, нажав на кнопку «Согласовать» (Согласовать);
— утвердить заявку, нажав на кнопку «Утвердить» (Утвердить);
— отметить заявку как выполненную, нажав на кнопку «Выполнено» (Выполнено);
— закрыть заявку, нажав на кнопку «Закрыть заявку» (Закрыть заявку);
— отклонить заявку, нажав на кнопку «Отклонить» (Отклонить). При нажатии на кнопку заявка закрывается со статусом «Не утверждена» или «Не согласована»;
— отправить заявку на корректировку, нажав на кнопку «Вернуть на корректировку» (Вернуть на корректировку). На этапе согласования заявка уходит на корректировку пользователю, создавшему ее. На этапе утверждения заявка отправляется на корректировку исполнителю.

7.1.3 Фильтрация заявок

Для фильтрации заявок необходимо нажать кнопку «Фильтр» ( ). Откроется окно фильтрации, приведенное на рис. 54. Состав полей окна и правила их заполнения приведены в таблице 29.

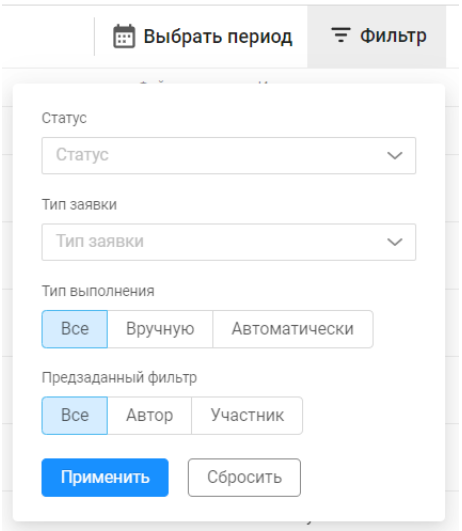


Рисунок 54 – Окно фильтрации на вкладке «Заявки»

Таблица 29 – Состав и описание полей окна фильтрации списка заявок

Поле	Описание
Поле «Статус»	Раскрывающий список со статусами заявки
Поле «Тип заявки»	Раскрывающийся список с типами заявок, созданных на вкладке «Типы заявок»
Поле «Тип выполнения»	Переключатель: — «Все»; — «Вручную»; — «Автоматически»
Поле «Предзаданный фильтр»	Переключатель: — «Все»; — «Автор»; — «Участник»
Элементы управления	
Применить	При нажатии кнопки окно фильтрации закрывается, введенные настройки фильтрации применяются
Сбросить	При нажатии кнопки окно фильтрации закрывается без применения введенных настроек

1) Заполнить необходимые параметры фильтрации.
2) Нажать кнопку «Применить».

Окно фильтрации закроется, на странице отобразятся заявки, соответствующие заданным правилам фильтрации. Для отмены заданных правил фильтрации и отображения в списке всех записей необходимо повторно нажать на кнопку «Фильтр» и нажать кнопку «Сбросить».

7.2 Вкладка «Типы заявок»

На вкладке отображаются существующие типы заявок.

На странице список типов заявок реализован в виде таблицы (рис. 55).

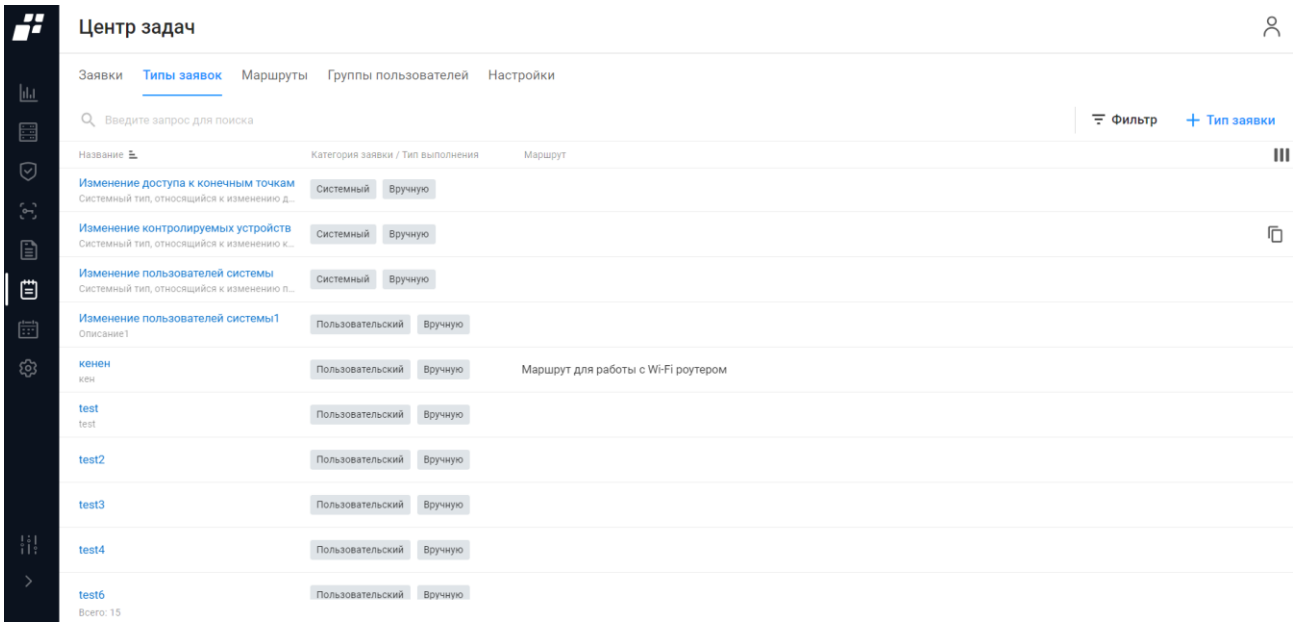


Рисунок 55 – Вкладка «Типы заявок»

Для каждой записи списка отображаются следующие данные:

- название типа заявки. Является ссылкой, при переходе по которой открывается окно редактирования типа заявки (более подробно описано в подразделе 7.2.2);
- категория заявки и способ выполнения заявки;
- маршрут.

Над списком располагаются:

- поле поиска (Введите запрос для поиска) для поиска искомой записи в списке;
- кнопка «Фильтр» (Фильтр) для фильтрации списка заявок;
- кнопка «Тип заявки» (+ Тип заявки) для создания новой заявки;
- кнопка «Колонки» ( ) для изменения отображения колонок на странице.

При выборе строки с необходимой заявкой в правом углу строки появляются следующие кнопки:

- кнопка «Удалить» ( ) для удаления заявки (для удаления доступны только пользовательские типы заявок);
- кнопка «Создать копию» ( ) для создания копии заявки.

7.2.1 Создание нового типа заявки

Для создания нового типа заявки пользователю необходимо:

1) Нажать на странице (см. рис. 52) кнопку «Заявка» (+ Заявка).
2) Откроется страница создания нового типа заявки. Состав и описание полей страницы приведены в таблице 30.

Таблица 30 – Состав и описание полей страницы создания нового типа заявки

Поле	Описание
Поле «Название»	Текстовое поле для ввода названия типа заявки. Параметры ввода текста: от 1 до 250 любых символов
Поле «Описание»	Текстовое поле для ввода описания типа заявки. Параметры ввода текста: от 1 до 4000 любых символов
Поле «Маршрут»	Раскрывающийся список маршрутов
Поле «Тип выполнения»	Заполняется автоматически: «Вручную»
Элементы управления	
Создать	При нажатии на кнопку окно создания типа заявки закрывается, новый тип заявки отображается в списке
Отменить	При нажатии на кнопку окно создания типа заявки закрывается без сохранения данных

3) Заполнить поля страницы соответствующими параметрами.
4) Нажать кнопку «Создать».

Автоматически запустится процесс проверки заполнения всех обязательных полей и уникальности создаваемой заявки.

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

7.2.2 Редактирование типа заявки

Редактирование типа заявки выполняется следующим способом:

1) Пользователю необходимо кликнуть на название необходимого типа заявки.
2) Откроется страница редактирования. Страница содержит внесенные ранее данные.
3) Внести требуемые изменения на странице редактирования и нажать кнопку «Сохранить».

Автоматически запускается процесс проверки заполненности всех обязательных полей и уникальности редактируемого типа заявки.

При обнаружении незаполненных обязательных полей под полем появится сообщение красного цвета: «Обязательное поле». Пользователю необходимо корректно заполнить

поля окна и повторно нажать кнопку «Сохранить».

7.2.3 Фильтрация типов заявок

Для фильтрации типов заявок необходимо нажать кнопку «Фильтр» ( ). Откроется окно фильтрации, приведенное на рис. 56. Состав полей окна и правила их заполнения приведены в таблице 31.

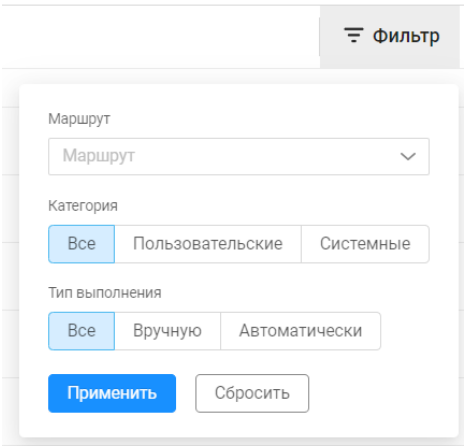


Рисунок 56 – Окно фильтрации на вкладке «Типы заявок»

Таблица 31 – Состав и описание полей окна фильтрации списка типов заявок

Поле	Описание
Поле «Маршрут»	Раскрывающийся список маршрутов, созданных на вкладке «Маршруты»
Поле «Категория»	Переключатель: — «Все»; — «Пользовательские»; — «Системные»
Поле «Тип выполнения»	Переключатель: — «Все»; — «Вручную»; — «Автоматически»
Поле «Актуальность»	Переключатель: — «Все»; — «Активные»; — «Архивные»
Элементы управления	
Применить	При нажатии кнопки окно фильтрации закрывается, введенные настройки фильтрации применяются
Сбросить	При нажатии кнопки окно фильтрации закрывается без применения введенных настроек

4) Заполнить необходимые параметры фильтрации.
5) Нажать кнопку «Применить».

Окно фильтрации закроется, на странице отобразятся типы заявок, соответствующие заданным правилам фильтрации. Для отмены заданных правил фильтрации и отображения в списке всех записей необходимо повторно нажать на кнопку «Фильтр» и нажать кнопку «Сбросить».

7.3 Вкладка «Маршруты»

Вкладка «Маршруты» содержит маршруты следования заявок (рис. 55).

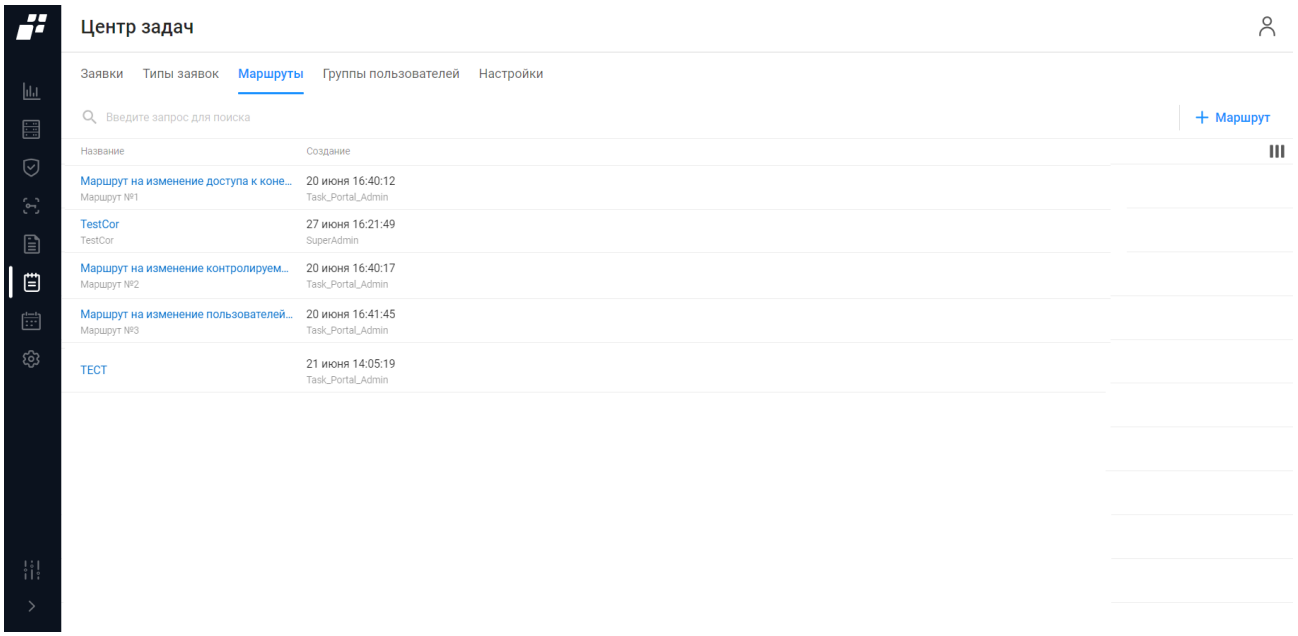


Рисунок 57 – Вкладка «Маршруты»

После установки комплекса и первой авторизации вкладка «Маршруты» не содержит ни одного маршрута, на странице отображается сообщение «Список маршрутов пуст. Вы можете создать маршрут при помощи кнопки ниже» и кнопка «Создать маршрут» для перехода в окно создания нового маршрута.

Для каждой записи списка отображаются следующие данные:

- название маршрута. Является ссылкой, при переходе по которой открывается окно редактирования маршрута (более подробно описано в п. 7.3.2);
- дата создания маршрута и логин пользователя, создавшего маршрут.

Над списком располагаются:

- поле поиска (Введите запрос для поиска) для поиска искомой записи в списке;
- кнопка «Маршрут» (+ Маршрут) для создания нового маршрута;
- кнопка «Колонки» ( ) для изменения отображения колонок на странице.

При выборе строки с необходимой заявкой в правом углу строки появляются следующие кнопки:

- кнопка «Удалить» ( ) для удаления маршрута;
- кнопка «Создать копию» ( ) для создания копии и последующего

редактирования маршрута.

7.3.1 Создание нового маршрута

Проверить, что созданы необходимые группы пользователей на вкладке «Группы пользователей» раздела «Центр задач». При необходимости добавить соответствующих пользователей в БД комплекса.

Страница создания маршрута представляет собой конструктор с последовательным выполнением заданных стадий (рис. 58).

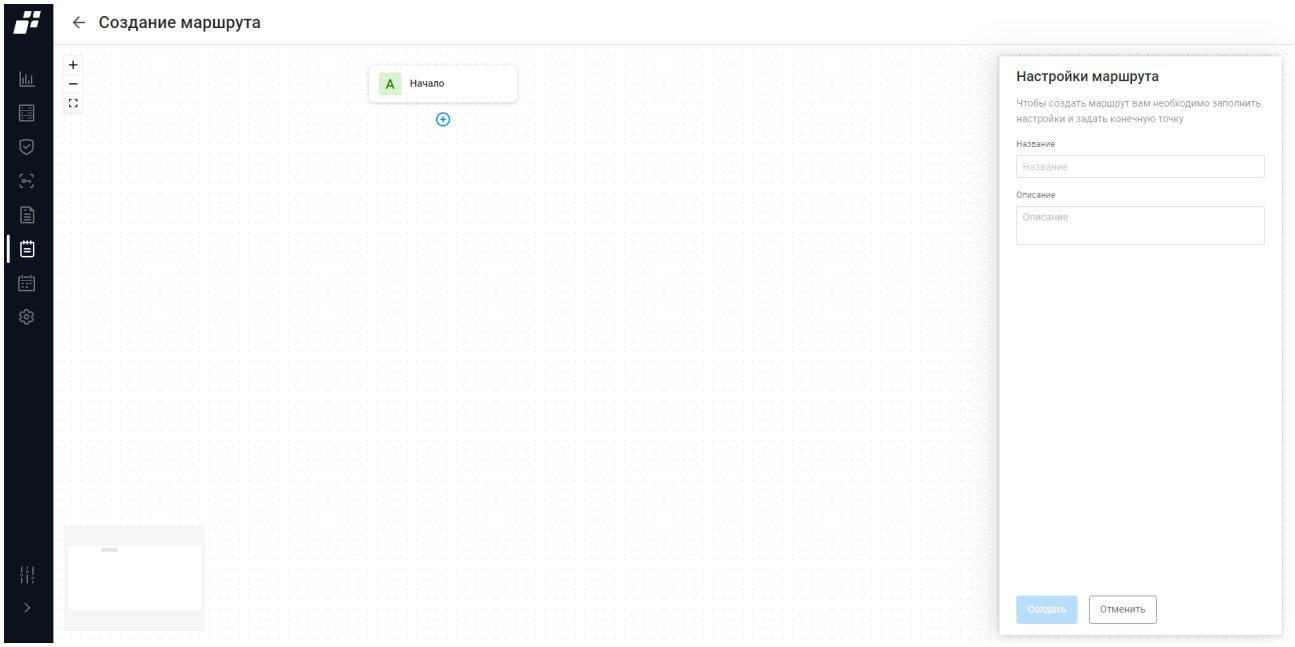


Рисунок 58 – Страница создания маршрута

На странице отображаются следующие элементы:

- поле для создания маршрута с начальным объектом «А – Начало»;
- кнопки масштаба;
- мини-карта для оценки общего вида маршрута;
- окно для настройки маршрута с полями «Название» и «Описание».

При добавлении стадии «Согласовано» необходимо выбрать группу пользователей, которые будут участвовать в согласовании заявки и добавить условие согласования.

При добавлении стадии «Утверждение» необходимо выбрать группу пользователей, которые будут утверждать заявку и добавить условие выполнения заявки.

При добавлении стадии «Выполнение» необходимо выбрать группу пользователей, которые будут исполнять заявку и добавить условие выполнения заявки.

При добавлении стадии «Проверка» необходимо выбрать группу пользователей, которые будут проверять заявку и добавить условие проверки заявки.

Условие «И/ИЛИ»:

- «И» – все пользователи, принадлежащие выбранной группе должны отреагировать на заявку, чтобы заявке присвоился следующий статус;
- «ИЛИ» – один пользователь из принадлежащих выбранной группе должен отреагировать на заявку, чтобы заявке присвоился следующий статус.

На стадиях «Согласование», «Проверка» и «Выполнение» пользователь из соответствующей группы может отправить заявку на корректировку.

Для добавления в список нового маршрута пользователю необходимо скомбинировать стадии маршрута и дополнительные шаги, назначить группы пользователей для основных стадий заявки, указать название и описание маршрута и нажать кнопку «Сохранить». Примеры маршрутов приведены в приложении А.

Существуют следующие основные стадии заявки:

- «Начало»;
- «Согласование» – заявка находится в стадии согласования;
- «Утверждение» – заявка находится в стадии утверждения;
- «Выполнение» – заявка находится в стадии выполнения;
- «Проверка» – заявка находится в стадии проверки;
- «Корректировка» – заявка находится в стадии корректировки.

Дополнительные шаги при прохождении заявки по маршруту:

- «Условие» – шаг, позволяющий выбрать одну из стадий: «Завершение», «Корректировка», «Утверждение», «Выполнение» или «Проверка»;
- «Уведомление» — группы пользователей, указанные в маршруте заявки, будут получать уведомления об изменении статуса заявки согласно выбранному маршруту;
- «Завершение» — закрытие заявки или ее отклонение одним из группы пользователей, указанных в маршруте.

Статусы для каждой стадии заявки:

- «Новая» — заявка создана в системе;
- «На согласовании» — заявка отправлена на согласование группе пользователей;
- «Срок истек» — заданный на вкладке «Настройки» срок статуса заявки истек;
- «Не согласована» — заявка не согласована одним или несколько пользователями в зависимости от заданных условий в поле «Условия»;

— «На утверждении» — заявка на стадии утверждения;
— «Не утверждена» — заявка не утверждена одним или несколькими пользователями в зависимости от заданных условий в поле «Условия»;
— «В работе» — заявка взята в работу группой пользователей, указанных в маршруте;
— «Проверка» — заявка находится на стадии проверки;
— «На корректировке» — заявка находится на стадии корректировки;
— «Закрыта» — заявка закрыта. Заявка выполнена или отклонена.

Статусы недоступны для редактирования.

7.3.2 Редактирование маршрута

Редактирование маршрута выполняется следующим способом:

1) Пользователю необходимо кликнуть на название необходимого маршрута.
2) Откроется страница редактирования. Страница содержит внесенные ранее данные.
3) Внести требуемые изменения на странице редактирования и нажать кнопку «Сохранить».

Автоматически запускается процесс проверки заполненности всех обязательных полей и уникальности редактируемого маршрута.

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

7.4 Вкладка «Группы пользователей»

Вкладка «Группы пользователей» содержит группы пользователей, которые участвуют в маршруте выполнения заявки (рис. 55).

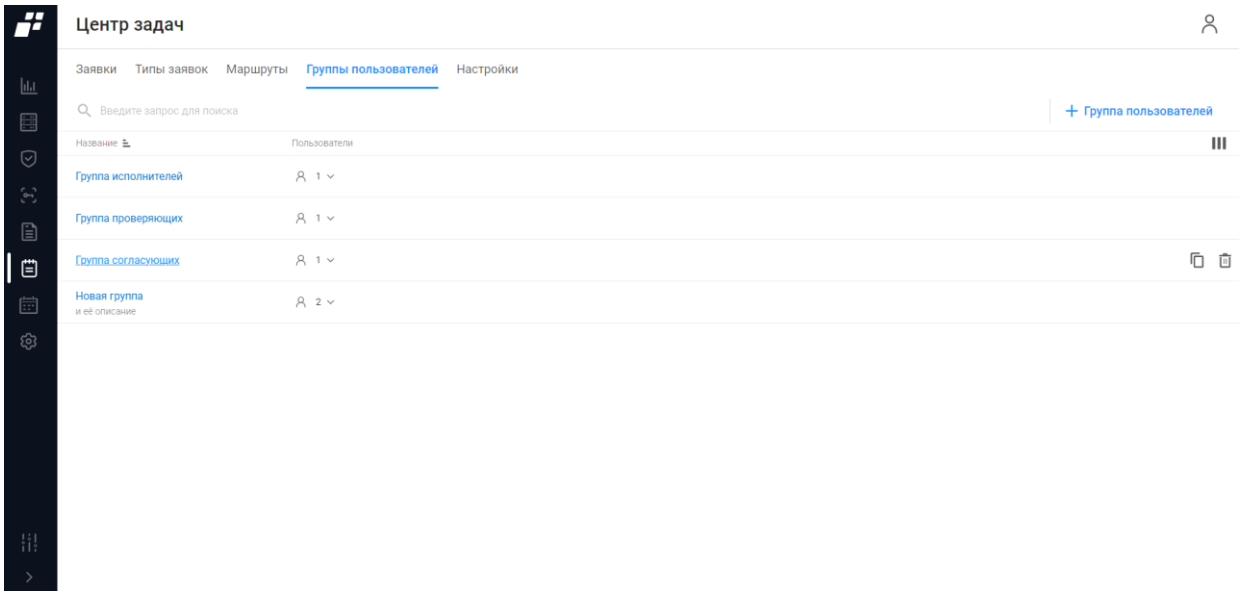


Рисунок 59 – Вкладка «Группы пользователей»

После установки комплекса и первой авторизации вкладка «Группы пользователей» не содержит ни одной группы, на странице отображается сообщение «Список групп пользователей пуст. Вы можете создать группу пользователей при помощи кнопки ниже» и кнопка «Создать группу пользователей» для перехода в окно создания группы пользователей.

Для каждой записи списка отображаются следующие данные:

- название группы. Является ссылкой, при переходе по которой открывается окно редактирования группы (более подробно описано в п. 7.4.2);
- количество пользователей, входящих в группу.

Над списком располагаются:

- поле поиска (Введите запрос для поиска) для поиска искомой записи в списке;
- кнопка «Группа пользователей» (+ Группа пользователей) для создания новой группы;
- кнопка «Колонки» ( ) для изменения отображения колонок на странице.

При выборе строки с необходимой группой в правом углу строки появляются следующие кнопки:

— кнопка «Удалить» ( ) для удаления группы;

— кнопка «Создать копию» ( ) для создания копии и последующего редактирования группы.

7.4.1 Создание новой группы пользователей

Для создания новой группы пользователей пользователю необходимо:

1) Нажать на странице (см. рис. 59) кнопку «Группа пользователей» (+ Группа пользователей).
2) Откроется страница создания новой группы пользователей. Состав и описание полей страницы приведены в таблице 32.

Таблица 32 – Состав и описание полей страницы создания новой группы

Поле	Описание
Поле «Название»	Текстовое поле для ввода названия группы пользователей. Параметры ввода текста: от 1 до 250 любых символов
Поле «Описание»	Текстовое поле для ввода описания группы пользователей. Параметры ввода текста: от 1 до 4000 любых символов
Поле «Пользователи»	Поле для выбора пользователей. При переходе по ссылке открывается окно для добавления пользователей в создаваемую группу
Элементы управления	
Создать	При нажатии на кнопку окно создания группы закрывается, группа отображается в списке
Отменить	При нажатии на кнопку окно создания группы закрывается без сохранения данных

3) Заполнить поля страницы соответствующими параметрами.
4) Нажать кнопку «Создать».

Автоматически запустится процесс проверки заполнения всех обязательных полей и уникальности создаваемой группы пользователей.

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

7.4.2 Редактирование группы пользователей

Редактирование группы пользователей выполняется следующим способом:

1) Пользователю необходимо кликнуть на название необходимой группы.
2) Откроется страница редактирования. Страница содержит внесенные ранее данные.

3) Внести требуемые изменения на странице редактирования и нажать кнопку «Сохранить».

Автоматически запустится процесс проверки заполненности всех обязательных полей и уникальности редактируемой группы.

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

7.5 Вкладка «Настройки»

Данная вкладка позволяет пользователю задать максимальный размер прикрепляемого файла и временной промежуток прохождения каждой стадии.

На рисунке 60 приведена страница вкладки «Настройки».

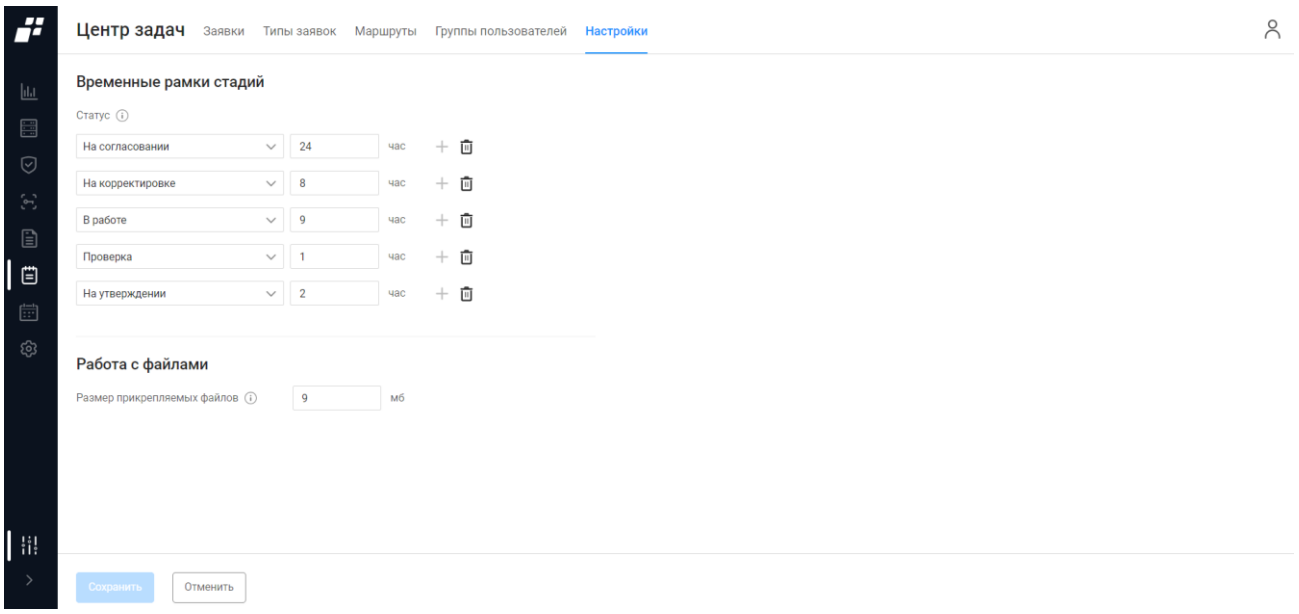


Рисунок 60 – Вкладка «Настройки»

Состав и описание полей страницы приведены в таблице

Таблица 53.

Таблица 33 – Состав и описание полей вкладки «Настройки»

Поле	Описание
Блок полей «Временные рамки стадий»	
Поле «Статус»	Таблица статусов заявки
Поле для ввода количества часов	Поле для ввода количества часов, отведенных для перехода заявки из статуса в статус
Блок полей «Работа с файлами»	
Поле «Размер прикрепляемых файлов»	Поле для установки максимального размера прикрепляемого к заявке файла в Мб

8 Раздел «События»

В данном разделе агрегируются системные события, события, связанные с пользователями комплекса, и события из функциональных модулей «Efros NA», «Efros NAC», «Efros VC», «Efros FA», «Efros ICC» или «Efros NFA».

8.1 Центр задач

Отображаемые данные и доступная функциональность подраздела «Центр задач» зависит от наличия лицензии на один из функциональных модулей: «Efros NA», «Efros NAC», «Efros VC», «Efros FA», «Efros ICC» или «Efros NFA».

Данный подраздел отображает сводный список событий, связанных с заявками из раздела «Центр задач» (рис. 61).

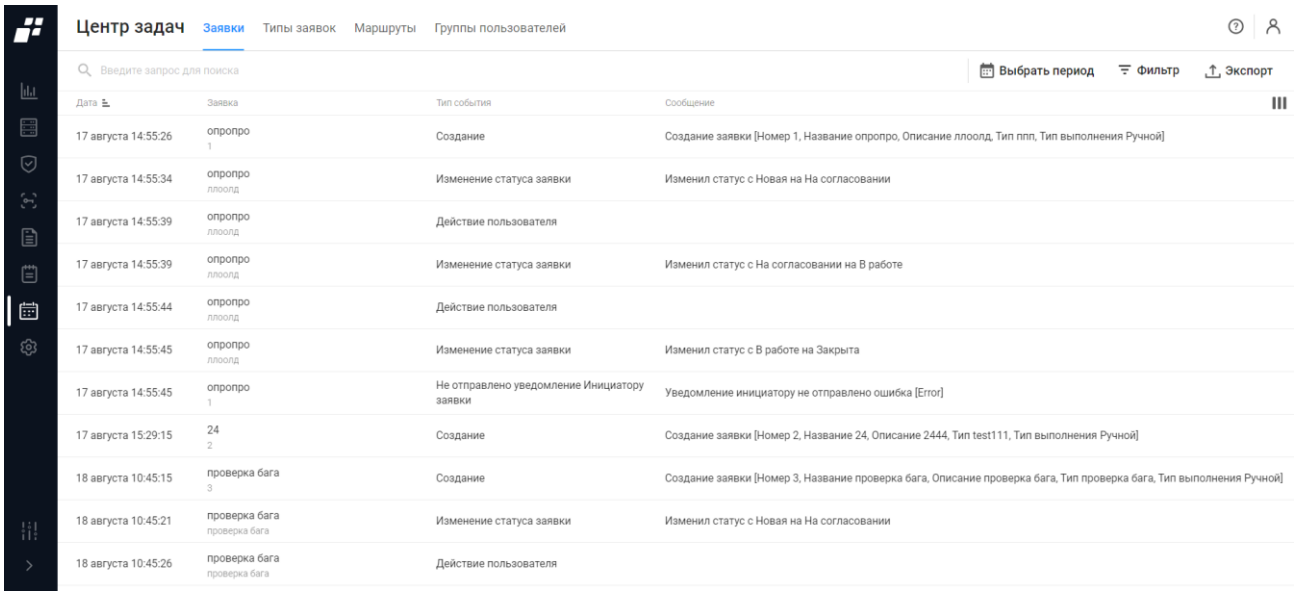


Рисунок 61 – Подраздел «Центр задач»

Страница содержит вкладки:

- «Заявки» – содержит события, связанные с созданием и изменением статуса заявки;
- «Типы заявок» – содержит события, связанные с созданием\изменением типов заявок;
- «Маршруты» – содержит события, связанные с созданием\изменением маршрутов;
- «Группы пользователей» – содержит события, связанные с созданием\изменением групп пользователей.

На странице список событий реализован в виде таблицы (см. рис. 61). Для каждой

записи списка отображаются следующие данные:

- дата и время фиксации события;
- название и описание заявки;
- тип заявки (вкладка «Типы заявок»);
- маршрут (вкладка «Маршруты»);
- группа пользователей, принимающая участие в движении заявки (вкладка «Группы пользователей»);
- тип события;
- сообщение – краткое описание события.

Над списком событий располагаются:

- поле поиска (Введите запрос для поиска) для поиска искомой записи в списке;
- кнопка «Выбрать период» (Выбрать период) для фильтрации событий по заданному периоду;
- кнопка «Фильтр» (Фильтр) для фильтрации событий по заданным параметрам;
- кнопка «Экспорт» (Экспорт) для экспорта журнала событий в формате csv и xlsx);
- кнопка «Колонки» ( ) для изменения отображения колонок на странице.

8.2 Объекты защиты

Отображаемые данные и доступная функциональность подраздела «Объекты защиты» зависит от наличия лицензии на один из функциональных модулей: «Efros NA», «Efros NAC», «Efros VC», «Efros FA», «Efros ICC» или «Efros NFA».

Данный подраздел содержит сводный список событий безопасности, полученных от ОЗ с возможностями «Контроль устройств», «Контроль доступа» и «Потоки данных» (рис. 62).

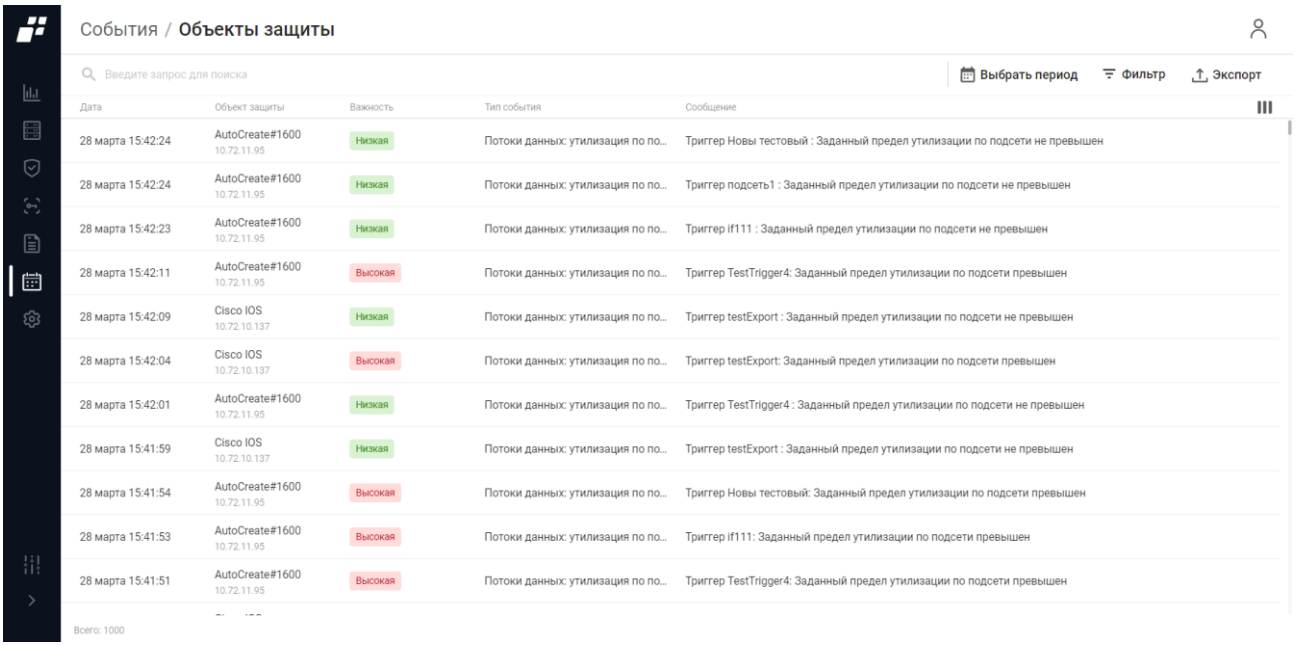


Рисунок 62 – Подраздел «Объекты защиты»

Для каждой записи списка отображаются следующие данные:

- дата фиксации события;
- название и IP-адрес ОЗ;
- важность зафиксированного события;
- тип события;
- краткое описание события.

Над списком событий располагаются:

- поле поиска (Введите запрос для поиска) для поиска искомой записи в списке;
- кнопка «Выбрать период» (Выбрать период) для фильтрации событий по заданному периоду;
- кнопка «Фильтр» (Фильтр) для фильтрации списка событий;
- кнопка «Экспорт» (Экспорт) для экспорта журнала событий в формате csv и xlsx;
- кнопка «Колонки» ( ) для изменения отображения колонок на странице.

8.3 Аудит

Отображаемые данные и доступная функциональность подраздела «Аудит» зависит от наличия хотя бы одной лицензии на функциональный модуль.

Данный подраздел содержит список событий, связанных с действиями пользователя при работе с комплексом (рис. 63).

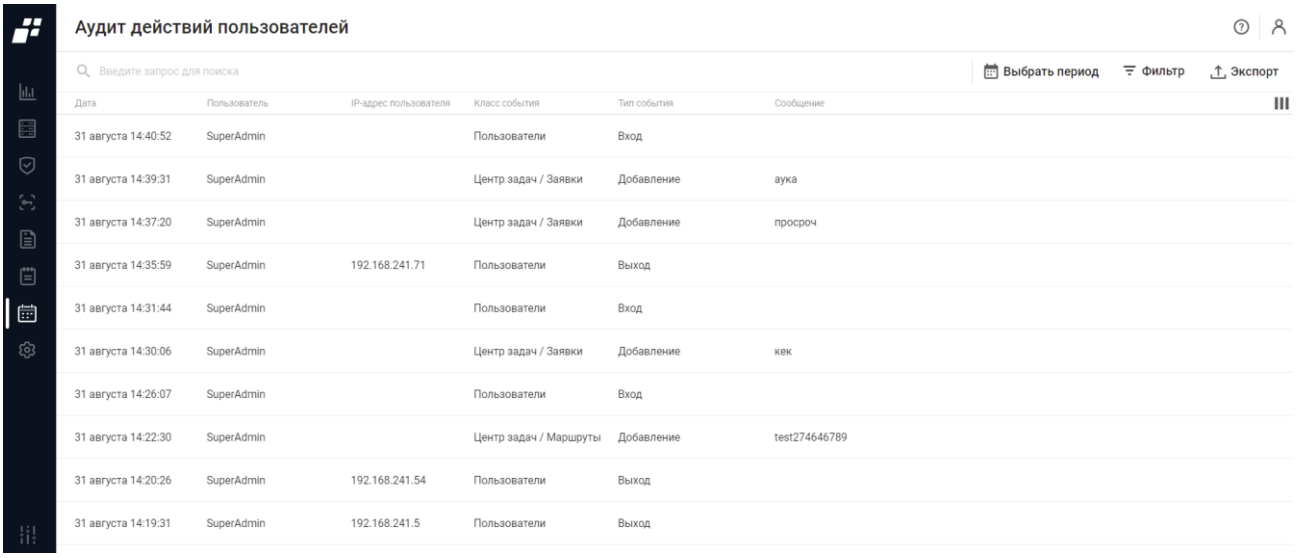


Рисунок 63 – Подраздел «Аудит»

Для каждой записи списка отображаются следующие данные:

- дата фиксации события;
- логин пользователя комплекса, с кем связано произошедшее событие;
- IP-адрес пользователя;
- класс события;
- тип события;
- краткое описание события.

Над списком событий располагаются:

- поле поиска (Введите запрос для поиска) для поиска искомой записи в списке;
- кнопка «Выбрать период» (Выбрать период) для фильтрации событий по заданному периоду;
- кнопка (Фильтр) для фильтрации событий по заданным параметрам;
- кнопка «Экспорт» (Экспорт) для экспорта журнала аудита в формате csv и xlsx;

— кнопка «Колонки» ( ) для изменения отображения колонок на странице.

8.4 Доступ в сеть

Подраздел «Доступ в сеть» доступен пользователю для работы при наличии лицензии на функциональный модуль «Efros NAC».

Данный подраздел содержит список событий, связанных с попытками аутентификации пользователей на оборудовании и с работой пользователей на устройствах (рис. 64).

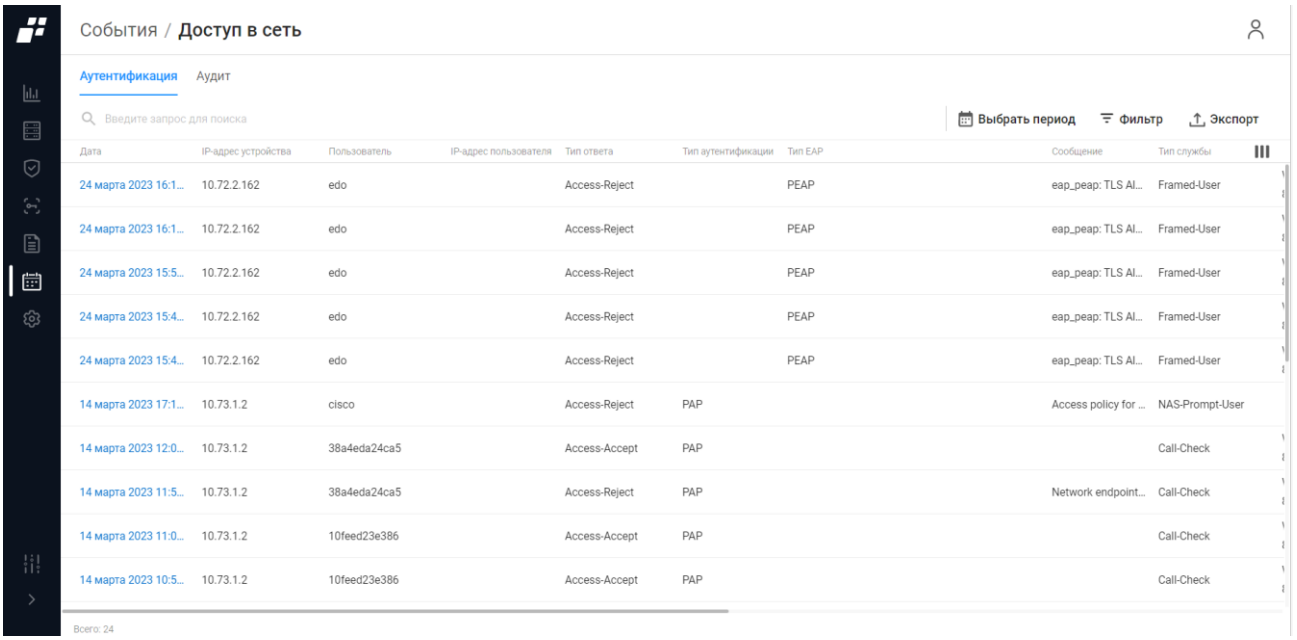


Рисунок 64 – Подраздел «Доступ в сеть»

Страница содержит следующие вкладки:

— «Аутентификация» – содержит события, связанные с попытками аутентификации сетевых пользователей (результаты проверки подлинности сетевых пользователей);
— «Аудит» – содержит события, связанные с работой сетевых пользователей на устройствах после получения доступа к ним.

Над списком событий располагаются:

— поле поиска (Введите запрос для поиска) для поиска искомой записи в списке;
— кнопка (Фильтр) для фильтрации событий по заданным параметрам;
— кнопка «Экспорт» (Экспорт) для экспорта журнала событий в формате csv и xlsx;
— кнопка «Колонки» ( ) для изменения отображения колонок на странице.

8.5 Доступ на оборудование

Подраздел «Доступ на оборудование» доступен пользователю для работы при наличии лицензии на функциональный модуль «Efros NAC».

Данный подраздел содержит список событий, связанных с попытками аутентификации сетевых пользователей на оборудовании, авторизации и с работой на устройствах (рис. 65).

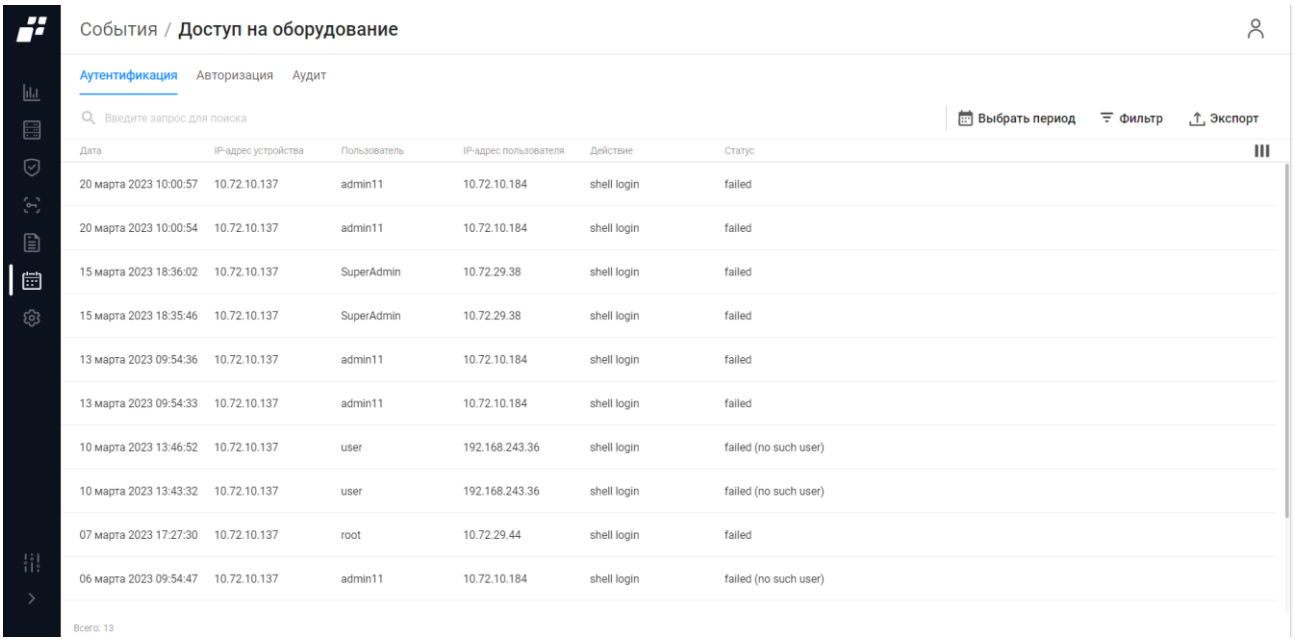


Рисунок 65 – Подраздел «Доступ на оборудование»

Страница содержит вкладки:

- «Аутентификация» – содержит события, связанные с попытками аутентификации сетевых пользователей (результаты проверки подлинности сетевых пользователей);
- «Авторизация» – содержит события, связанные с попытками авторизации сетевых пользователей (результаты попыток сетевых пользователей выполнить команды на устройствах);
- «Аудит» – содержит события, связанные с работой сетевых пользователей на устройствах после получения доступа к ним.

Над списком событий располагаются:

- поле поиска (Введите запрос для поиска) для поиска искомой записи в списке;
- кнопка (Фильтр) для фильтрации событий по заданным параметрам;

— кнопка «Экспорт» (Экспорт) для экспорта журнала событий в формате csv и xlsx;

— кнопка «Колонки» ( ) для изменения отображения колонок на странице.

8.6 Системные события

Отображаемые данные и доступная функциональность раздела «Системные события» зависят от наличия лицензии хотя бы на один из функциональных модулей: «Efros NA», «Efros NAC», «Efros VC», «Efros FA» или «Efros ICC».

Данный подраздел содержит список внутренних событий комплекса и системных событий модулей «Efros NA», «Efros NAC», «Efros VC», «Efros FA» или «Efros ICC» (рис. 66).

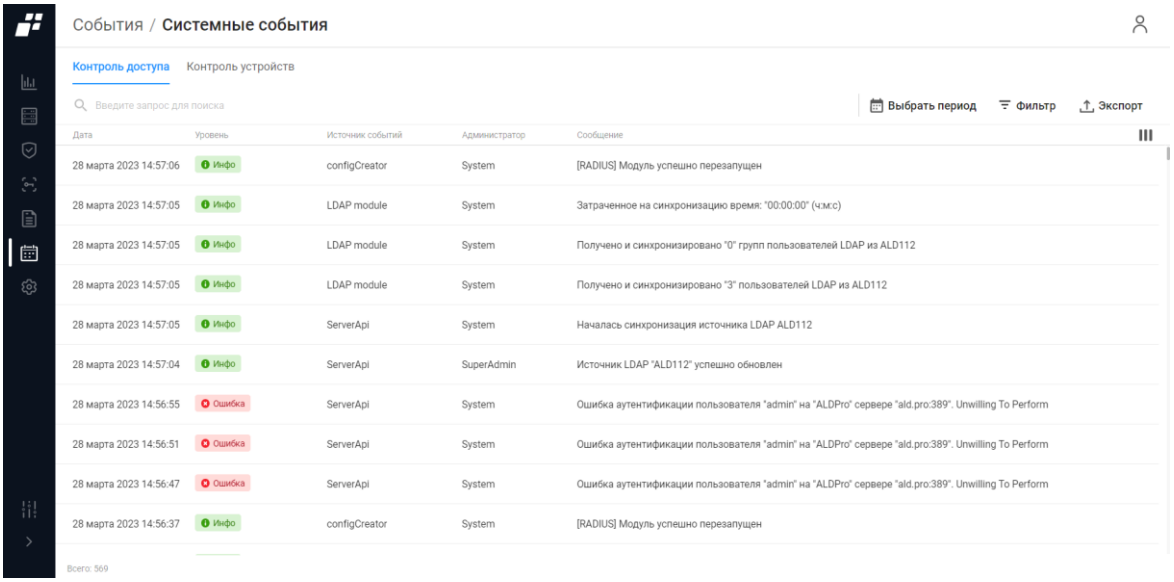


Рисунок 66 – Подраздел «Системные события»

Страница содержит вкладки:

— «Контроль доступа» – содержит системные события модуля «Efros NAC»;

— «Контроль устройств» – содержит системные события модулей «Efros NA», «Efros VC», «Efros FA» и «Efros ICC».

8.6.1 Вкладка «Контроль доступа»

На странице список событий реализован в виде таблицы (см. рис. 66). Для каждой записи списка отображаются следующие данные:

— дата и время фиксации события;

— уровень значимости события:

- «Информационное» – информационное сообщение;
- «Предупреждение» – предупреждение, не влияет не логику работы приложения;
- «Ошибка» – непредвиденное поведение.

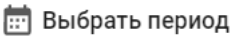
— источник события;

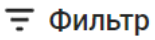
— пользователь;

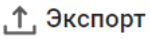
— сообщение – краткое описание события.

Над списком событий располагаются:

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

— кнопка «Выбрать период» () для фильтрации событий по заданному периоду;

— кнопка «Фильтр» () для фильтрации списка событий;

— кнопка «Экспорт» () для экспорта журнала событий в формате csv и xlsx;

— кнопка «Колонки» () для изменения отображения колонок на странице.

8.6.2 Вкладка «Контроль устройств»

На странице список событий реализован в виде таблицы (рис. 67).

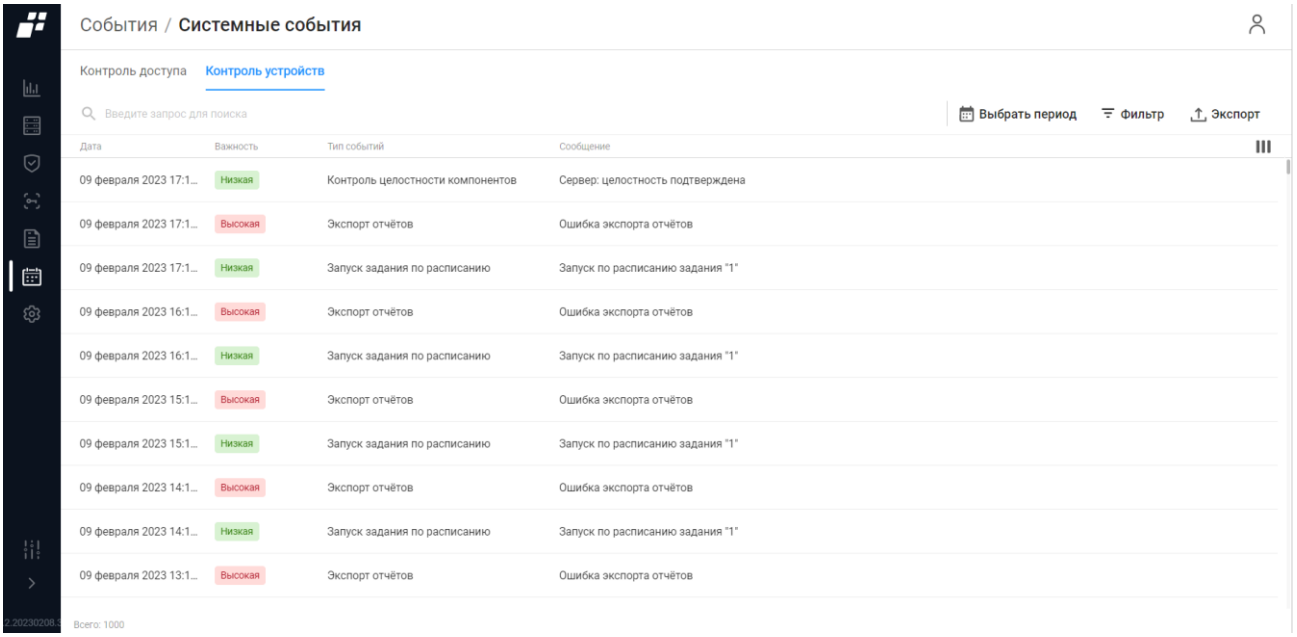


Рисунок 67 – Вкладка «Контроль устройств»

Для каждой записи списка отображаются следующие данные:

— дата и время фиксации события;

— уровень значимости события:

- «Высокое»;
- «Среднее»;
- «Низкое».

— тип события;

— сообщение – краткое описание события.

Над списком событий располагаются:

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

— кнопка «Колонки» ( ) для изменения отображения колонок на странице;

— кнопка «Выбрать период» (Выбрать период) для фильтрации событий по заданному периоду;

— кнопка «Фильтр» (Фильтр) для фильтрации событий по заданным параметрам;

— кнопка «Экспорт» (Экспорт) для экспорта журнала событий в формате csv и xlsx.

8.7 Фильтрация событий

Фильтрация событий осуществляется двумя способами.

Способ 1:

1) Нажать на кнопку «Выбрать период» (Выбрать период)».
2) Заполнить временной отрезок в появившемся окне.
3) Нажать кнопку «Применить».

Окно фильтрации закроется, на странице отобразятся записи с событиями, соответствующими заданным параметрам фильтрации. Для отмены заданных правил фильтрации и отображения в списке всех записей необходимо повторно нажать на кнопку «Выбрать период» и нажать кнопку «Сбросить».

Способ 2:

1) Нажать на кнопку «Фильтр» (Фильтр).
2) Заполнить параметры фильтрации.
3) Нажать кнопку «Применить»

Окно фильтрации закроется, на странице отобразятся записи с событиями, соответствующими заданным параметрам фильтрации. Для отмены заданных правил фильтрации и отображения в списке всех записей необходимо повторно нажать на кнопку «Фильтр» и нажать кнопку «Сбросить».

8.8 Экспорт журналов в формате CSV и XLSX

В ПК «Efros DO» реализована функция выгрузки записей из журналов событий в файлы формата CSV и XLSX. Для выгрузки записей необходимо:

1) Перейти на нужный подраздел раздела «События».
2) Выбрать вкладку, данные которой необходимо выгрузить.
3) Выполнить, при необходимости, поиск и фильтрацию данных журнала.
4) Нажать над таблицей журнала кнопку «Экспорт» (Экспорт). Откроется окно настройки параметров выгрузки, приведенное на рис. 68.

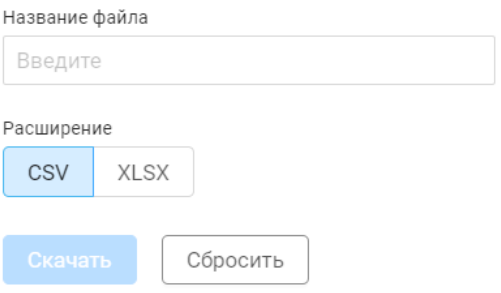


Рисунок 68 – Окно настройки параметров выгрузки

5) Ввести название файла, который будет сформирован в результате выгрузки.
6) Указать установкой переключателя формат файла.
7) Нажать кнопку «Скачать».

После завершения процесса выгрузки записей файл сохранится на локальном ПК, в верхней части страницы отобразится сообщение «Файл <имя файла> успешно создан и экспортирован».

В файл выгружаются данные всех колонок вкладки, с учетом поиска и фильтрации.

9 Раздел «Администрирование»

Отображаемые данные и доступная функциональность раздела «Администрирование» зависят от наличия хотя бы одной лицензии.

Для работы необходимо перейти в раздел «Администрирование», далее подраздел «Пользователи» или, если панель свернута, нажать на пиктограмму «⚙», панель автоматически раскроется и отобразятся все разделы (рис. 69).

9.1 Пользователи

В ПК «Efros DO» выделяются следующие роли:

- пользователи (администраторы) ПК «Efros DO»;
- пользователи (администраторы) ОЗ;
- пользователи сервисов (сетевые пользователи), предоставляемых ОЗ (контролируемыми устройствами) (более подробно описано в документе «Руководство пользователя. Часть 3. Контроль доступа»).

В данном подразделе описывается процесс создания/редактирования/удаления пользователей/групп пользователей ПК «Efros DO» и пользователей ОЗ.

Страница содержит вкладки:

- «Пользователи» – содержит пользователей и группы пользователей, зарегистрированных в комплексе. Вкладка активна по умолчанию;
- «Роли» – содержит список ролей для реализации ролевого метода управления доступом к комплексу;
- «Настройки безопасности» – содержит параметры для настройки парольной политики.

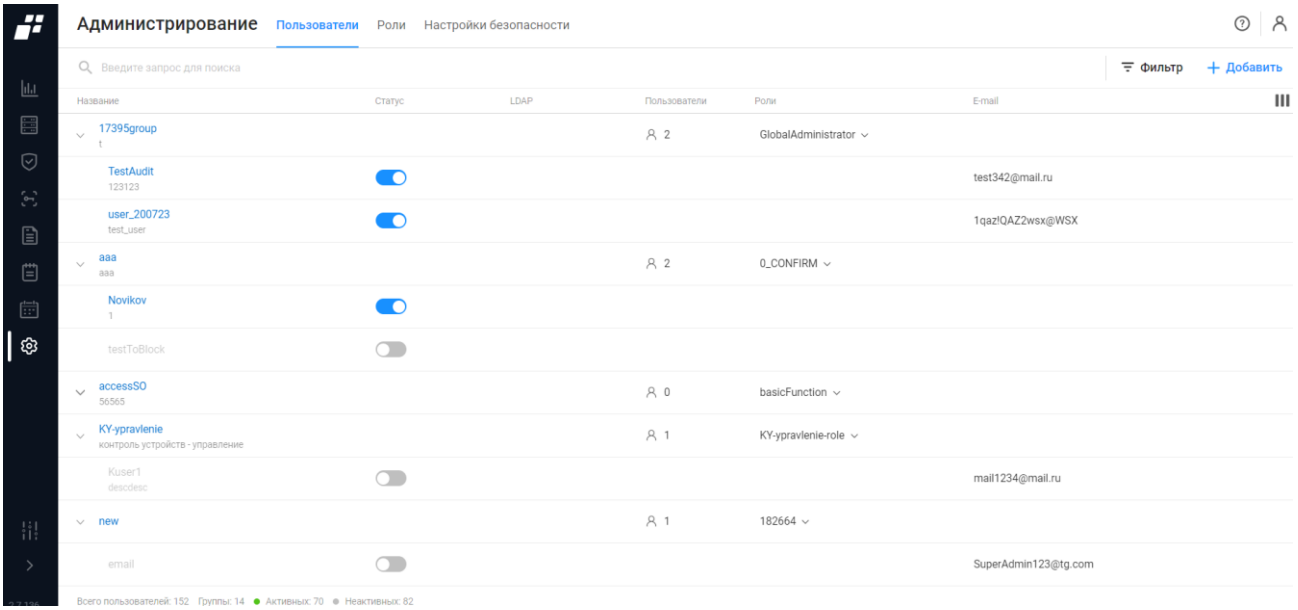


Рисунок 69 – Раздел «Администрирование»

9.1.1 Вкладка «Пользователи»

На странице список пользователей и групп пользователей реализован в виде таблицы. Для каждой записи списка отображаются следующие данные:

- название – имя пользователя/группы пользователей в ПК «Efros DO». Является ссылкой, при переходе по которой открывается окно для редактирования данных пользователя/группы пользователей;
- статус (у группы пользователей отсутствует). Переключатель:
  - « » – пользователь активен;
  - « » – пользователь неактивен.
- LDAP – служба каталогов, из которой был добавлен пользователь (у группы пользователей отсутствует);
- количество пользователей, входящих в группу;
- количество ролей, назначенных пользователю. Является раскрывающимся списком с перечнем привилегий;
- почтовый адрес пользователя, привязанный к аккаунту в ПК «Efros DO».

Над списком с пользователями и группами пользователей располагаются:

- поле поиска (Введите запрос для поиска) для поиска искомой записи в списке;
- кнопка «Фильтр» (Фильтр) для фильтрации списка пользователей;
- кнопка «Добавить (Добавить) позволяет добавить нового пользователя или

группу пользователей;

— кнопка «Колонки» ( ) для изменения отображения колонок на странице.

При выборе строки с необходимым пользователем в правом углу строки появляются следующие кнопки:

— кнопка «Изменить пароль» ( ) позволяет сменить пароль пользователю;

— кнопка «Удалить» ( ) позволяет удалить выбранного пользователя.

В нижней части страницы отображается информация об общем количестве пользователей, о количестве групп пользователей, количество активных и неактивных пользователей.

9.1.1.1 Создание пользователя

Для создания пользователя необходимо выполнить следующие действия:

1) Нажать на странице «Пользователи» кнопку «Добавить» (Добавить).
2) Из раскрывающегося списка выбрать «Пользователь» (рис. 70).

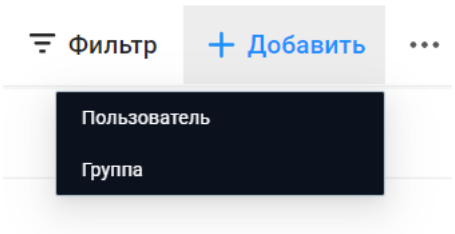


Рисунок 70 – Создание пользователя

3) Откроется страница «Создание пользователя» (рис. 71). Состав и описание полей страницы приведены в таблице 34.

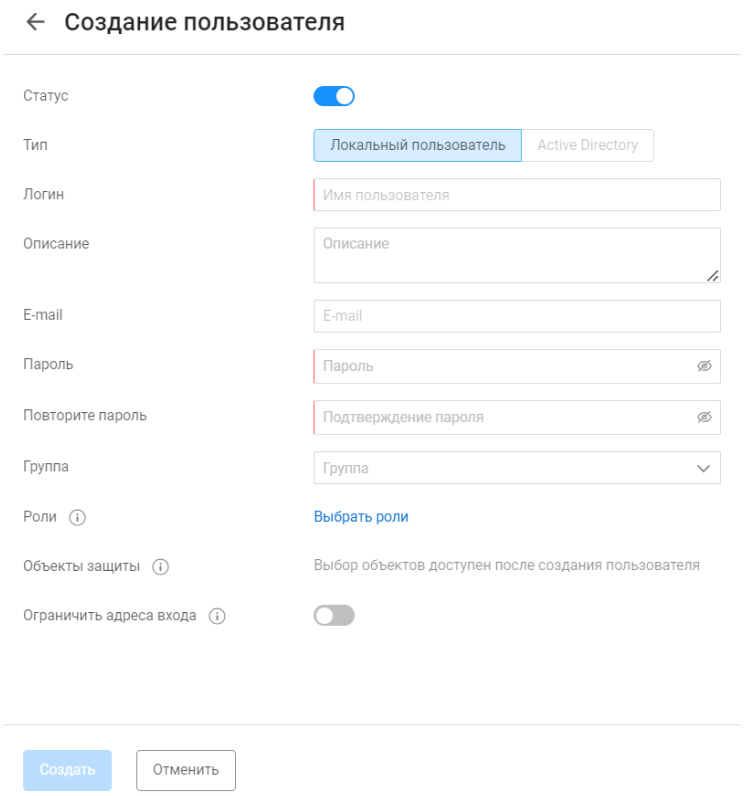


Рисунок 71 – Страница «Создание пользователя»

Таблица 34 – Состав и описание полей страницы создания пользователей

Поле	Описание
Поле «Статус»	Переключатель: — «Активен» ( ) – пользователю разрешена авторизация в комплексе; — «Неактивен» ( ) – пользователю запрещена авторизация в комплексе. По умолчанию переключатель установлен в положение «Активен»
Поле «Тип»	Поле со списком для выбора типа добавляемого пользователя. Содержит значения: «Локальный пользователь»[5]. Тип пользователя «Active Directory» недоступен
Поле «Логин»	Текстовое поле для ввода логина пользователя. Параметры ввода текста: от 1 до 32 символов. Дополнительные символы: буквы латинского алфавита, цифры, «_», «–»
Поле «Описание»	Текстовое поле для ввода логина пользователя.

[5] Создание доменного пользователя с ролью «GlobalAdministrator» (доступны все привилегии) запрещено

Поле	Описание
	Параметры ввода текста: от 1 до 250 любых символов
Поле «Email»	В поле указывается почтовый адрес пользователя для привязки к почте аккаунта пользователя ПК
Поле «Пароль»	Текстовое поле для ввода пароля пользователя. Пароль должен соответствовать требованиям, заданным при настройке парольной политики, подробное описание приведено в п. 9.1.3 При вводе символы пароля заменяются знаком «●». Для просмотра введенного значения необходимо нажать в поле ввода кнопку «Просмотреть» ( )
Поле «Повторите пароль»	Текстовое поле для повторного ввода пароля пользователя. При вводе символы пароля заменяются знаком «●». Для просмотра введенного значения необходимо нажать в поле ввода кнопку «Просмотреть» ( )
Поле «Группа»	Выбрать в раскрывающемся списке групп пользователей наименование требуемой группы
Поле «Роли»	Является ссылкой. Позволяет выбрать в окне «Выбор ролей» необходимую роль для пользователя (для доступа к различным разделам комплекса)
Поле «Объекты защиты»	Поле доступно только после создания пользователя
Переключатель «Ограничить адреса входа»	Ограничение возможности подключения пользователя к серверу «ПК Efros DO» только с указанных адресов. При вхождении пользователя в группу, действуют ограничения группы
Элементы управления	
Создать	При нажатии на кнопку окно создания пользователя закрывается, пользователь отображается в списке
Отменить	При нажатии на кнопку окно создания пользователя закрывается без сохранения данных

4) Заполнить форму необходимыми параметрами.
5) Нажать кнопку «Создать».

Автоматически запускается процесс проверки заполненности всех обязательных полей и уникальности добавляемого пользователя по имени.

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

9.1.1.2 Создание группы пользователей

При включении пользователя в какую–либо группу его привилегии замещаются на привилегии, присвоенные группе. Пользователь может входить только в одну группу.

Для создания группы пользователей необходимо выполнить следующие действия:

1) Нажать на кнопку «Добавить» (+ Добавить).
2) Из раскрывающегося списка выбрать «Группу» (рис. 70).
3) Откроется страница «Создание группы» (рис. 72). Состав и описание полей страницы приведены в таблице кнопку «Создать».
4) Таблица 35.
5) Заполнить форму необходимыми параметрами.

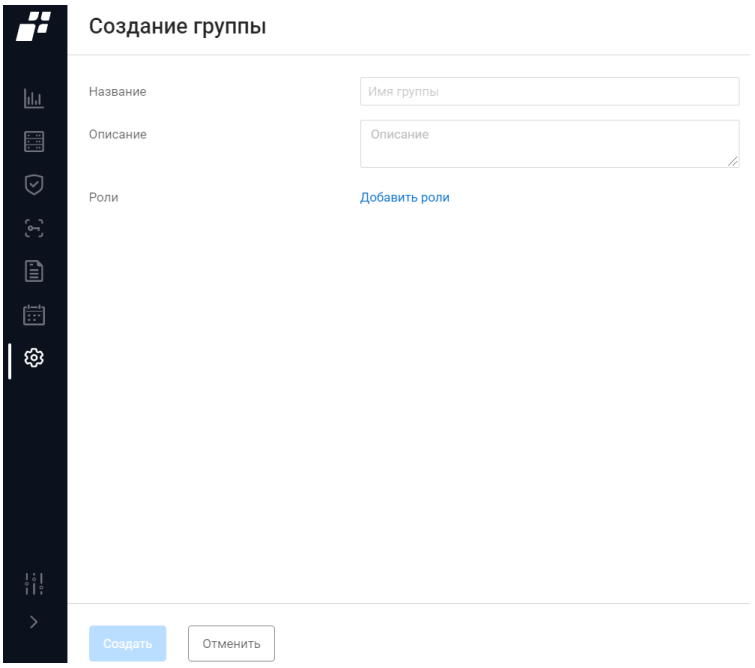


Рисунок 72 – Страница «Создание группы»

6) Нажать кнопку «Создать».

Таблица 35 – Состав и описание полей страницы создания группы пользователей

Поле	Описание
Поле «Название»	Текстовое поле для ввода названия группы. Параметры ввода текста: от 1 до 50 символов. Дополнительные символы: буквы латинского алфавита, цифры, «_», «–»
Поле «Описание»	Текстовое поле для ввода описания группы пользователей. Параметры ввода текста: от 1 до 250 любых символов
Поле «Роли»	Является ссылкой. Позволяет выбрать в окне «Выбор ролей»

Поле	Описание
	необходимую роль для группы пользователей (для доступа к различным разделам комплекса)
Поле «Объекты защиты»	Поле доступно только после создания пользователя
Переключатель «Ограничить адреса входа»	Ограничение возможности подключения пользователя к серверу «ПК Efros DO» только с указанных адресов
Элементы управления	
Создать	При нажатии кнопки выполняется переход на страницу списка пользователей с сохранением внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу списка пользователей без сохранения внесенных данных

Автоматически запускается процесс проверки заполненности всех обязательных полей и уникальности добавляемой группы пользователей.

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

9.1.1.3 Редактирование пользователя/группы пользователей

Редактирование пользователя/группы пользователей выполняется следующим способом:

1) Пользователю необходимо кликнуть на название пользователя/группы пользователей.
2) Откроется страница редактирования. Страница содержит внесенные ранее данные.
3) Пользователю необходимо внести требуемые изменения на странице редактирования и нажать кнопку «Сохранить».

Автоматически запускается процесс проверки заполненности всех обязательных полей и уникальности редактируемого пользователя/группы пользователей.

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

9.1.1.4 Фильтрация пользователей/групп пользователей

Для фильтрации данных в таблице пользователей и групп пользователей необходимо нажать кнопку «Фильтр» (Фильтр). Откроется окно фильтрации (рис. 73). Состав и описание полей окна приведены в таблице 36.

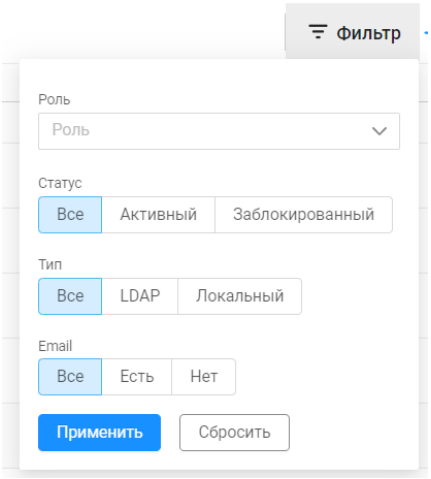


Рисунок 73 – Окно фильтрации списка пользователей

Таблица 36 – Состав и описание полей окна фильтрации пользователей

Поле	Описание
Поле «Роль»	Выбрать в раскрывающемся списке ролей необходимую роль пользователя
Поле «Статус»	Выбрать необходимый статус пользователя: — «Все» – отображаются все пользователи; — «Активный» – отображаются только активные пользователи; — «Заблокированный» – отображаются заблокированные пользователи
Поле «Тип»	Выбрать тип пользователя: — «Все» – отображаются все пользователи; — «LDAP» – отображаются пользователи, добавленные из внешних источников данных; — «Локальный» – отображаются только локальные пользователи
Поле «Email»	Выбрать по наличию у пользователей email: — «Все» – отображаются все пользователи; — «Есть» – отображаются пользователи, у которых есть email; — «Нет» – отображаются пользователи, у которых email отсутствует
Элементы управления	

Поле	Описание
Сбросить	При нажатии кнопки окно фильтрации закрывается без применения введенных настроек
Применить	При нажатии кнопки окно фильтрации закрывается, введенные настройки фильтрации применяются

Необходимо заполнить параметры фильтрации и нажать кнопку «Применить».

Отобразятся пользователи, 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».

9.1.2 Вкладка «Роли»

Данная вкладка отображает список ролей для реализации ролевого метода управления доступом к комплексу (рис. 74). Доступ к функциональности комплекса определяется наличием привилегии доступа к конкретной функции каждого подключаемого модуля.

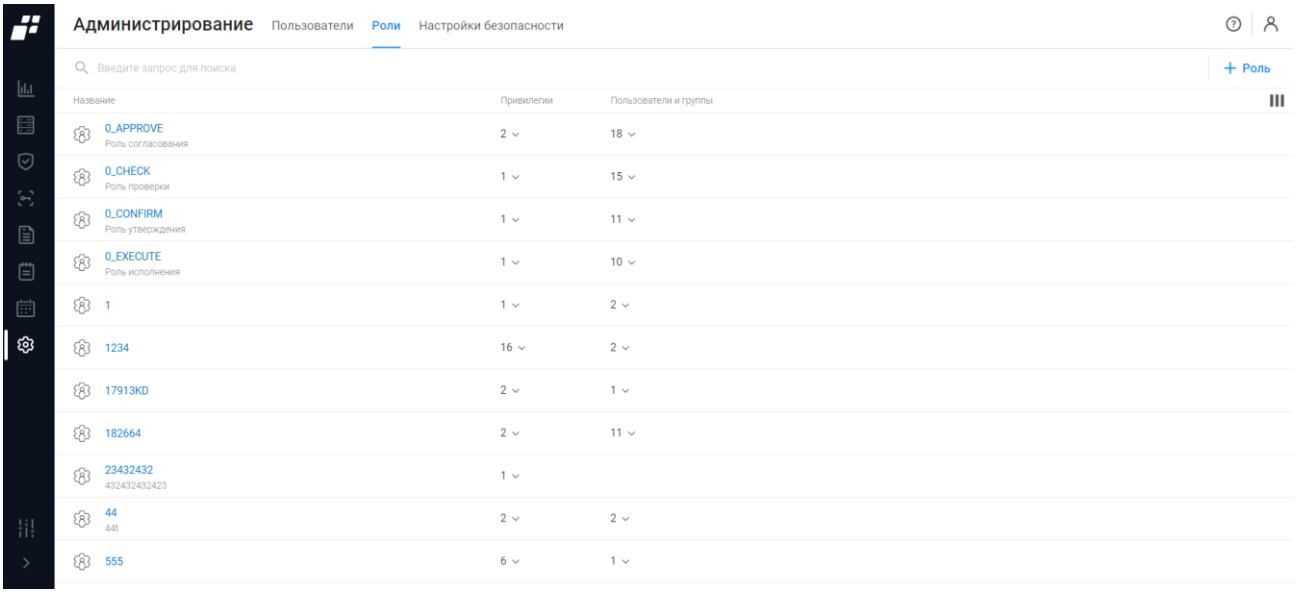


Рисунок 74 – Вкладка «Роли»

На странице список ролей реализован в виде таблицы. Для каждой записи списка отображаются следующие данные:

- иконка с обозначением роли;
- название роли. Позволяет перейти на страницу редактирования роли;
- описание роли;
- количество назначенных привилегий у каждой роли. Является раскрывающимся списком с перечнем привилегий;
- количество пользователей и групп пользователей с данной ролью.

Над списком ролей располагаются:

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

— кнопка «Роль» (+ Роль) для перехода в окно создания новой роли пользователя.

9.1.2.1 Создание роли

Для создания новой роли необходимо выполнить следующие действия:

1) Нажать на кнопку «Роль» (+ Роль).
2) Откроется страница «Создание роли пользователя» (рис. 75). Состав и описание полей страницы приведены в таблице 37.

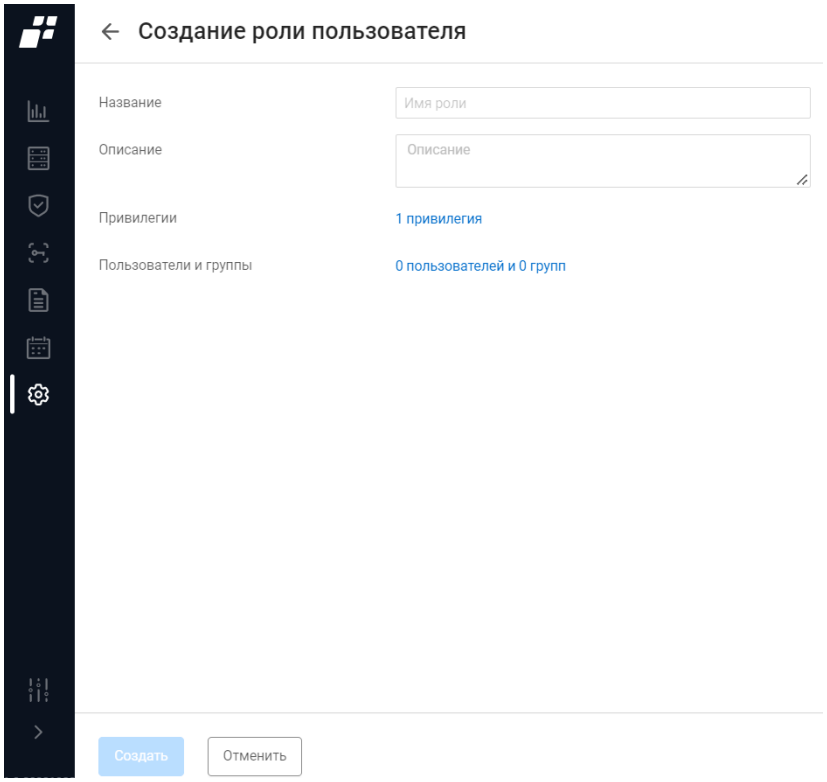


Рисунок 75 – Страница «Создание роли пользователя»

Таблица 37 – Состав и описание полей окна создания роли пользователя

Поле	Описание
Поле «Название»	Текстовое поле для ввода названия роли. Параметры ввода текста: от 1 до 50 символов. Дополнительные символы: буквы латинского алфавита, цифры, «_», «–»
Поле «Описание»	Текстовое поле для ввода описания роли. Параметры ввода текста: от 1 до 250 любых символов
Поле «Привилегии»	По умолчанию поле содержит 1 привилегию (Основные функции). Для добавления новых привилегий необходимо

Поле	Описание
	нажать на ссылку и перейти в окно выбора одной или нескольких привилегий. Далее назначить необходимые привилегии и, определив уровень доступа к выбранной привилегии, нажать кнопку «Выбрать»
Поле «Пользователи и группы»	По умолчанию поле содержит ссылку на пользователей и группы пользователей, которые зарегистрированы в комплексе. При необходимости выбрать пользователей и группы пользователей, которым будет назначена новая роль и нажать кнопку «Выбрать»
Элементы управления	
Создать	При нажатии кнопки выполняется переход на страницу списка ролей с сохранением внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу списка ролей без сохранения внесенных данных

3) Заполнить поля страницы соответствующими данными.
4) Нажать кнопку «Создать».

Автоматически запускается процесс проверки заполненности всех обязательных полей и уникальности создаваемой роли.

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

9.1.2.2 Редактирование роли

Редактирование роли выполняется следующим способом[6]:

1) Пользователю необходимо кликнуть на название роли.
2) Откроется страница редактирования роли. Страница содержит внесенные ранее данные.
3) Пользователю необходимо внести требуемые изменения на странице редактирования и нажать кнопку «Сохранить».

Автоматически запускается процесс проверки заполненности всех обязательных полей и уникальности редактируемой роли.

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

[6] Роль «GlobalAdministrator» для редактирования недоступна

9.1.3 Вкладка «Настройки безопасности»

Для настройки парольной политики необходимо перейти на вкладку «Настройки безопасности» (рис. 76).

Состав и описание полей страницы приведены в таблице 38.

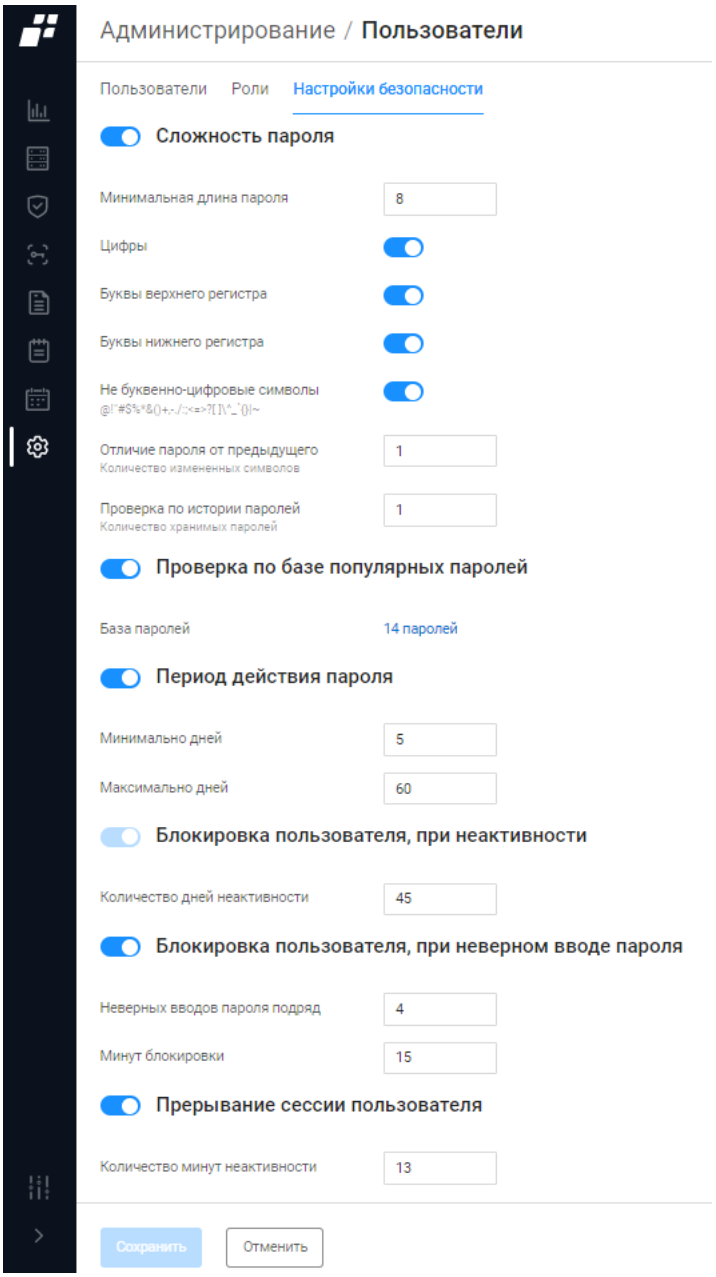


Рисунок 76 – Вкладка «Настройки безопасности»

Таблица 38 – Состав и описание полей вкладки «Настройки безопасности»

Поле	Описание
Группа полей «Сложность пароля»	
Поле «Минимальная длина пароля»	Числовое поле для ввода минимально допустимой длины пароля. Допустимые значения: от 8 до 30.

Поле	Описание
	Значение по умолчанию – 8
Поле «Цифры»	Переключатель с двумя положениями: — «Да» ( ) – пароль должен содержать хотя бы одну цифру; — «Нет» ( ) – наличие в пароле цифр необязательно По умолчанию переключатель установлен в положение «Нет» ( )
Поле «Буквы верхнего регистра»	Переключатель с двумя положениями: — «Да» ( ) – пароль должен содержать хотя бы одну букву верхнего регистра латинского алфавита; — «Нет» ( ) – наличие в пароле букв верхнего регистра необязательно. По умолчанию переключатель установлен в положение «Нет» ( )
Поле «Буквы нижнего регистра»	Переключатель с двумя положениями: — «Да» ( ) – пароль должен содержать хотя бы одну букву нижнего регистра латинского алфавита; — «Нет» ( ) – наличие в пароле букв нижнего регистра необязательно. По умолчанию переключатель установлен в положение «Нет» ( )
Поле «Не буквенно-цифровые символы»	Переключатель с двумя положениями: — «Да» ( ) – пароль должен содержать хотя бы один не буквенно–цифровой символ (@#$&%); — «Нет» ( ) – наличие в пароле не буквенно–цифровых символов необязательно. По умолчанию переключатель установлен в положение «Нет» ( )
Поле «Отличие пароля от предыдущего»	Числовое поле для ввода минимального количества символов, которые пользователь должен изменить в старом пароле при замене его на новый. Допустимые значения: от 0 до 3. Значение по умолчанию: 3

Поле	Описание
Поле «Проверка по истории паролей»	Числовое поле для ввода количества последних использовавшихся пользователем паролей. При смене пароля не допускается использование в качестве нового пароля значения, совпадающего с хранящимся в БД ПК «Efros DO». Допустимые значения: от 1 до 100. Значение по умолчанию: 5
Группа полей «Проверка по базе популярных паролей»	
Поле «База паролей»	Содержит ссылку. При переходе открывается окно со списком самых популярных паролей
Группа полей «Период действия пароля»	
Поле «Минимально дней»	Числовое поле для ввода времени (в днях) действия первого пароля пользователя (используемого им при первой авторизации в ПК «Efros DO»). После истечения указанного времени пароль необходимо изменить (пользователю при попытке запуска веб-приложения будет выведено соответствующее сообщение). Допустимые значения: от 0 до 60. Значение по умолчанию: 0
Поле «Максимально дней»	Числовое поле для ввода времени (в днях) действия пароля пользователя (второго и последующих). После истечения указанного времени пароль необходимо изменить (пользователю при попытке запуска веб-приложения будет выведено соответствующее сообщение). Допустимые значения: от 1 до 60. Значение по умолчанию: 60
Группа полей «Блокировка пользователя, при неактивности»	
Поле «Количество дней неактивности»	Числовое поле, указывающее количество дней неактивности пользователя, по истечении которых производится блокировка учетной записи пользователя. Значение по умолчанию: 45. Недоступно для корректировки
Группа полей «Блокировка пользователя, при неверном вводе пароля»	
Поле «Неверных вводов пароля подряд»	Числовое поле для ввода количества неуспешных попыток ввода пароля. После превышения указанного количества неуспешных попыток авторизации пользователь блокируется на время, указанное в параметре «Минут блокировки» (см. ниже в таблице). Допустимые значения: от 3 до 4. Значение по умолчанию: 4

Поле	Описание
Поле «Минут блокировки»	Числовое поле для ввода интервала времени (в минутах), на который блокируется учетная запись пользователя после превышения разрешенного количества неуспешных попыток авторизации. Допустимые значения: от 15 до 60 Значение по умолчанию: 15
Группа поле «Прерывание сессии пользователя»	
Поле «Количество минут неактивности»	Числовое поле для ввода интервала времени (в минутах) бездействия пользователя, после которого осуществляется блокировка веб-интерфейса с необходимостью повторной авторизации. Допустимые значения: от 10 до 30 Значение по умолчанию: 10
Элементы управления	
Сохранить	При нажатии кнопки окно настройки безопасности закрывается, введенные изменения применяются
Отменить	При нажатии кнопки окно настройки безопасности закрывается без применения изменений
При необходимости поля можно отключить, передвинув переключатель в положение « » – поле будет недоступно для внесения изменений	

1) Ввести в поля страницы требуемые значения.
2) Нажать кнопку «Сохранить». После чего введенные параметры будут сохранены в БД ПК «Efros DO» и будут применяться при авторизации пользователей и при смене пароля.

9.2 Лицензия

Данный подраздел предоставляет пользователю комплекса информацию о наличии лицензии на продукт и сроках ее действия (рис. 77).

По окончанию срока действия лицензии действия пользователя в системе блокируются. За 14 дней до даты окончания срока действия пользователь получает предупреждение в виде сообщения. Все сервисы системы по сбору и логированию информации выполняют свою работу в течение 7 дней после окончания срока действия лицензии. Если в этот период лицензия будет продлена, работа комплекса не остановится. Полная остановка работы комплекса прекращается спустя 7 дней с даты окончания действия лицензии.

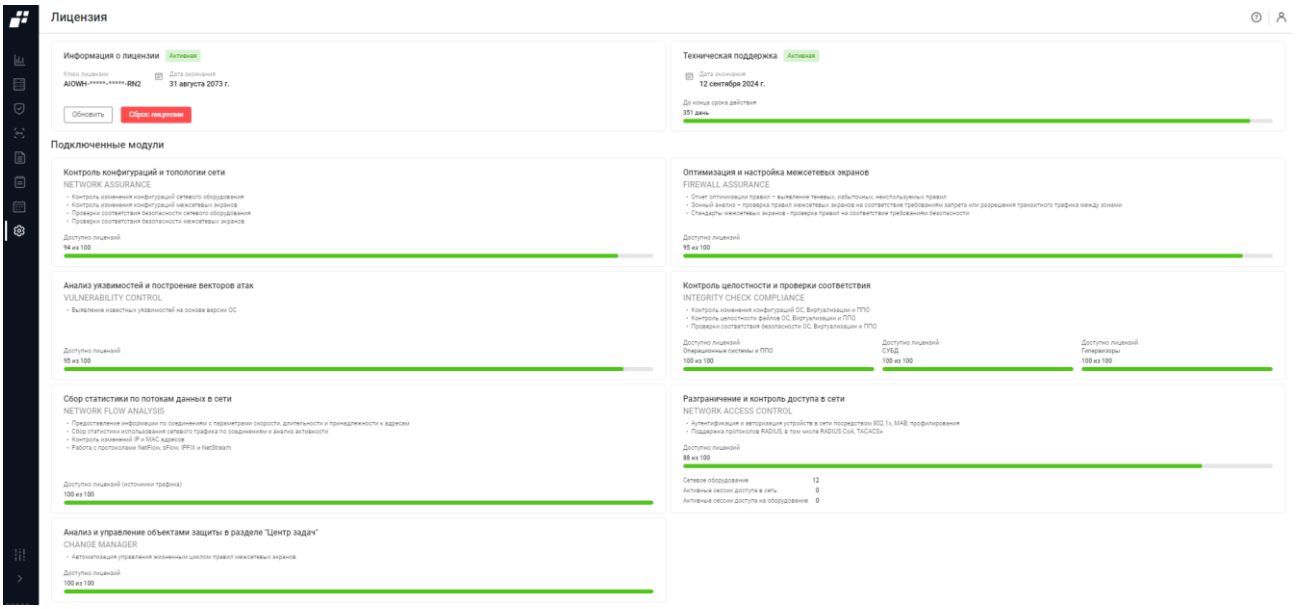


Рисунок 77 – Страница подраздела «Лицензия»

Состав и описание полей страницы подраздела «Лицензия» приведен в таблице 39.

Таблица 39 – Состав и описание полей страницы подраздела «Лицензии»

Поле	Описание
Поле «Информация о лицензии»	Содержит следующую информацию: — статус лицензии; — ключ лицензии; — дата окончания лицензии
Кнопка «Обновить»	Позволяет обновить лицензию
Кнопка «Сброс лицензии»	Позволяет сбросить лицензию
Поле «Техническая	Содержит следующую информацию:

Поле	Описание
поддержка»	— статус технической поддержки; — вид технической поддержки; — дата окончания технической поддержки; — количество оставшихся дней до окончания технической поддержки
Блок полей «Подключенные модули»	Содержит следующую информацию: — название модуля; — описание функций; — количество доступных лицензий на оборудование для каждого модуля

Подробно данный раздел рассмотрен в документе «ПК «Efros DO». Руководство администратора».

9.3 Сертификаты

Подраздел «Сертификаты» доступен пользователю для работы при наличии лицензии на функциональный модуль «Efros NAC».

Данный подраздел позволяет работать со списками SSL-сертификатов (рис. 78).

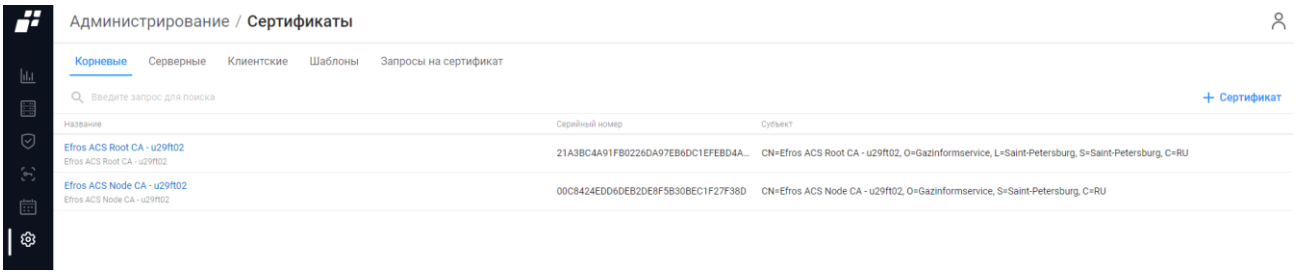


Рисунок 78 – Подраздел «Сертификаты»

Страница подраздела содержит следующие вкладки:

- «Корневые» – предназначена для ведения списка корневых сертификатов;
- «Серверные» – предназначена для ведения списка серверных сертификатов;
- «Клиентские» – предназначена для ведения списка клиентских сертификатов;
- «Шаблоны» – предназначена для ведения шаблонов клиентских сертификатов;
- «Запросы на сертификат» – предназначена для ведения списка запросов на сертификаты.

После установки ПК «Efros DO» в комплексе используются самоподписанные корневой и серверный сертификаты (далее – предустановленные сертификаты). Удаление предустановленных сертификатов пользователям комплекса недоступно.

9.3.1 Вкладка «Корневые»

Корневые сертификаты – это сертификаты, которые используются для подтверждения серверных сертификатов и выпуска клиентских сертификатов.

На странице список сертификатов реализован в виде таблицы (см. рис. 78). Для каждой записи списка отображаются следующие данные:

- название сертификата, присвоенное при импортировании;
- серийный номер, присвоенный центром сертификации;
- параметры сертификата, указанные в самом сертификате.

Над таблицей списка корневых сертификатов располагаются:

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

— кнопка «Сертификат» () для поиска искомой записи в списке;

— кнопка «Колонки» () для изменения отображения колонок на странице.

При наведении курсора на строку сертификата, в правой части строки появляются следующие элементы:

— кнопка «Удалить» (), отображается при наведении курсора на название сертификата;

— кнопка «Экспортировать» () для экспорта сертификата.

9.3.1.1 Ведение списка корневых сертификатов

Для добавления корневого сертификата пользователю необходимо:

1) Нажать кнопку «Сертификат» ().
2) Откроется окно «Создание корневого сертификата» (рис. 79).

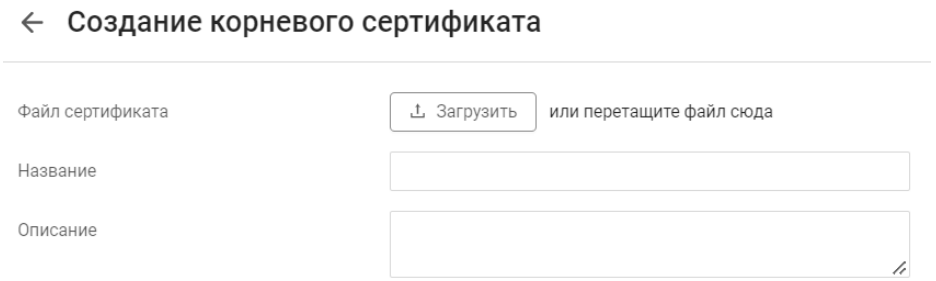


Рисунок 79 – Страница «Создание корневого сертификата»

3) Выбрать файл с добавляемым сертификатом, для чего:
— нажать кнопку «Загрузить»;
— выбрать в стандартном окне ОС файл сертификата.
4) Ввести в полях «Название» и «Описание» соответствующие данные сертификата.
5) Нажать кнопку «Создать». Окно закроется и в таблице добавится строка с данными нового сертификата.

Пользователь с соответствующей привилегией имеет возможность просмотреть данные сертификата и изменить название и описание, для чего необходимо:

1) Нажать на название сертификата.
2) В открывшемся окне (рис. 80):
— просмотреть данные сертификата;
— внести требуемые изменения и нажать кнопку «Сохранить». Окно «Редактирование корневого сертификата» закроется, внесенные изменения

будут сохранены.

Предустановленные корневые сертификаты недоступны для удаления внесения изменений.

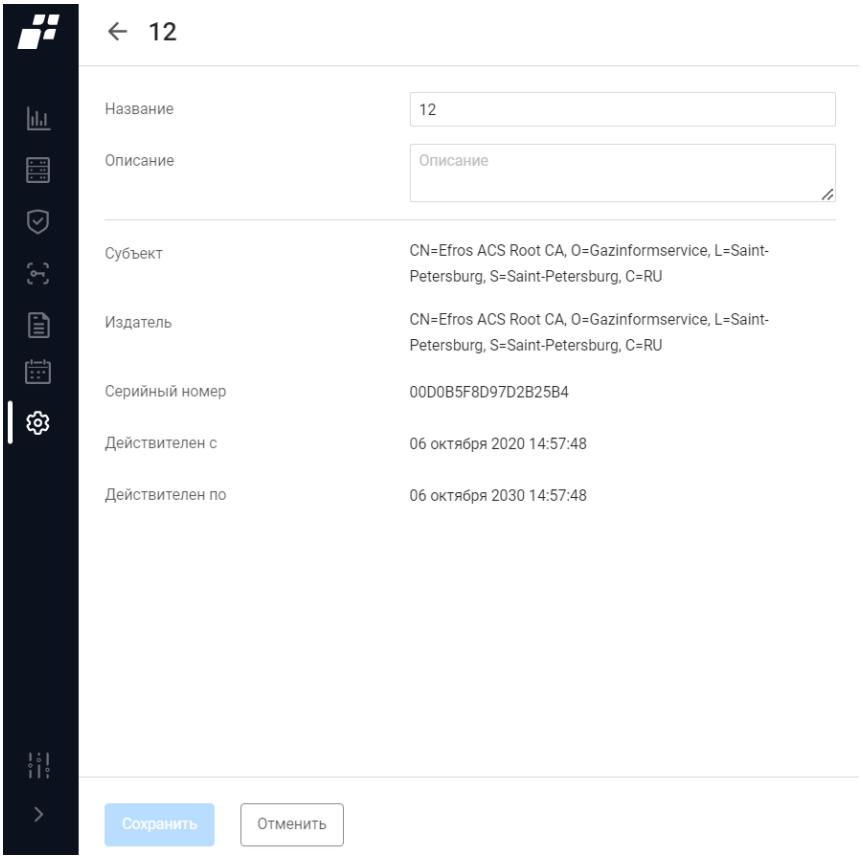


Рисунок 80 – Окно «Редактирование корневого сертификата»

Кроме того, пользователь имеет возможность экспортировать пользовательский корневой сертификат на локальную ЭВМ, для чего необходимо нажать в строке требуемого сертификата кнопку «Экспортировать» ( ).

9.3.2 Вкладка «Серверные»

Серверные сертификаты применяются для безопасной работы с веб-приложением ПК «Efros DO» по HTTPS и для аутентификации пользователей и устройств по EAP.

Серверные сертификаты генерируются либо пользователем ПК «Efros DO» на основе уже имеющегося корневого сертификата и запроса на сертификат, либо генерируются удостоверяющим центром и импортируются в комплекс.

Самоподписной серверный сертификат, который предустановлен в ПК «Efros DO», связан с соответствующим корневым сертификатом.

На странице список сертификатов реализован в виде таблицы (рис. 81).

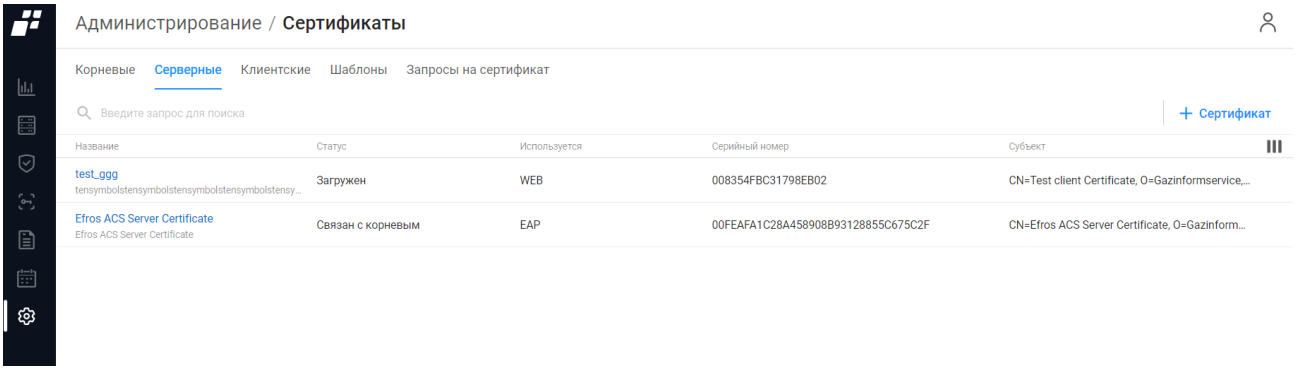


Рисунок 81 – Вкладка «Серверные»

Для каждой записи списка отображаются следующие данные:

— название сертификата, присвоенное при импортировании;

— статус сертификата:

- «Загружен», но не найден связанный с ним корневой сертификат;
- «Связан с корневым» – есть связанный с серверным сертификатом корневой сертификат.

— использование сертификата:

- «WEB» – сертификат используется для установки доверенного соединения при доступе к веб-приложению ПК «Efros DO»;
- «EAP» – сертификат используется для установки доверенного соединения при доступе к АСО.

— серийный номер, присвоенный центром сертификации;

— данные субъекта сертификата.

Над таблицей списка серверных сертификатов располагаются:

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

— кнопка «Сертификат» (+ Сертификат) для перехода в окно создания нового корневого сертификата;

— кнопка «Колонки» ( ) для изменения отображения колонок на странице.

При наведении курсора на строку сертификата, в правой части строки появляется кнопка «Удалить» ( ) для удаления сертификата.

9.3.2.1 Ведение списка серверных сертификатов

Добавление серверных сертификатов выполняется автоматически после привязки к запросу сертификата, полученного от центра сертификации (см. п. 9.3.5), либо путем импорта уже имеющегося в организации серверного сертификата в БД комплекса.

Создание серверного сертификата выполняется аналогично созданию корневых сертификатов (см. п.п. 9.3.1.1), за исключением того, что в окне «Создание серверного

сертификата» (рис. 82):

1) Выбирается не только файл сертификата, но и файл закрытого ключа для сертификата.
2) При необходимости указывается, что сертификат используется для веб-приложения.

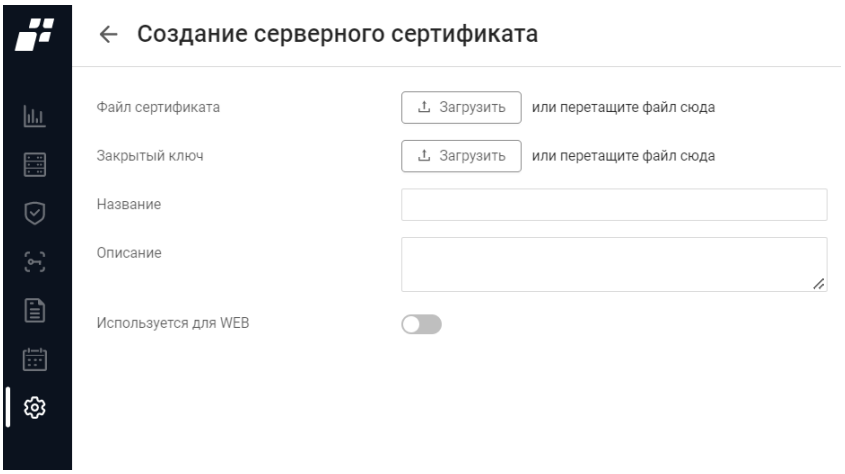


Рисунок 82 – Страница «Создание серверного сертификата»

Пользователь с соответствующей привилегией имеет возможность просмотреть данные сертификата и внести изменения в его параметры (название, описание, тип использования), для чего необходимо:

1) Выбрать в строке требуемого сертификата его название. Откроется окно «Редактирование серверного сертификата» (рис. 83).
2) Внести требуемые изменения в название и/или описание сертификата.
3) Установкой/отменой установки флага в поле группы «Используется для WEB».
4) Нажать кнопку «Сохранить». Внесенные изменения будут сохранены.

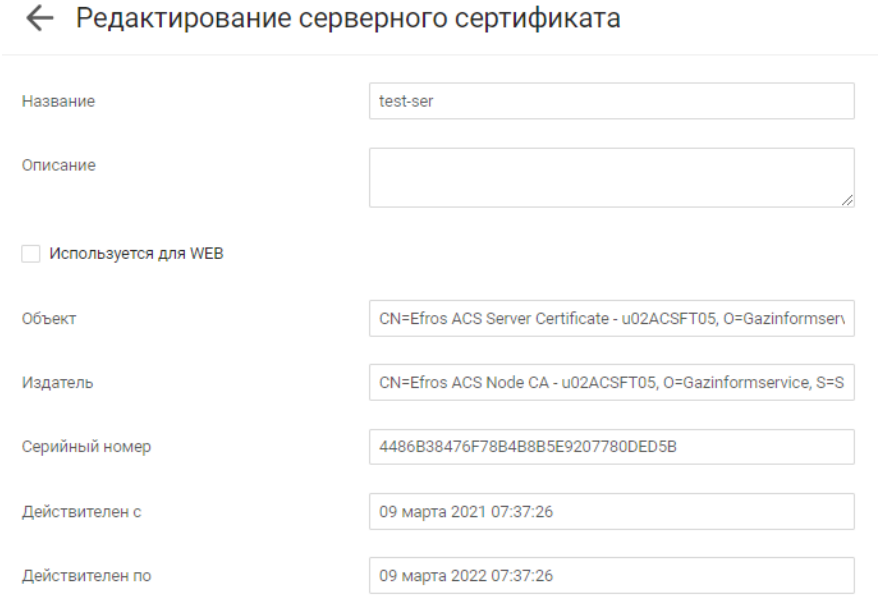


Рисунок 83 – Окно «Редактирование серверного сертификата»

Предустановленные серверные сертификаты недоступны для удаления и внесения изменений.

9.3.3 Вкладка «Клиентские»

После установки ПК «Efros DO» список клиентских сертификатов пуст, на странице отображается сообщение «Список пуст. Вы можете создать сертификат при помощи кнопки ниже» и кнопка «Создать» для перехода на страницу создания нового клиентского сертификата.

На странице список сертификатов реализован в виде таблицы (рис. 84).

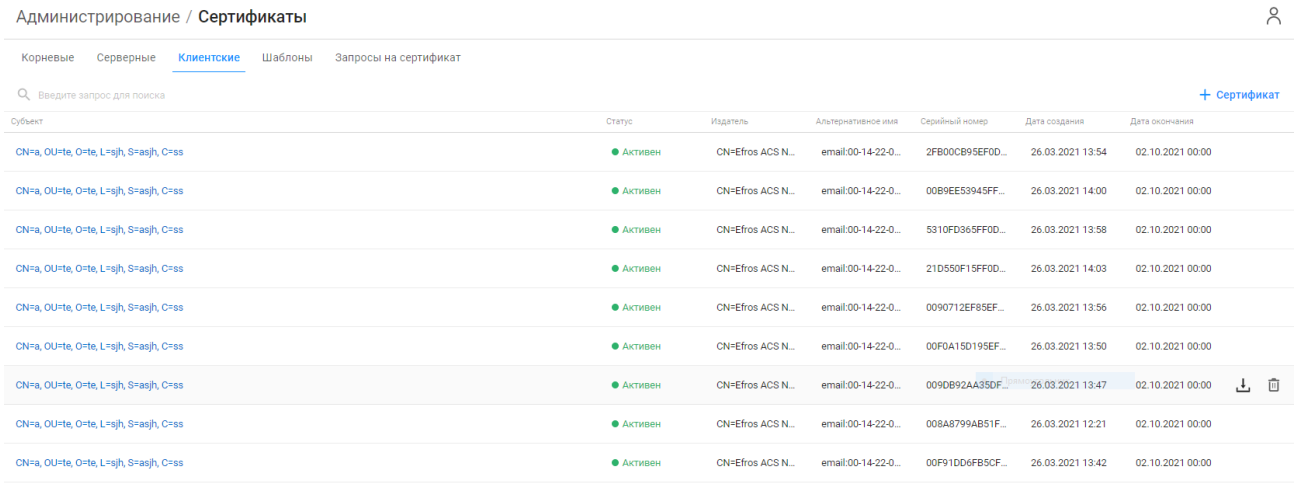


Рисунок 84 – Вкладка «Клиентские»

Для каждой записи списка отображаются следующие данные:

- данные субъекта сертификата;
- статус сертификата:
  - «Активен» (●) – сертификат действует;
  - «Отозван» (●) – сертификат отозван.
- данные издателя сертификата;
- альтернативное имя;
- серийный номер, присвоенный сертификату при его генерации в ПК;
- дата создания сертификата;
- дата окончания срока действия сертификата.

Над списком клиентских сертификатов располагаются:

- поле поиска (Введите запрос для поиска) для поиска искомой записи в списке;
- кнопка «Сертификат» (+ Сертификат) для перехода в окно создания нового

корневого сертификата;

— кнопка «Колонки» ( ) для изменения отображения колонок на странице.

При наведении курсора на строку сертификата, в правой части строки появляются следующие элементы:

— кнопка «Экспортировать» ( ) – для экспорта сертификата;

— кнопка «Отозвать» ( ) – для отзыва клиентского сертификата.

9.3.3.1 Ведение списка клиентских сертификатов

Для успешного создания клиентского сертификата необходимо создать шаблоны. Более подробно описано в п. 9.3.4.

Для выпуска клиентских сертификатов необходимо:

1) Нажать кнопку «Сертификат» (+ Сертификат) над таблицей клиентских сертификатов.
2) Откроется окно создания нового клиентского сертификата (рис. 85).

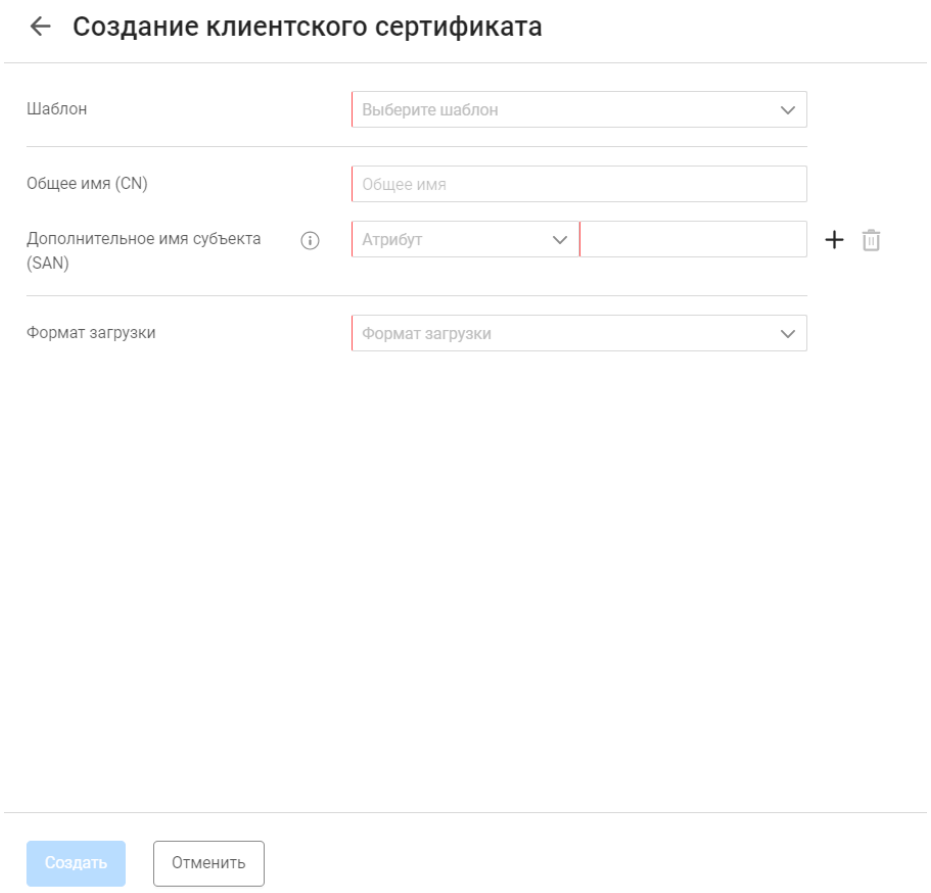


Рисунок 85 – Страница «Создание клиентского сертификата»

3) Выбрать в поле «Шаблон» название требуемого шаблона.

4) Если в выбранном шаблоне заполнено поле «Общее имя (CN)», то это значение отобразится в поле «Общее имя (CN)» формы выпуска сертификата, иначе – заполнить поле вручную.
5) Указать дополнительное имя (одно или несколько) субъекта, для чего в поле «Дополнительное имя субъекта (SAN)»:
— выбрать в поле «Атрибут» параметр: «MAC-адрес», «Имя участника-пользователя», «DNS»;
— ввести проверяемое при проверке сертификата значение параметра;
— в автоматически добавленной строке группы указать тип и значение второго дополнительного имени при необходимости;
— повторить действия по добавлению для всех требуемых параметров;
— при необходимости, удалить ошибочно добавленные параметры, нажав соответствующие им кнопки «Удалить» ( ).
6) Выбрать один из форматов загрузки:
— «Сертификат в PEM формате, Ключ в PKCS8 PEM формате» – будет выгружен следующий состав файлов: «ca.pem», «client.key», «client.pem»;
— «Сертификат и ключ в файле PKCS12 формата» – будет выгружен следующий состав файлов: «ca.pem», «client.key», «client.p12».

Выбор формата загрузки определяется требованиями ПО, установленного на клиентской ЭВМ, для экспорта клиентского сертификата и публичной части корневого сертификата. Например, IIS принимает сертификаты в формате PKCS12, файл «client.p12» содержит в себе сам клиентский сертификат и закрытый ключ сертификата, файл «ca.pem» является файлом-контейнером, который хранит в себе открытую, публичную часть корневого сертификата.

7) Нажать кнопку «Создать».

Будет запущен процесс генерации архива с сертификатом и ключом. По окончанию процесса отобразится соответствующее сообщение.
Выпущенный сертификат будет внесен в список клиентских сертификатов и будет доступен пользователю для отзыва и удаления. В разделе «События» будет внесено сообщение о генерации сертификата.
Полученные в результате сертификат и ключ необходимо загрузить на клиентскую ЭВМ.

9.3.4 Вкладка «Шаблоны»

После установки ПК «Efros DO» список шаблонов сертификатов пуст, на странице отображается сообщение *«Список пуст. Вы можете создать шаблон сертификата при помощи кнопки ниже»* и кнопка «Создать» для перехода на

страницу создания нового шаблона сертификата.

На странице список сертификатов реализован в виде таблицы (рис. 86).

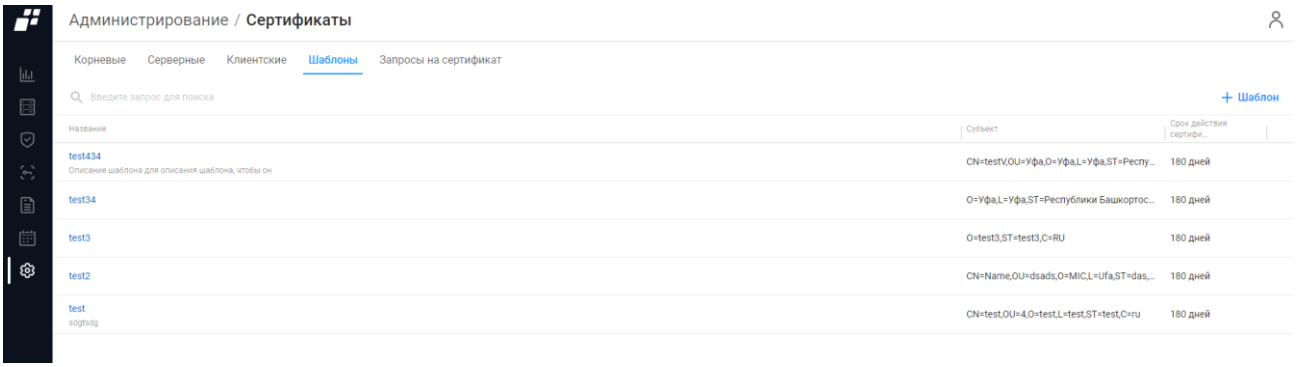


Рисунок 86 – Вкладка «Шаблоны»

Для каждой записи списка отображаются следующие данные:

- название шаблона;
- данные субъекта сертификата;
- срок действия сертификата.

Над таблицей списка шаблонов сертификатов располагаются:

- поле поиска (Введите запрос для поиска) для поиска искомой записи в списке;
- кнопка «Шаблон» (+ Шаблон) для создания шаблона сертификата;
- кнопка «Колонки» ( ) для изменения отображения колонок на странице.

При наведении курсора на строку сертификата, в правой части строки появляется кнопка «Удалить» ( ) для удаления шаблона.

9.3.4.1 Ведение списка шаблонов клиентских сертификатов

Для добавления нового шаблона клиентского сертификата необходимо:

1) Нажать на кнопку «Шаблон» (+ Шаблон).
2) Откроется страница «Создание шаблона» (рис. 87).

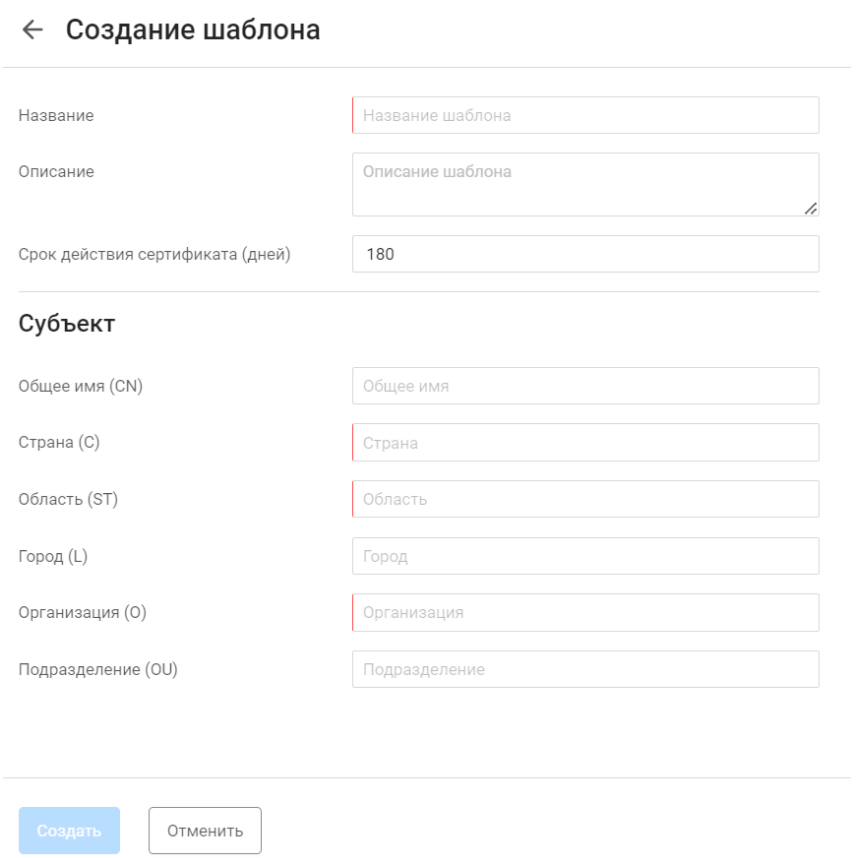


Рисунок 87 – Страница «Создание шаблона»

3) Ввести название и описание шаблона.
4) Ввести срок действия сертификата (от 180 до 3652[7] дней).
5) Заполнить поля группы «Субъект» данными клиента.
6) Нажать кнопку «Создать».

Будет запущен процесс проверки заполненности всех обязательных полей и уникальности добавляемого шаблона по названию. По окончании проверки на странице отобразится сообщение либо об ошибке, либо об успешном создании шаблона.

9.3.5 Вкладка «Запросы на сертификаты»

После установки ПК «Efros DO» список запросов на сертификат пуст, на странице отображается сообщение *«Список пуст. Вы можете создать запрос на сертификат при помощи кнопки ниже»* и кнопка «Создать» для перехода на страницу создания нового запроса.

На странице список запросов реализован в виде таблицы (рис. 88).

[7] Максимально допустимое значение 3652 дня соответствует значению – 10 лет

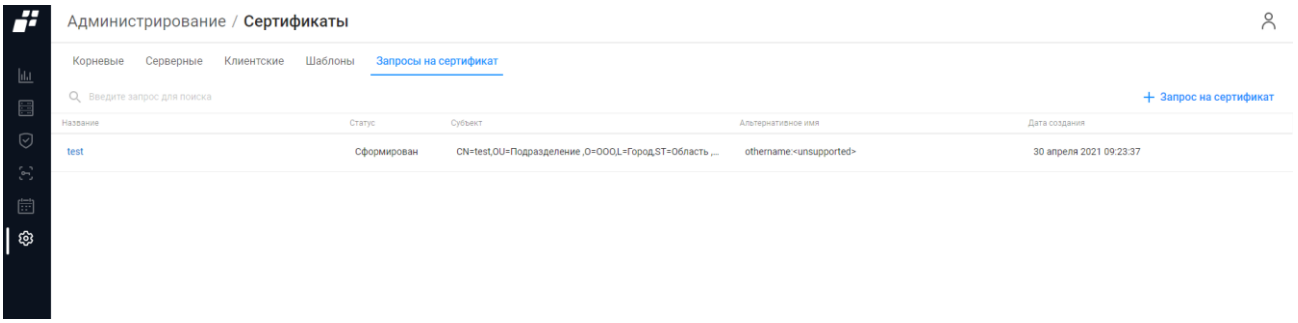


Рисунок 88 – Вкладка «Запросы на сертификат»

Для каждой записи списка отображаются следующие данные:

— название, присвоенное при создании запроса;

— статус:

- Сформирован» (после создания);
- «Подтвержден» (после привязки сформированного по запросу сертификата).

— данные субъекта сертификата;

— альтернативные параметры, указанные при формировании запроса;

— дата создания запроса на сертификат.

Над списком запросов располагаются:

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

— кнопка «Запрос на сертификат» (+ Запрос на сертификат) для создания запроса на сертификат;

— кнопка «Колонки» ( ) для изменения отображения колонок на странице.

При наведении курсора на строку сертификата, в правой части строки появляются следующие элементы:

— кнопка «Привязать» ( ) для привязывания сертификата к запросу;

— кнопка «Экспортировать» ( ) для экспорта запроса на сертификат;

— кнопка «Удалить» ( ) для удаления сертификата.

9.3.5.1 Ведение списка запросов на сертификаты

Для формирования нового запроса на сертификат необходимо:

1) Нажать кнопку «Запрос на сертификат» (+ Запрос на сертификат).
2) Откроется окно «Создание запроса на сертификат» (рис. 89).

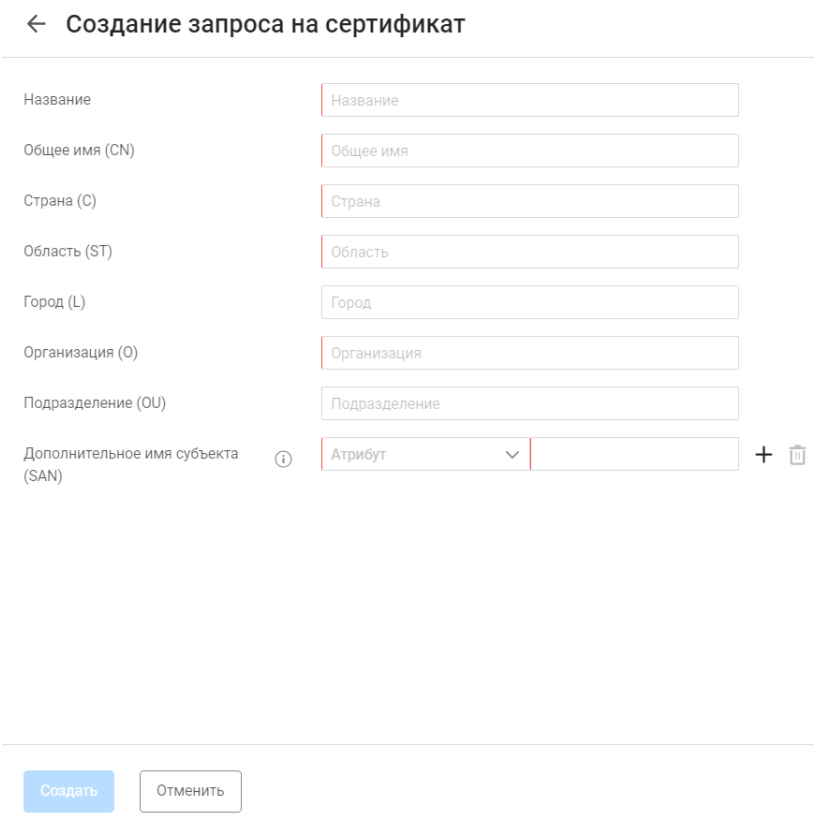


Рисунок 89 – Окно «Создание запроса на сертификат»

3) Заполнить поля необходимыми данными.
4) Нажать кнопку «Создать».

Пользователь с соответствующей привилегией имеет возможность просмотреть параметры запроса, для чего необходимо нажать в строке запроса на текст-ссылку в графе «Название». Откроется окно «Информация о запросе» (рис. 90).

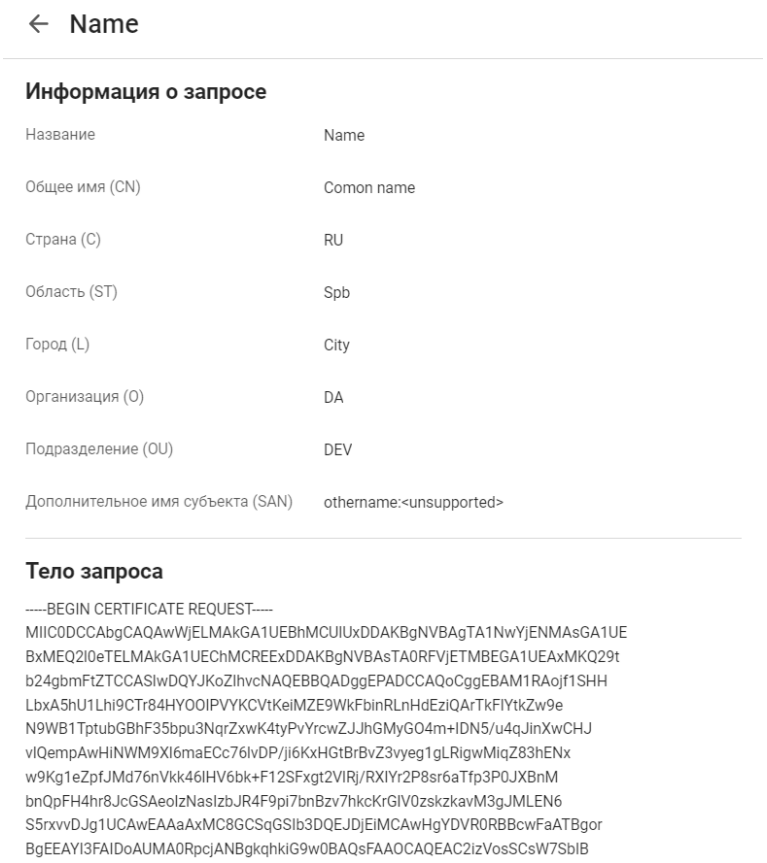


Рисунок 90 – Окно «Информация о запросе»

Для экспорта запроса на локальную ЭВМ пользователю необходимо:

1) Вернуться на вкладку «Запросы на сертификат».
2) В строке с запросом на сертификат нажать кнопку «Экспортировать» ( ). Запрос на сертификат автоматически сохранится на локальную ЭВМ.

Далее, после отправки запроса в центр сертификации и получения сертификата, пользователю необходимо привязать полученный сертификат к запросу, для чего:

1) Нажать в строке с запросом на сертификат кнопку «Привязать сертификат» ( ).
2) В открывшемся окне (рис. 91) выбрать файл сертификата, нажав кнопку «Выбрать файл» и выбрав в стандартном окне ОС требуемый файл.

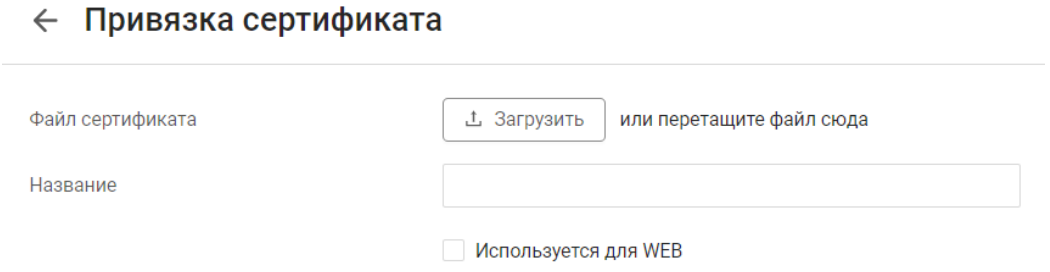


Рисунок 91 – Окно привязки сертификата к запросу

3) Ввести название сертификата, которое будет использоваться.
4) Указать, при необходимости, установкой флага в поле «Используется для WEB» использование сертификата для установки доверенного соединения при доступе к веб-приложению ПК «Efros DO».
5) Нажать кнопку «Добавить».

Окно привязки закроется, после успешного завершения проверки соответствия сертификата запросу и корректности сертификата:

- запросу будет присвоен статус «Подтвержден»;
- в окне просмотра параметров запроса добавится вкладка «Информация о сертификате» с данными прикрепленного сертификата;
- сертификат будет добавлен в список серверных сертификатов.

9.4 Планировщик

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

Пользователю разрешено создавать задачи для любого типа устройств. Запуск события/расписания возможен только при наличии установленного внешнего модуля для работы с устройством.

Предустановленные задачи, запуск которых автоматизирован:

— задачи по событию:

- восстановить пароль – отправление кода восстановления пользователю, запросившему восстановление пароля;
- оповестить об окончании расчета векторов атак;
- выполнение конфигурирования и восстановления;
- изменения контролируемых отчетов;
- ошибки конфигурирования и восстановления;
- ошибки при работе с устройством;
- первые ошибки при работе с устройством.

— задачи по расписанию:

- обновить базу уязвимостей – обновление уязвимостей для установленных модулей;
- синхронизировать с внешними источниками – периодический запуск синхронизации LDAP;
- оповестить пользователя о блокировке учетной записи;
- освободить лицензию конечных точек для повторного использования - освобождение лицензии для активных конечных точек без полученной команды остановки аудита. С момента последнего начала\обновления на конечной точке прошло времени больше значения, заданного параметром «Длительность активной сессии».

Для работы с подразделом «Планировщик» пользователю необходимо перейти в раздел «Администрирование», далее в подраздел «Планировщик» или, если панель свернута, – нажать на пиктограмму «», панель автоматически раскроется и отобразятся все разделы (рис. 92).

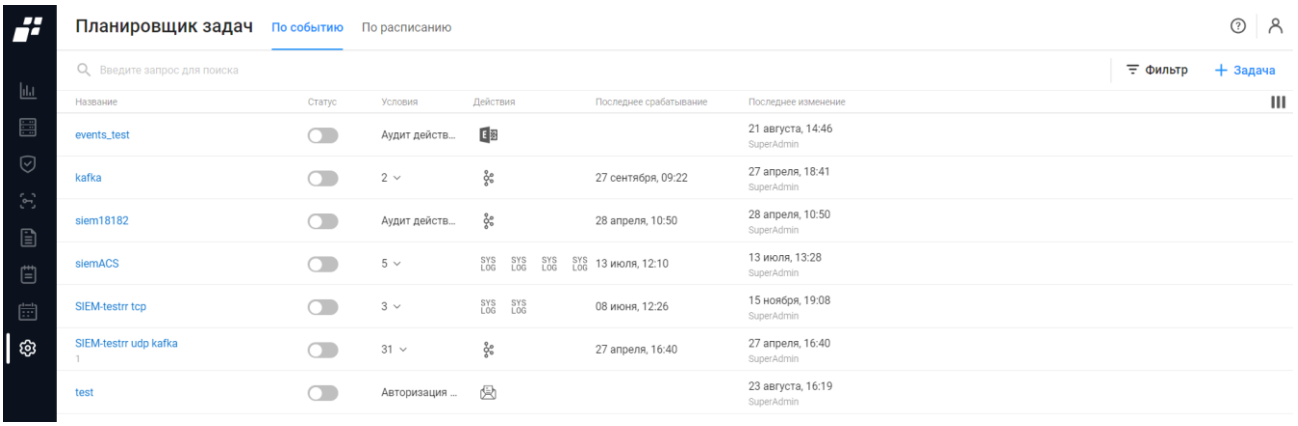


Рисунок 92 – Подраздел «Планировщик»

Страница содержит следующие вкладки:

- «По событию» – предназначена для создания триггеров (условий), которые реагируют на события, произошедшие на устройствах или в самом комплексе;
- «По расписанию» – предназначена для настройки загрузки отчетов и выполнения операций с устройствами в соответствии со своими индивидуальными условиями работы.

9.4.1 Вкладка «По событию»

На странице список задач по событию реализован в виде таблицы. Для каждой записи списка отображаются следующие данные:

- Название и описание задачи по событию. Является ссылкой. При переходе открывается окно редактирования задачи по событию;
- Состояние. Переключатель, отображает активность задачи (включен или выключен);
- Условия. Является раскрывающимся списком. Условия задаются при создании задачи;
- Действия: «Отправить сообщение» ( ), «Отправить сообщение через Exchange» ( ), «Отправить Syslog-сообщение» ( ), «Отправить в Apache Kafka» ( );
- Последнее срабатывание. Отображается ДД.ММ и ЧЧ:ММ последнего срабатывания обработчика события;
- Последнее изменение. Отображается ДД.ММ., ЧЧ:ММ и логин пользователя, совершившего последнее изменение обработчика события.

Над списком задач располагаются:

- поле поиска (Введите запрос для поиска);
- кнопка «Фильтр» (Фильтр) для фильтрации списка задач по событию;

— кнопка «Задача» (+ Задача) для создания задачи по событию;

— кнопка «Колонки» ( ) для изменения отображения колонок на странице.

При наведении курсора на строку с задачей, в правой части строки появляется кнопка «Удалить» ( ) для удаления задачи.

9.4.1.1 Создание задачи по событию

Для добавления задачи по событию необходимо выполнить следующие действия:

1) Нажать кнопку «Задача» (+ Задача).
2) В открывшемся окне «Создание задачи по событию» (рис. 93) заполнить необходимые параметры. Состав и описание полей страницы приведены в таблице 40.

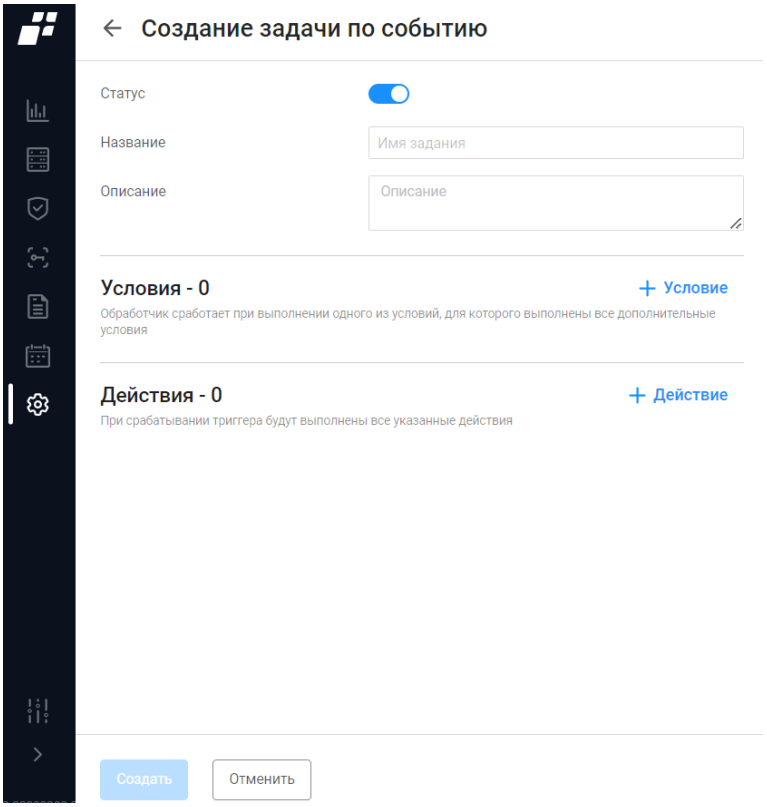


Рисунок 93 – Страница «Создание задачи по событию»

Таблица 40 – Состав и описание страницы «Создание задачи по событию»

Поле	Описание
Поле «Статус»	При установленном переключателе осуществляется обработка событий, при снятом – триггер выключен
Поле «Название»	Текстовое поле для ввода названия задачи. Параметры ввода текста: от 1 до 250 любых символов
Поле «Описание»	Текстовое поле для ввода описания задачи.

	Параметры ввода текста: от 1 до 4000 любых символов
Поле «Условия»	Выбор условий через кнопку «Условия» (+ Условие) для выполнения правил обработки событий
Поле «Действия»	Выбор типа выполняемого действия через кнопку «Действия» (+ Действие)
Элементы управления	
Создать	При нажатии кнопки выполняется переход на страницу списка задач с сохранением внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу списка задач без сохранения внесенных данных

3) В поле «Условия» нажать кнопку «Условие» (+ Условие). Из раскрывающегося списка выбрать тип события, при совершении которого ожидается реакция системы (рис. 94).

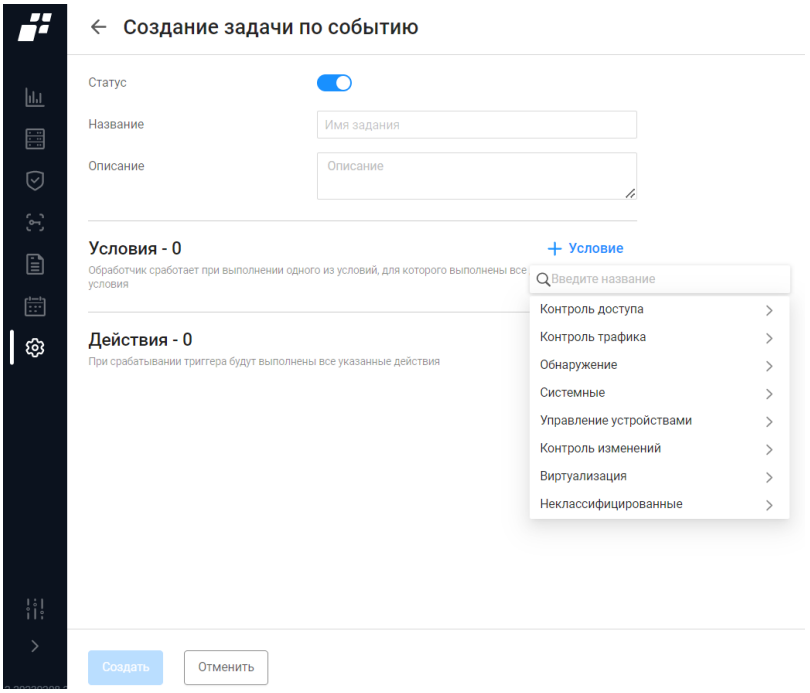


Рисунок 94 – Окно создания условий для задачи

4) Из раскрывающегося списка значений выбрать параметр события, для которого задается условие. В зависимости от вида выбранного параметра в окне отобразится ряд вариантов значений (рис. 95).

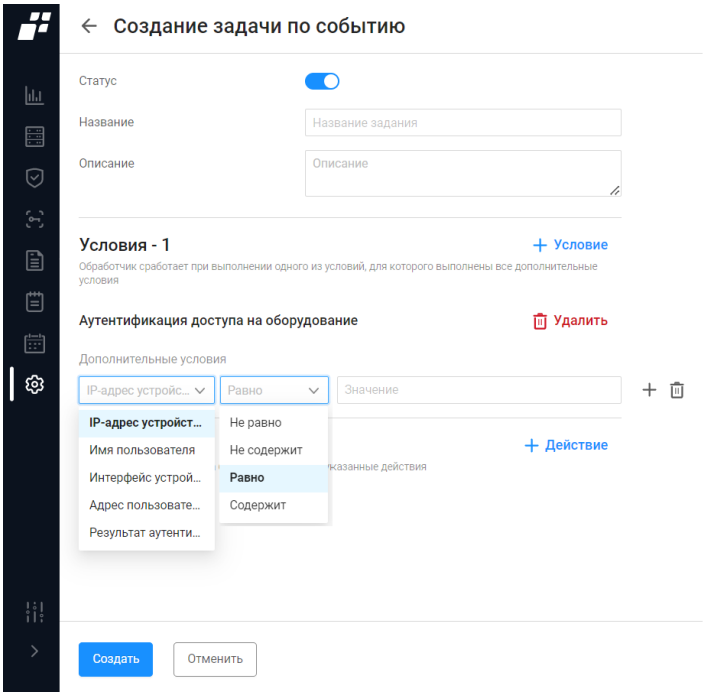


Рисунок 95 – Выбор дополнительных условий

5) В поле «Действия» нажать кнопку «Действие» (+ Действие). Из раскрывающегося списка выбрать тип события, при совершении которого ожидается реакция системы. Из раскрывающегося списка поля «Действия» выбрать тип действия, которое будет выполнено в комплексе в ответ на произошедшее событие (рис. 96).

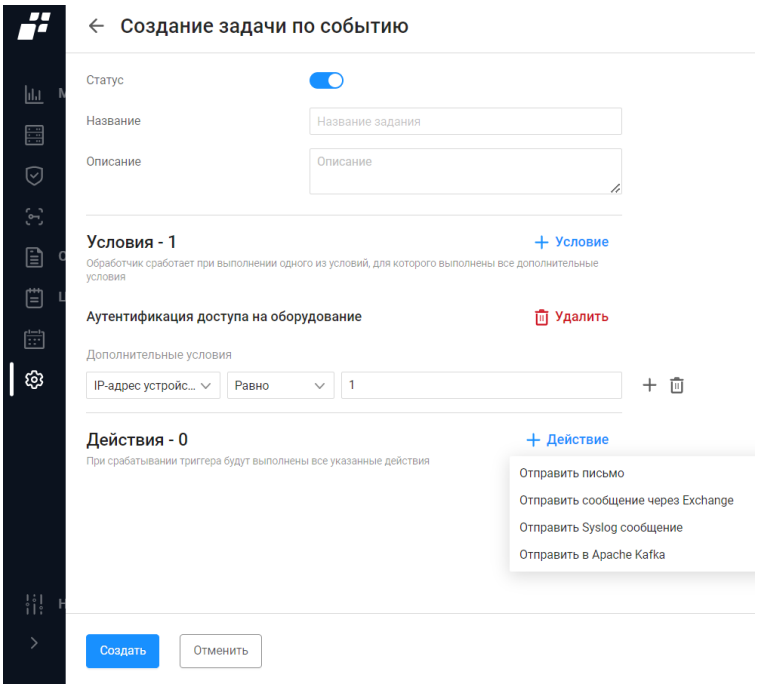


Рисунок 96 – Окно создания действий для задачи по событию

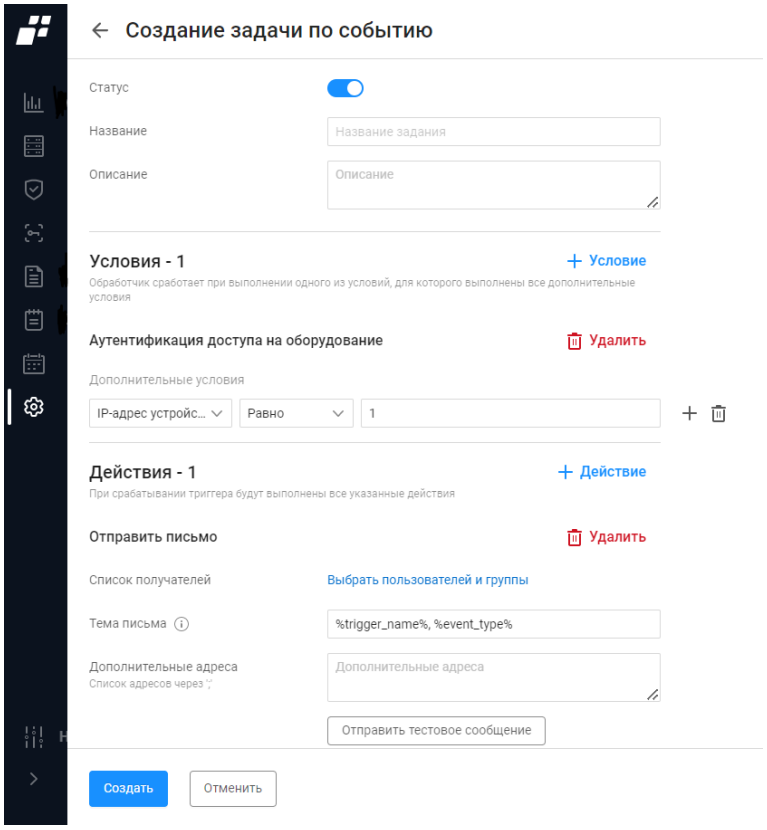


Рисунок 97 – Дополнительные параметры для действий

6) Заполнить необходимые параметры страницы (рис. 97). Для каждого действия свой список параметров.
7) Нажать кнопку «Создать».

9.4.1.2 Редактирование задачи по событию

Редактирование задачи по событию выполняется следующим способом:

1) Пользователю необходимо выбрать требуемую задачу.
2) Откроется страница редактирования задачи по событию. Страница содержит внесенные ранее данные.
3) Пользователю необходимо внести требуемые изменения на странице редактирования и нажать кнопку «Сохранить».

Автоматически запускается процесс проверки заполненности всех обязательных полей и уникальности редактируемой задачи.

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

9.4.2 Вкладка «По расписанию»

На странице список задач по расписанию реализован в виде таблицы (рис. 98).

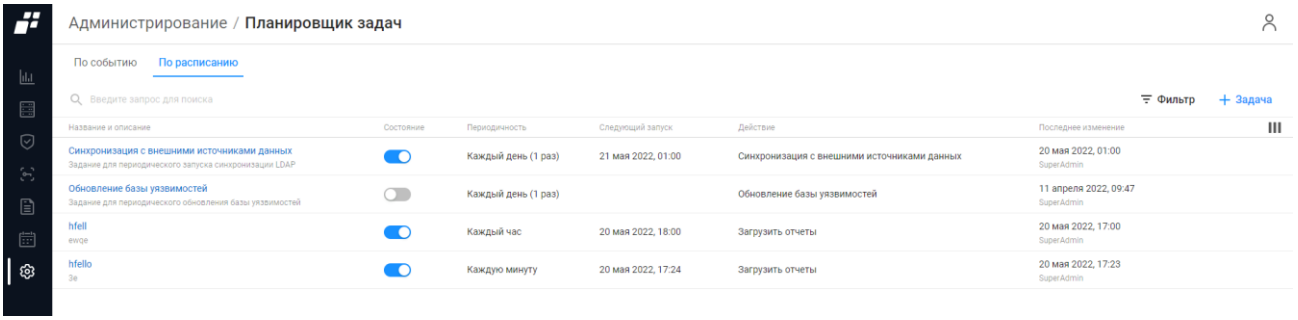


Рисунок 98 – Вкладка «По расписанию»

Для каждой записи списка отображаются следующие данные:

- Название и описание задачи по выполнению расписания. Является ссылкой, при переходе по которой открывается окно редактирования расписания;
- Состояние. Переключатель, отображает активность задачи (включена или выключена);
- Периодичность. Интервал запуска задачи по расписанию;
- Дата следующего запуска;
- Действие. Действие, которое должно совершиться при наступлении срока выполнения задачи по расписанию;
- Дата внесения последних изменений и логин пользователя, совершившего последнее изменение задачи по расписанию.

Над списком задач располагаются:

- поле поиска (Введите запрос для поиска);
- кнопка «Фильтр» (Фильтр) для фильтрации задач по расписанию;
- кнопка «Добавить задачу» (+ Задача);
- кнопка «Колонки» ( ) для изменения отображения колонок на странице.

При наведении курсора на строку с задачей, в правой части строки появляется кнопка «Удалить» ( ) для удаления задачи (если задача отключена) и кнопка «Запустить выполнение задачи», если задача выключена.

9.4.2.1 Создание задачи по расписанию

Для создания новой задачи по расписанию необходимо выполнить следующее:

1) Нажать на кнопку « + Задача ».
2) Откроется страница «Создание задачи по расписанию» (рис. 99).
3) На странице заполнить необходимые поля и нажать кнопку «Создать». Состав и описание полей страницы приведены в таблице 41.

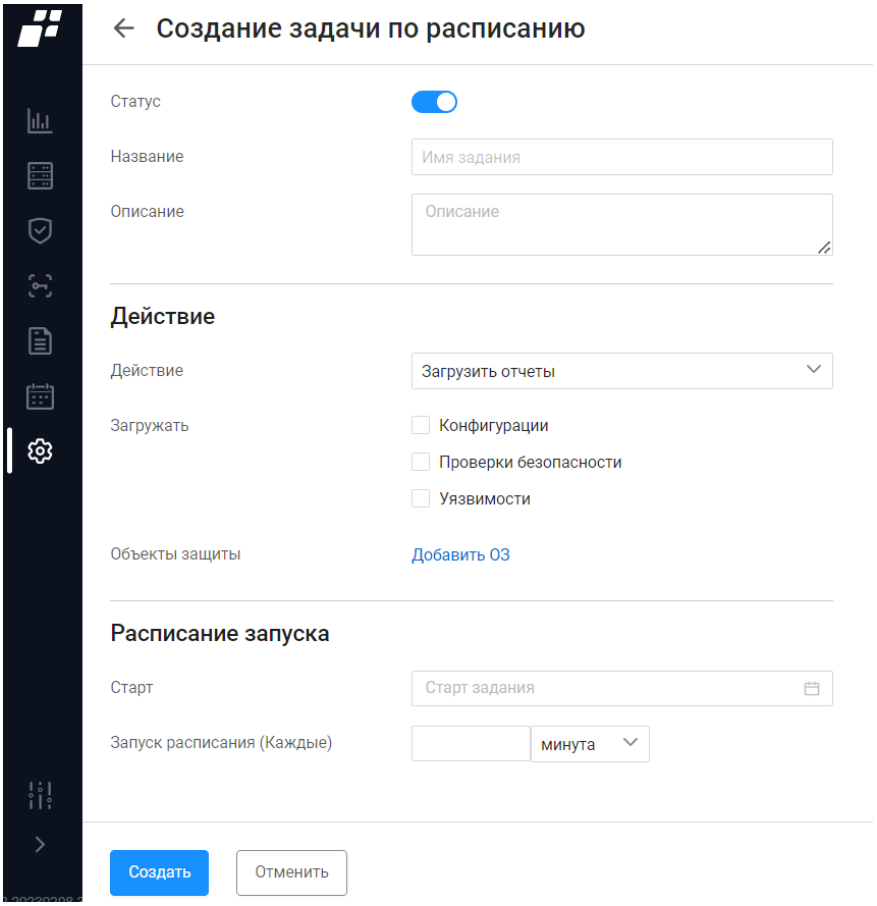


Рисунок 99 – Страница «Создание задачи по расписанию»

Таблица 41 – Состав и описание страницы «Создание задачи по расписанию»

Поле	Описание
Поле «Статус»	Переключатель: — «Включен» ( ) – задача активна; — «Выключен» ( ) – задача неактивна
Поле «Название»	Текстовое поле для ввода названия задачи. Параметры ввода текста: от 1 до 250 любых символов
Поле «Описание»	Текстовое поле для ввода описания задачи. Параметры ввода текста: от 1 до 4000 любых символов
Группа полей «Действие»	
Поле «Действие»	Раскрывающийся список для выбора действия по расписанию: — «Загрузить отчеты» – при выборе действия необходимо выбрать вид загружаемого отчета; — «Обновление базы уязвимостей»; — «Синхронизация с внешними источниками данных»;

Поле	Описание
	— «Загрузить уязвимости со сканера». Дополнительные параметры зависят от выбранного действия в поле «Действие»
Поле «Загружать»	Предназначено для выбора объектов для загрузки по расписанию. Состав переключателей: — «Конфигурации»; — «Проверки безопасности»; — «Уязвимости»
Поле «Объекты ОЗ»	Является ссылкой. При переходе открывается окно для выбора ОЗ
Группа полей для действия «Загрузить уязвимости со сканера»	
Поле «Сканер уязвимостей»	Переключатель: — «MaxPatrol8». При выборе появляются дополнительные поля; — «RedCheck». При выборе появляются дополнительные поля
Поле «Доступ к директории»	Переключатель: — «Сетевой»; — «SSH подключение»
Дополнительные поля для MaxPatrol8, доступ «Сетевой»	
Поле «Путь до директории»	Путь до директории, из которой забираются отчеты сканирования в формате XML
Поле «Подключение»	Переключатель: — «Пользователь и пароль». Необходимо указать пользователя и пароль для доступа к директории; — «Анонимно»
Кнопка «Проверить доступность директории»	Проверить доступность директории. Результат проверки выводится на экран
Дополнительные поля для MaxPatrol8, доступ «SSH подключение»	
Поле «Адрес сервера»	Адрес сервера, на котором расположена директория, из которой забираются отчеты сканирования в формате XML
Поле «Пользователь»	Логин пользователя для доступа в директорию
Поле «Пароль»	Пароль пользователя для доступа в директорию
Поле «Путь до директории»	Путь до директории, из которой забираются отчеты сканирования в формате XML

Поле	Описание
Кнопка «Проверить доступность директории»	Проверить доступность директории. Результат проверки выводится на экран
Дополнительные поля для RedCheck	
Поле «URL API»	Путь до директории, из которой забираются отчеты сканирования в формате XML
Поле «Пользователь»	Логин пользователя для доступа в директорию
Поле «Пароль»	Пароль пользователя для доступа в директорию
Кнопка «Проверить подключение»	Проверить доступность директории. Результат проверки выводится на экран
Группа полей «Расписание запуска»	
Поле «Старт»	Поле для настройки временных параметров запуска расписания
Поле «Запуск расписания (Каждые)»	Предназначено для настройки временных параметров запуска расписания. Состав полей группы зависит от выбранного временного интервала: минута, час, день, неделя, месяц
Поле «Время старта»	Время запуска расписания
Поле «Следующий запуск»	Время повторного запуска расписания. Рассчитывается автоматически
Элементы управления	
Создать	При нажатии кнопки выполняется переход на страницу списка задач с сохранением внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу списка задач без сохранения внесенных данных

9.4.2.2 Редактирование задачи по расписанию

Редактирование задачи по расписанию выполняется следующим способом:

1) Пользователю необходимо выбрать требуемую задачу.
2) Откроется страница редактирования задачи по расписанию. Страница содержит внесенные ранее данные.
3) Пользователю необходимо внести требуемые изменения на странице редактирования и нажать кнопку «Сохранить».

Автоматически запускается процесс проверки заполненности всех обязательных полей и уникальности редактируемой задачи.

При обнаружении незаполненных обязательных полей под полем появится сообщение красного цвета: «Обязательное поле». Пользователю необходимо корректно заполнить

поля окна и повторно нажать кнопку «Сохранить».

9.4.3 Фильтрация в планировщике задач

Для фильтрации задач необходимо нажать кнопку «Фильтр» (Фильтр). Откроется окно фильтрации, приведенное на рис. 100.

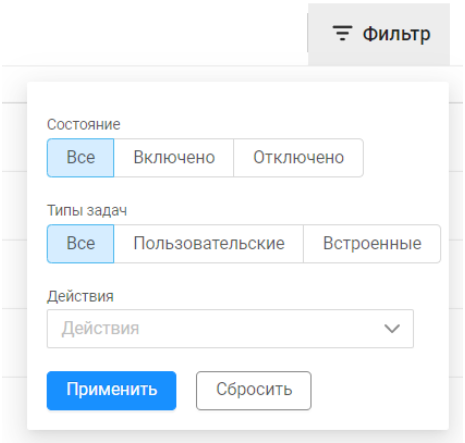


Рисунок 100 – Окно фильтрации

Состав полей окна и правила их заполнения приведены в таблице 42.

Таблица 42 – Состав и описание полей окна фильтрации

Поле	Описание
Поле «Состояние»	Поле с вариантом выбора: — «Все»; — «Включено»; — «Отключено»
Поле «Типы задач»	Поле с переключателем: — «Все»; — «Пользовательские»; — «Встроенные»
Поле «Действие»	Поле с раскрывающимся списком возможных действий
Элементы управления	
Применить	При нажатии кнопки окно фильтрации закрывается, введенные настройки фильтрации применяются
Сбросить	При нажатии кнопки окно фильтрации закрывается без применения введенных настроек

1) Заполнить необходимые параметры фильтрации.
2) Нажать кнопку «Применить».

На странице отобразятся записи с задачами, соответствующими заданным параметрам фильтрации. Для отмены заданных правил фильтрации и отображения в списке всех записей необходимо повторно нажать на кнопку «Фильтр» и нажать кнопку «Сбросить».

10 Раздел «Настройки»

Отображаемые данные и доступная функциональность раздела «Настройки» зависят от наличия хотя бы одной лицензии.

Раздел состоит из трех групп настроек:

- «Контроль доступа»;
- «Контроль устройств»;
- «Общие».

Для просмотра раздела пользователю необходимо выбрать в панели главного меню раздел «Настройки» или, если панель свернута, нажать на пиктограмму «  »,панель автоматически раскроется и отобразятся все разделы

10.1 TACACS+ и RADIUS

Подраздел «TACACS+ и RADIUS» доступен пользователю для работы при наличии лицензии на функциональный модуль «Efros NAC».

Данный подраздел обеспечивает возможность централизованной сетевой идентификации сетевых пользователей и управления доступом на сетевых устройствах, у которых на клиентском уровне поддерживаются протоколы TACACS+ и (или) RADIUS.

В ПК «Efros DO» поддерживается работа со следующими типами сетевых устройств:

- активное сетевое оборудование (АСО): маршрутизаторы, коммутаторы, и другое оборудование, поддерживающее протоколы TACACS+ и RADIUS;
- клиентское оборудование: стационарные и мобильные рабочие станции пользователей контролируемой сети, принтеры, факсы и прочие сетевые устройства типа «конечная точка».

Подраздел предназначен для настройки параметров работы комплекса с сервисами протоколов TACACS+ и RADIUS (рис. 101).

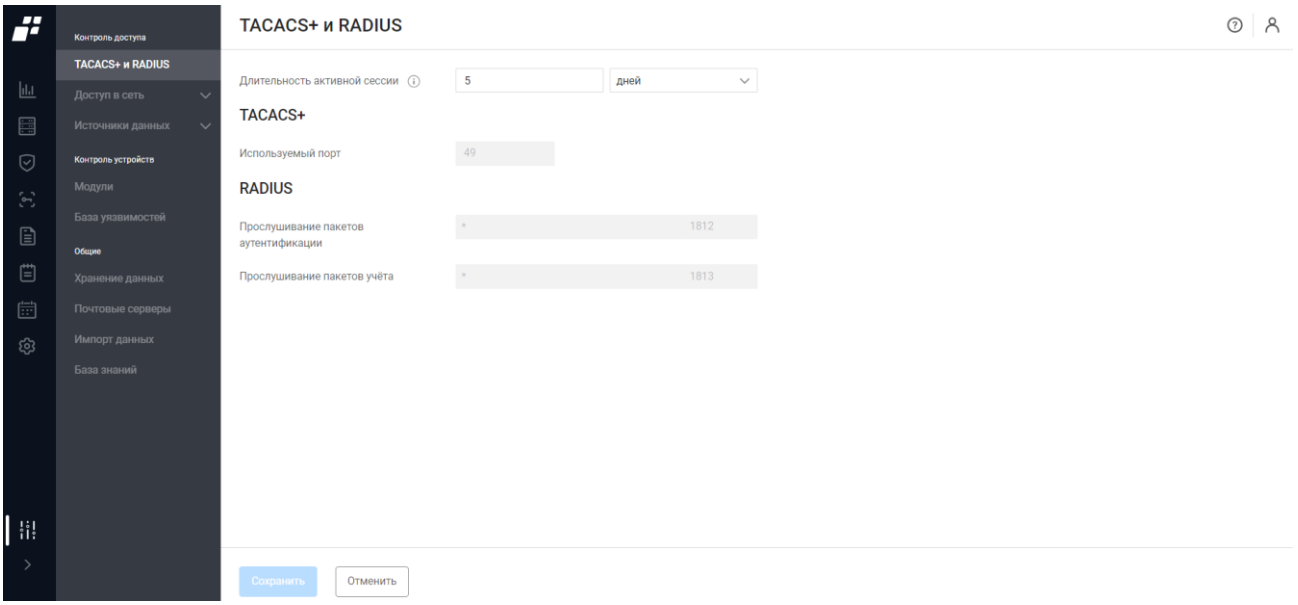


Рисунок 101 – Подраздел «TACACS+ и RADIUS»

Состав и описание полей подраздела приведены в таблице 43.

Таблица 43 – Состав и описание полей страницы «TACACS+ и RADIUS»

Поле	Описание
Поле «Длительность активной сессии»	Поле для ввода времени жизни активной сессии. Активная сессия – это сессия, для которой получено начало Аудита RADIUS, но остановка Аудита RADIUS еще не получена. Параметр используется для сброса активной сессии конечной точки при отсутствии остановки Аудита RADIUS для подсчета количества лицензий функционального модуля «Efros NAC»
*Группа полей протокола TACACS+	
Поле «Используемый порт»	Порт для протокола TACACS+. По умолчанию содержит значение 49
*Группа полей протокола RADIUS	
Поле «Прослушивание пакетов аутентификации»	Содержит поля: — IP-адреса прослушиваемых серверов; — номер порта прослушивания пакетов аутентификации. По умолчанию прослушиваются все сервера в сети (значение «*») и порт прослушивания – 1812
Поле «Прослушивание пакетов учета»	Содержит поля: — IP-адреса прослушиваемых серверов; — номер порта прослушивания пакетов учета. По умолчанию прослушиваются все сервера в сети (значение «*») и порт прослушивания – 1813
Элементы управления	

Поле	Описание
Сохранить	При нажатии кнопки выполняется сохранение внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу без сохранения внесенных данных
*поля недоступны для редактирования	

Для выполнения настройки протоколов необходимо:

1) Заполнить поля страницы соответствующими параметрами.
2) Нажать кнопку «Сохранить».

После чего введенные параметры будут сохранены в ПК «Efros DO».

10.2 Доступ в сеть

Подраздел «Доступ в сеть» доступен пользователю для работы при наличии лицензии на функциональный модуль «Efros NAC».

Настройка доступа в сеть подключенных к ПК «Efros DO» устройств с использованием расширяемого протокола аутентификации EAP (далее – протокол EAP) включает в себя настройку EAP (используемого по умолчанию типа EAP и параметров сессий), настройку используемых методов EAP (протоколов) и настройку конфигураций TLS.

После завершения редактирования и сохранения измененных параметров настройки:

- введенные параметры будут сохранены в БД модуля «Efros NAC»;
- клиентское оборудование сможет получить доступ в сеть с использованием протокола EAP.

10.2.1 Настройки EAP

Для выполнения настройки EAP пользователю необходимо:

1) Выбрать раздел «Настройки», далее подраздел «Доступ в сеть» и вкладку «Настройки EAP» (см. рис. 102). Состав и описание полей страницы приведены в таблице 44.

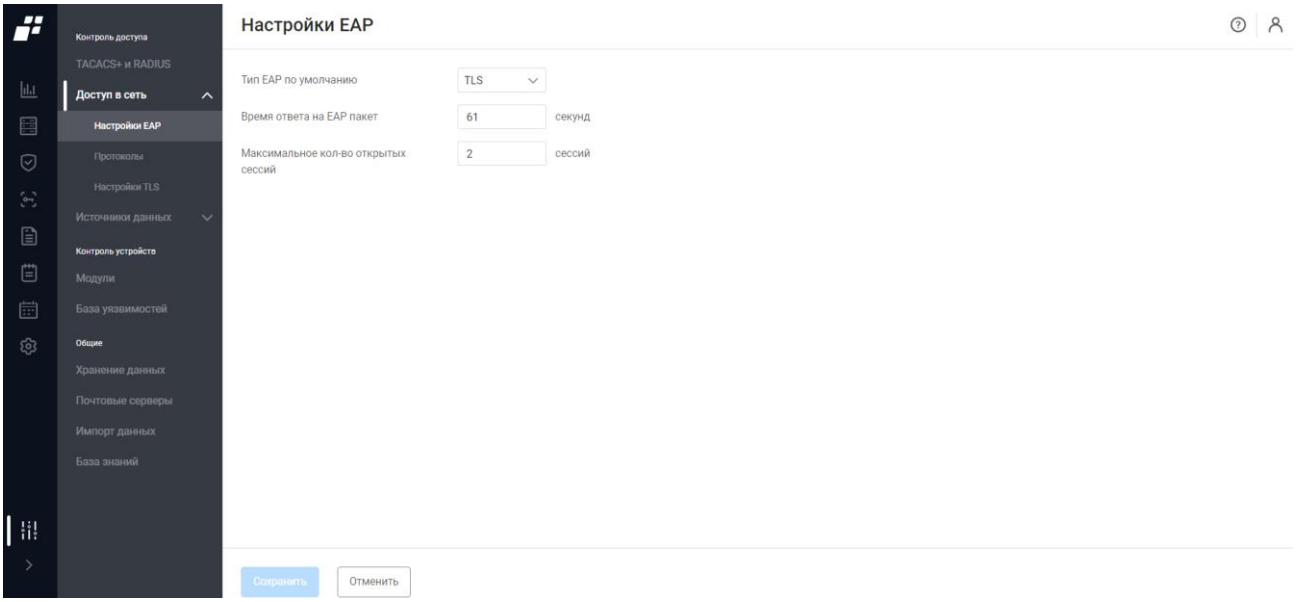


Рисунок 102 – Страница «Настройки EAP»

2) Выбрать используемый по умолчанию тип EAP.
3) Ввести в поля вкладки требуемые значения параметров:
   – время ответа на EAP-пакет в секундах;
   – максимальное количество открытых сессий.
4) Нажать кнопку «Сохранить». Введенные настройки EAP будут сохранены, перезапустится служба протокола для применения новых настроек.

Таблица 44 – Состав и описание полей страницы «Настройки EAP»

Поле	Описание
Поле «Тип EAP по умолчанию»	Поле со списком для выбора типа EAP, используемого по умолчанию при получении запроса на аутентификацию от АСО. Список содержит следующие типы EAP: MD5, PEAP, TLS, TTLS
Поле «Время ответа на EAP пакет»	Поле для ввода времени хранения данных аутентификатора между запросами и ответами на EAP–пакеты (в секундах). По истечении заданного интервала времени данные удаляются. Допустимые значения: от 1 до 16384
Поле «Максимальное кол–во открытых сессий»	Поле для ввода максимального допустимого количества сеансов, отслеживаемых модулем «Efros ACS». Допустимые значения: от 1 до 16384
Элементы управления	
Сохранить	При нажатии кнопки выполняется сохранение внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу без сохранения внесенных данных

10.2.2 Настройка используемых методов EAP (Протоколы)

Для выполнения настройки используемых методов EAP (далее – протоколов) необходимо:

1) Выбрать на странице «Настройки» в подразделе «Доступ в сеть» вкладку «Протоколы». Откроется страница «Протоколы» (рис. 103), содержащая блоки для настройки параметров используемых протоколов. Состав и описание полей блоков страницы приведены в таблице 45.
2) В заголовке каждого блока расположен переключатель с двумя положениями:
   — «Включен» ( ) – в ПК «Efros DO» включена поддержка соответствующего протокола;
   — «Выключен» ( ) – в ПК «Efros DO» выключена поддержка соответствующего протокола.
3) Настроить список используемых протоколов установкой переключателей в блоках вкладки в соответствующее положение.
4) Внести, при необходимости, изменения в параметры отдельных протоколов.
5) Нажать кнопку «Сохранить».

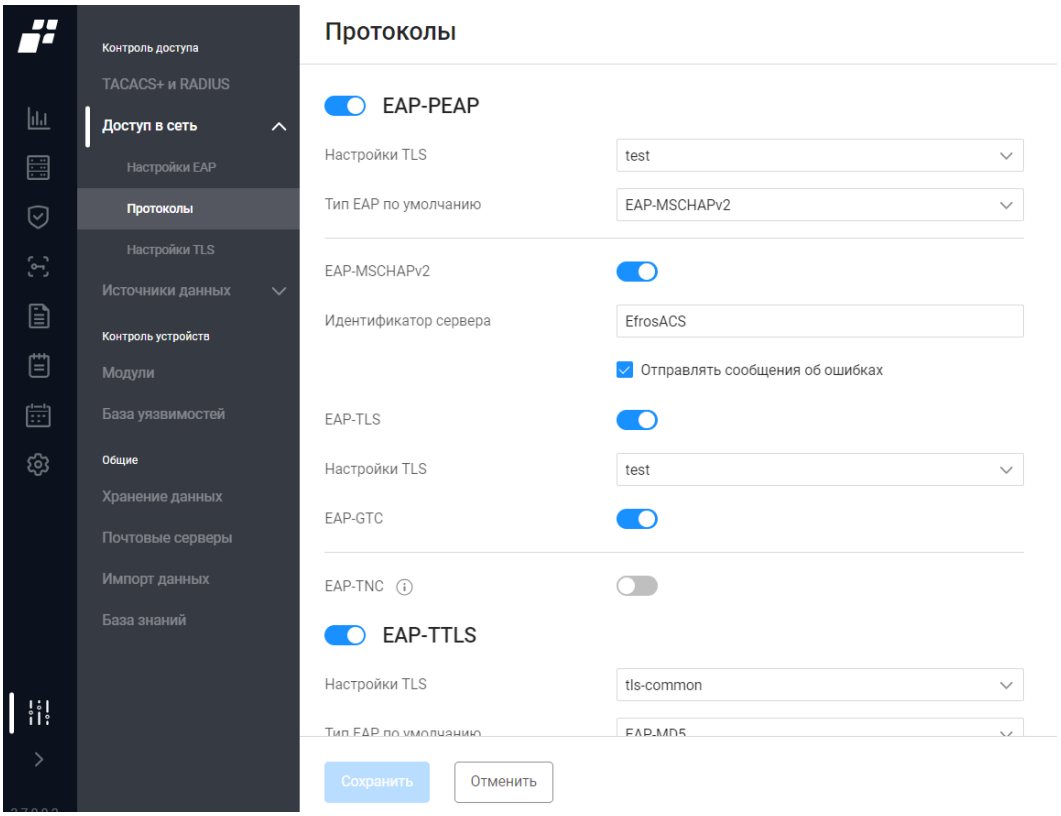


Рисунок 103 – Страница «Протоколы»

Таблица 45 – Состав и описание полей страницы вкладки «Протоколы» подраздела «Доступ в сеть»

Поле	Описание
Блок «EAP-PEAP» (рис. 104)	
Поле «Настройки TLS»	Поле с раскрывающимся списком для выбора используемой конфигурации TLS. Список содержит наименования конфигураций в соответствии со списком вкладки «Настройки TLS» подраздела «Доступ в сеть»
Поле «Тип EAP по умолчанию»	Поле с раскрывающимся списком для выбора типа EAP, используемого по умолчанию при получении запроса на аутентификацию от АСО
Поле «EAP-MSCHAPv2»	Переключатель для включения/выключения использования соответствующего типа EAP
Поле «Идентификатор сервера»	Поле для ввода/редактирования идентификатора модуля «Efros NAC»
Поле «EAP-TLS»	Поле с раскрывающимся списком для выбора используемой конфигурации TLS. Список содержит наименования конфигураций в соответствии со списком вкладки «Настройки TLS» подраздела «Доступ в сеть»
Поле для флага	При наличии в поле флага клиенту при неуспешной

Поле	Описание
«Отправлять сообщения об ошибках клиенту»	аутентификации отправляется сообщение об ошибке с причиной ошибки аутентификации
Поле «EAP-GTC»	Предназначен для включения/выключения использования соответствующего типа EAP
Поле «EAP-TNC»	Переключатель для включения/выключения проверки подключаемого устройства на соответствие требованиям политики безопасности
Блок «EAP-TTLS» (см. рис. 105)	
Поле «Настройки TLS»	Поле со списком для выбора используемой конфигурации TLS. Список содержит наименования конфигураций в соответствии со списком вкладки «Настройки TLS» подраздела «Доступ в сеть»
Поле «Тип EAP по умолчанию»	Поле со списком для выбора типа EAP, используемого методом по умолчанию при получении запроса на аутентификацию от АСО
Группы полей «EAP- MSCHAPv2», «EAP-TLS» и «EAP- GTC»	Состав групп аналогичен составу групп в блоке «EAP-PEAP» (см. выше)
Поле «EAP-MD5»	Предназначен для включения/выключения использования соответствующего типа EAP
Блок «EAP–TLS» (рис. 106)	
Поле «Настройки TLS»	Поле со списком для выбора используемой конфигурации TLS. Список содержит наименования конфигураций в соответствии со списком вкладки «Настройки TLS» подраздела «Доступ в сеть»
Поле «EAP-MD5»	Предназначен для включения/выключения использования соответствующего типа EAP. Блок «EAP-MD5». Не содержит дополнительных параметров
Элементы управления	
Сохранить	При нажатии кнопки выполняется сохранение внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу без сохранения внесенных данных

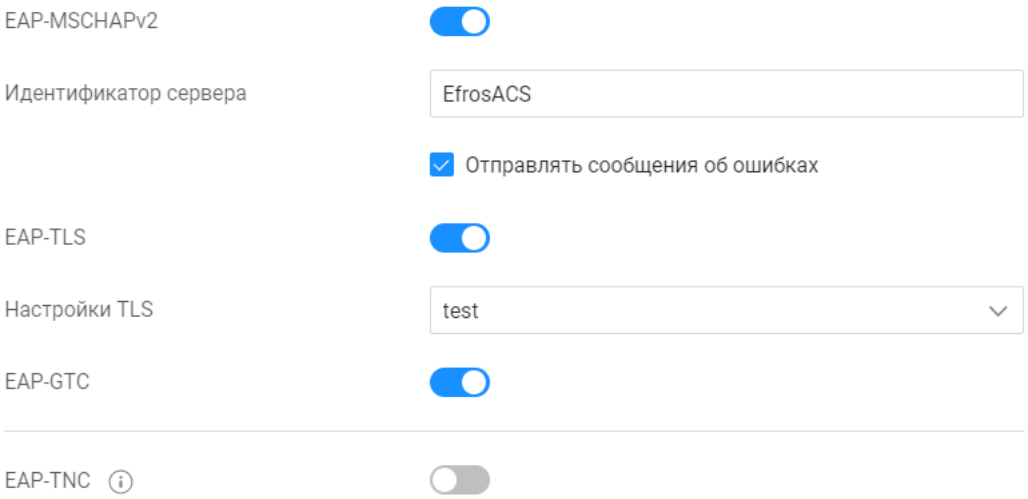


Рисунок 104 – Блок «EAP–PEAP»

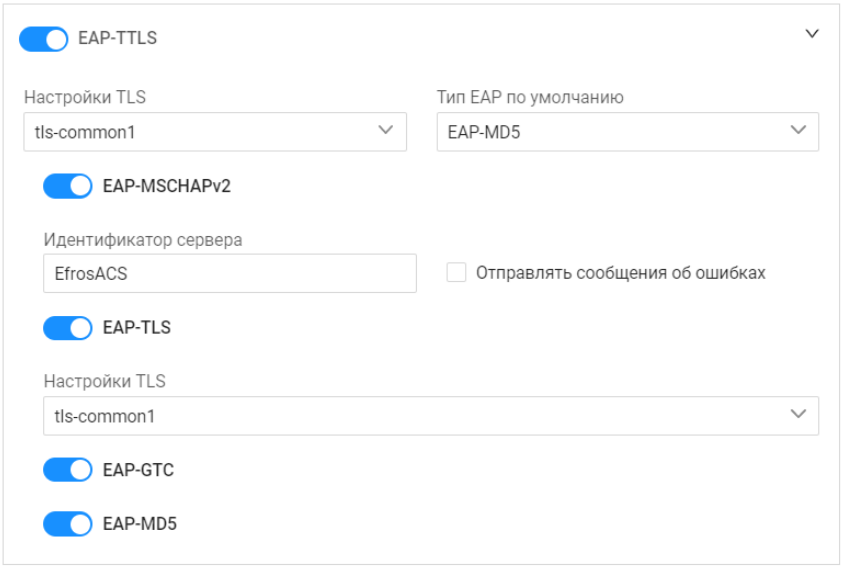


Рисунок 105 – Блок «EAP–TTLS»

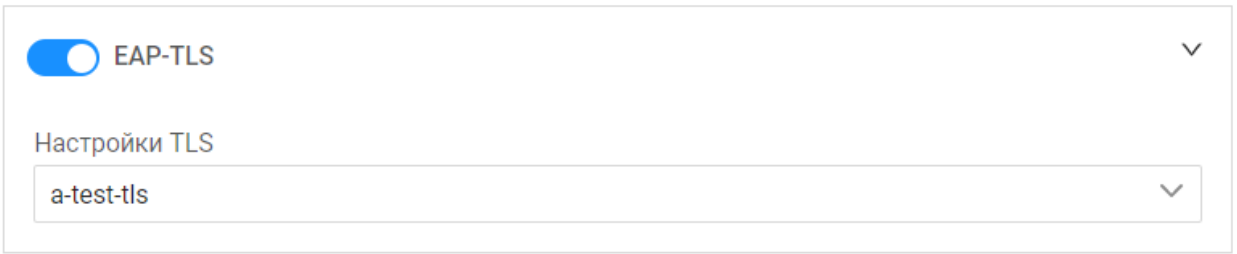


Рисунок 106 – Блок «EAP–TLS»

10.2.3 Настройки конфигураций TLS

Для выполнения настройки конфигураций TLS пользователю необходимо выбрать раздел «Настройки», далее подраздел «Доступ в сеть» и вкладку «Настройки TLS» (см. рис. 107).

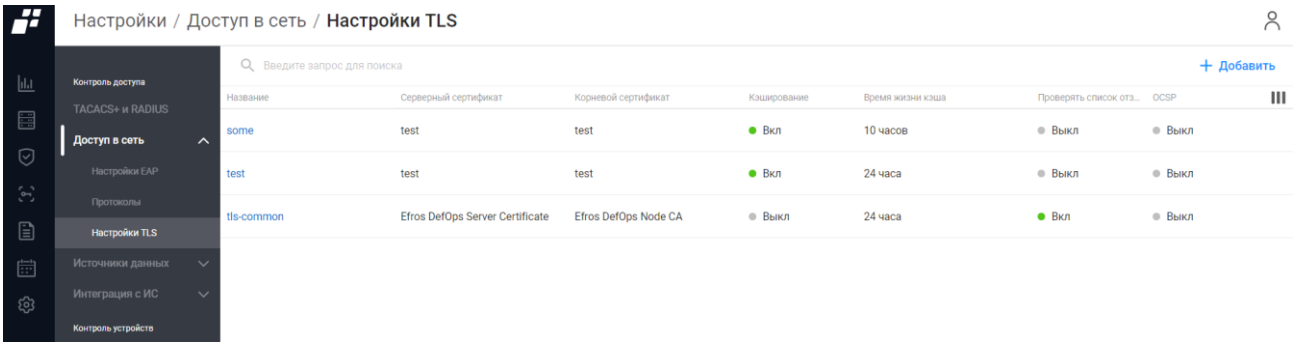


Рисунок 107 – Страница вкладки «Настройки TLS»

На странице список настроек реализован в виде таблицы. Для каждой записи списка отображаются следующие данные:

- название настройки;
- имя серверного сертификата, используемого при аутентификации устройств в сети;
- имя корневого сертификата, связанного с выбранным серверным сертификатом;
- кэширование;
- время жизни кэша;
- проверка списка отзывов сертификата;
- OCSP.

Над таблицей списка настроек располагаются:

- поле поиска (Введите запрос для поиска) для поиска искомой записи в списке;
- кнопка «Добавить» (+ Добавить) для перехода на страницу создания нового профиля TLS;
- кнопка «Содержание» ( ) для изменения отображения колонок на странице.

При наведении курсора на строку с настройкой, в правой части строки появляется кнопка «Удалить» ( ) для удаления настройки.

При установке комплекса по умолчанию установлена одна конфигурация с названием tls-common. Пользователь имеет возможность создавать новые конфигурации, вносить изменения в имеющиеся и удалять конфигурации. Для удаления доступны только те конфигурации, которые не привязаны ни к одному из протоколов (см. п.п. 10.2.2).

10.2.3.1 Создание настройки TLS

Для создания новой настройки TLS пользователю необходимо:

1) Нажать кнопку «Добавить». Откроется страница создания настройки TLS (рис. 108). Состав и описание полей страницы приведены в таблице 46.
2) Заполнить поля страницы требуемыми параметрами (таблица 46).

3) Нажать кнопку «Создать».

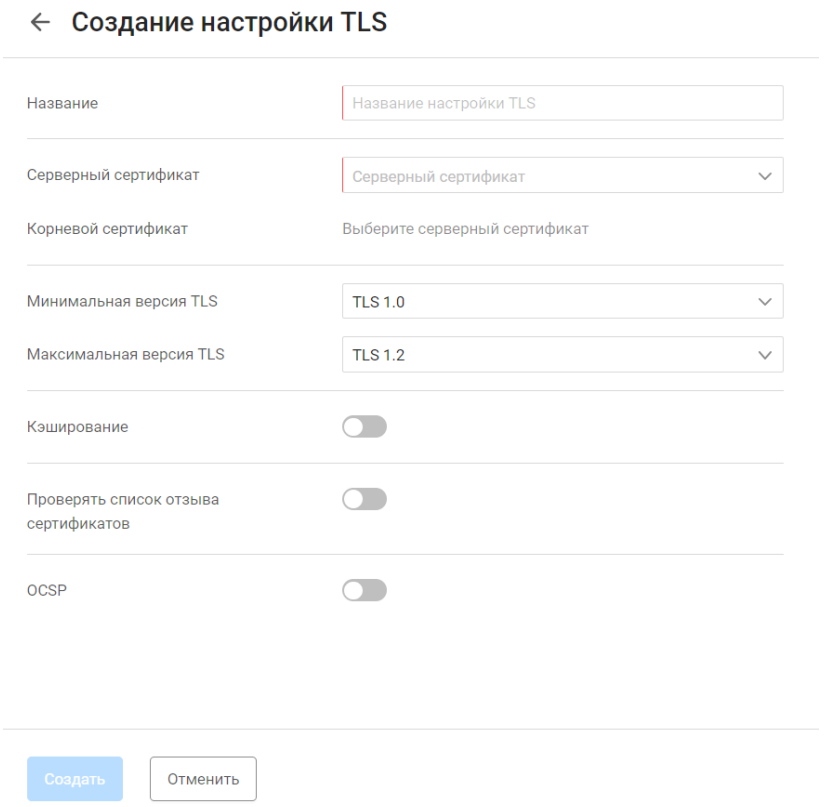


Рисунок 108 – Страница «Создание настройки TLS»

Таблица 46 – Состав и описание полей страницы создания настройки TLS

Поле	Описание
Поле «Название»	Поле для ввода названия конфигурации. Параметры ввода текста: от 1 до 50 символов. Допустимые символы: буквы латинского алфавита, цифры, «_», «–»
Поле «Серверный сертификат»	Поле со списком для выбора серверного сертификата, используемого при аутентификации устройств в сети. Содержит список серверных сертификатов, для которых однозначно определен корневой сертификат
Поле «Корневой сертификат»	Поле заполняется автоматически после выбора серверного сертификата. Содержит название корневого сертификата, связанного с выбранным серверным сертификатом. Поле не доступно для внесения изменений в ручном режиме
Поле «Минимальная версия TLS»	Раскрывающийся список версий TLS
Поле «Максимальная версия TLS»	Раскрывающийся список версий TLS
Поле «Кэширование»	Переключатель с двумя положениями:

Поле	Описание
	— «Включен» () – при восстановлении сеанса из кэша копируются атрибуты сеанса: ID сессии и имя пользователя; — «Выключен» () – при восстановлении сеанса атрибуты из кэша не копируются. Время хранения атрибутов сессии настраивается в поле «Время жизни кэша, час» (см. ниже)
Поле «Время жизни кэша, часы»	Поле для ввода времени хранения атрибутов сессии: ID сессии и имя пользователя (в часах). Допустимые значения: от 1 до 100. Значение по умолчанию – 1. Поле отображается и доступно для редактирования только если включен переключатель «Кэширование» (см. выше)
Поле «Проверять список отзыва сертификатов»	Переключатель с двумя положениями: — «Включен» () – клиентские сертификаты проверяются в модуле «Efros NAC» на их наличие в списке отозванных сертификатов (CRL); — «Выключен» () – проверка не выполняется
Поле «OCSP»	Переключатель с двумя положениями: — «Включен» () – клиентские сертификаты проверяются в модуле «Efros NAC» с использованием протокола OCSP; — «Выключен» () – проверка не выполняется
Элементы управления	
Создать	При нажатии кнопки выполняется сохранение внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу без сохранения внесенных данных

10.2.3.2 Редактирование настройки TLS

Для редактирования настройки TLS пользователю необходимо:

1) Выбрать в блоке требуемую настройку TLS и нажать на ее название. Откроется страница редактирования параметров настройки TLS.
2) Внести требуемые изменения в поля страницы.
3) Нажать кнопку «Сохранить». Внесенные изменения будут сохранены и применены, в журнале событий «События» будет внесено соответствующее сообщение с уровнем «Инфо».

Для удаления конфигурации пользователю необходимо:

1) Нажать в строке удаляемой конфигурации кнопку «Удалить» ( ).
2) Нажать в открывшемся окне подтверждения кнопку «Удалить».

Если конфигурация TLS привязана к одному из протоколов, то при попытке ее удаления отобразится сообщение об ошибке.

10.3 Источники данных

Подраздел «Источники данных» доступен пользователю для работы при наличии лицензии на функциональный модуль «Efros NAC».

10.3.1 Источник данных LDAP

Данный подраздел предназначен для настройки параметров работы модуля интеграции «Efros NAC» со службой каталогов AD, в которой хранятся учетные записи пользователей, связанные с учетными записями пользователей модуля интеграции «Efros NAC» (рис. 109).

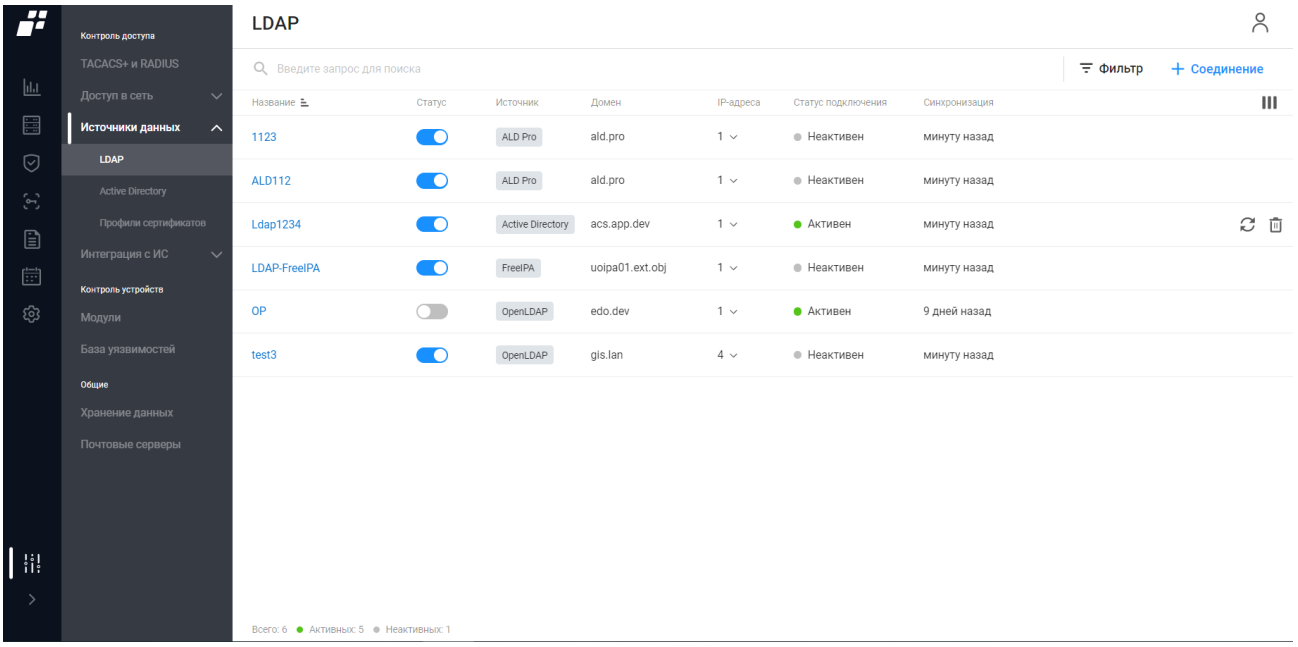


Рисунок 109 – Вкладка «LDAP»

На странице список источников реализован в виде таблицы. Для каждой записи списка отображаются следующие данные:

- название устанавливаемого соединения;
- статус соединения (активно/неактивно);
- источник данных;
- домен;
- IP-адрес;
- статус подключения;
- дата последней синхронизации данных.

Над списком соединений расположены:

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

— кнопка «Соединение» (+ Соединение) для создания нового LDAP соединения;

— кнопка «Фильтр» (Фильтр) для фильтрации списка соединений;

— кнопка «Колонки» ( ) для изменения отображения колонок на странице.

При наведении курсора на строку с настройкой, в правой части строки появляется кнопка «Удалить» ( ) для удаления источника данных и кнопка «Синхронизировать» « » для синхронизации данных с источником.

10.3.1.1 Создание нового соединения LDAP

Для создания нового подключения к LDAP-серверу администратору необходимо:

1) Нажать на кнопку «Соединение» (+ Соединение).
2) Откроется страница «Создание LDAP соединения» (рис. 110). Состав и описание полей страницы приведены в таблице 47.

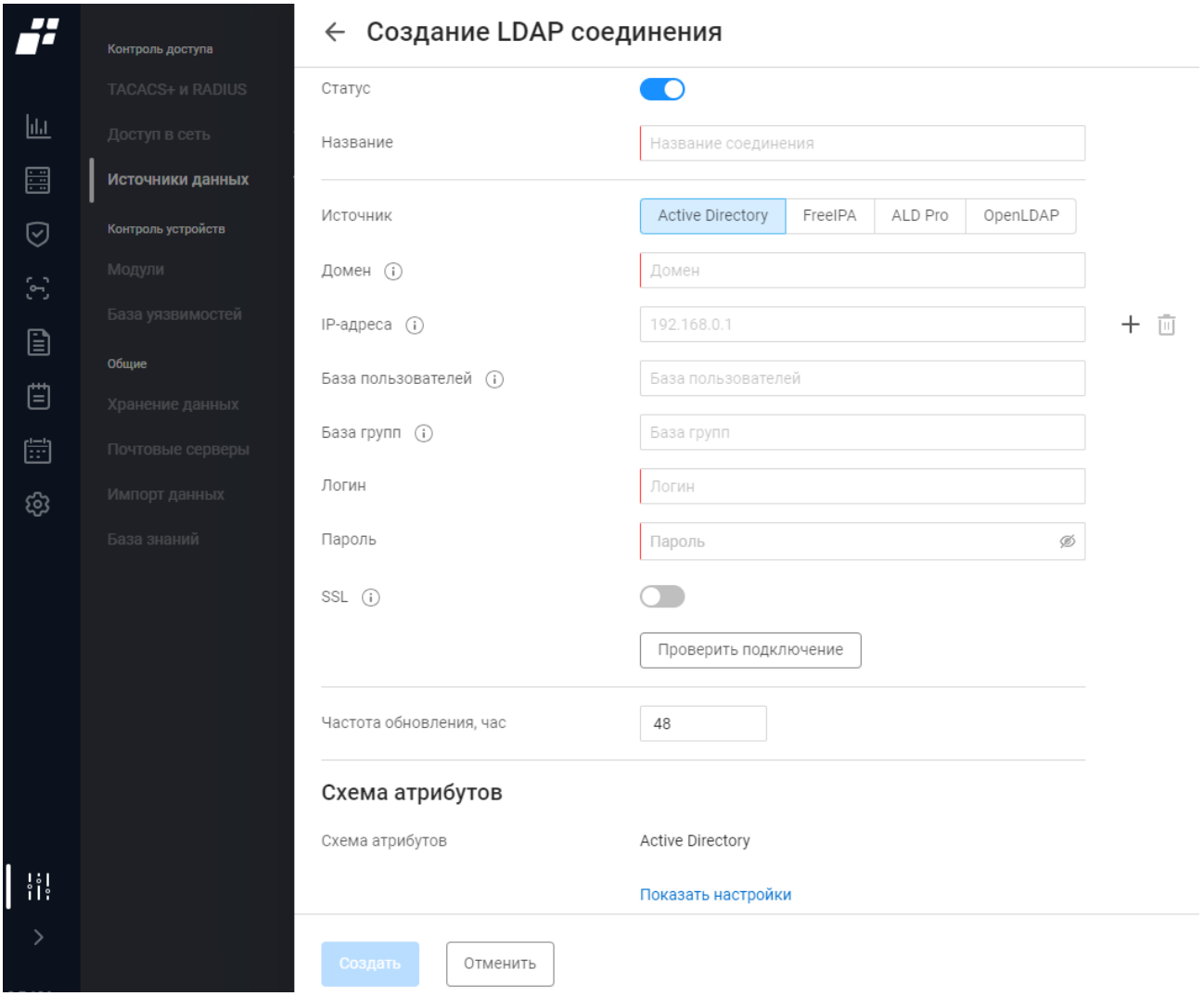


Рисунок 110 – Страница «Создание LDAP соединения»

Таблица 47 – Состав и описание полей страницы «Создание LDAP соединения»

Поле	Описание
Поле «Статус»	Содержит переключатель с двумя положениями: — «Включено» ( ) – подключение включено; — «Выключено» ( ) – подключение выключено
Поле «Название»	Поле для ввода названия нового соединения. Параметры ввода текста: от 1 до 50 символов. Допустимые символы: буквы латинского алфавита, цифры, «_», «–»
Поле «Источник»	Содержит варианты: — «Active Directory»; — «FreeIPA»; — «ALD Pro»; — «OpenLDAP» В зависимости от выбранного источника, по умолчанию будет использована соответствующая схема атрибутов. При необходимости, её можно отредактировать самостоятельно
Поле «Домен»	Поле для ввода имени домена для автоматического определения IP-адресов серверов служб каталогов. При корректно настроенном существующем сервере DNS и доступе к серверу ПК «Efros DO», IP-адрес определятся автоматически
Поле «IP-адреса»	Определяются автоматически. Указанные серверы должны быть доступны по следующим портам: — 389 – при использовании протокола LDAP; — 636 – при использовании протокола LDAPS (активированном переключателе SSL). Рекомендуется указывать только доступные IP-адреса для минимизации времени взаимодействия со службой каталогов
Поле «База пользователей»	Необходимо задать уровень, с которого будет осуществляться поиск пользователей в дереве служб каталогов. Если поле не заполнено, поиск выполняется по всему дереву служб каталогов. Для источника ALD Pro (например, домен ald.pro) рекомендуется указывать в формате:

Поле	Описание
	cn=users,cn=accounts,dc=ald,dc=pro
Поле «База групп»	Поле для ввода уровня, с которого будет осуществляться поиск групп пользователей в дереве служб каталогов. По умолчанию поле не заполнено и поиск данных выполняется по всему дереву служб каталогов. Для источника ALD Pro (например, домен ald.pro) рекомендуется указывать в формате: cn=groups,cn=accounts,dc=ald,dc=pro
Поле «Логин»	Поле для ввода имени пользователя, под которым выполняется подключение к службе каталогов
Поле «Пароль»	Поле для ввода пароля пользователя, под которым выполняется подключение к службе каталогов. При вводе символы пароля заменяются знаком «•». Для просмотра введенного значения необходимо нажать в поле ввода кнопку «Просмотреть» ( )
Поле «SSL»	Содержит переключатель с двумя положениями: — «Используется» ( ) – подключение к службе каталогов выполняется с использованием протокола SSL; — «Не используется» ( ) – подключение к службе каталогов выполняется без использования протокола SSL. По умолчанию установлено положение «Не используется»
Кнопка «Проверить подключение	При нажатии кнопки выполняется проверка успешности установления соединения с введенными параметрами с указанными службами каталогов
Поле «Частота обновления, час»	Поле для ввода числового значения времени обновления подключения
Поле «Схема атрибутов»	Отображается выбранный ранее в поле «Тип источника» тип LDAP-сервера
Поле «Схема атрибутов»	Поля отображаются на странице после нажатия в подзаголовке группы ссылки «Показать настройки». Поля содержат значения по умолчанию, при подключении к новой службе каталогов администратору необходимо проверить их на соответствие. Атрибуты пользователей: — «Отображаемое имя»; — «Имя аккаунта»;

Поле	Описание
	— «Группы пользователя»; — «Сертификат». Атрибуты групп: — «Идентификатор объекта»; — «Отображаемое имя»; — «Имя аккаунта»; — «Пользователи в группе»
Элементы управления	
Создать	При нажатии кнопки выполняется сохранение внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу без сохранения внесенных данных

3) Заполнить поля страницы необходимыми параметрами.
4) Проверить успешность подключения к указанной службе каталогов, нажав кнопку «Проверить подключение».

Если проверка завершилась сообщением об ошибке, внести, при необходимости, поправки в параметры и вновь проверить подключение.

5) После получения сообщения об успешном подключении, нажать кнопку «Создать».

Автоматически запускается процесс проверки заполненности всех обязательных полей и уникальности создаваемого соединения.

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

10.3.1.2 Редактирование соединения LDAP

Для редактирования соединения LDAP пользователю необходимо:

1) Выбрать в блоке нужное соединение и нажать на его имя. Откроется страница редактирования выбранного соединения.
2) Внести требуемые изменения в поля страницы.
3) Нажать кнопку «Сохранить».

Для удаления соединения пользователю необходимо:

1) Нажать в строке удаляемого соединения кнопку «Удалить» ( ).
2) Нажать в открывшемся окне подтверждения кнопку «Удалить». Соединение будет удалено, в журнале событий «События» будет внесено соответствующее

сообщение с уровнем «Инфо».

10.3.2 Источник данных Active Directory

Данный подраздел предназначен для настройки параметров работы модуля интеграции «Efros NAC» с контроллером домена, в котором хранятся учетные записи сетевых устройств, контролируемых модулем интеграции «Efros NAC» (рис. 111).

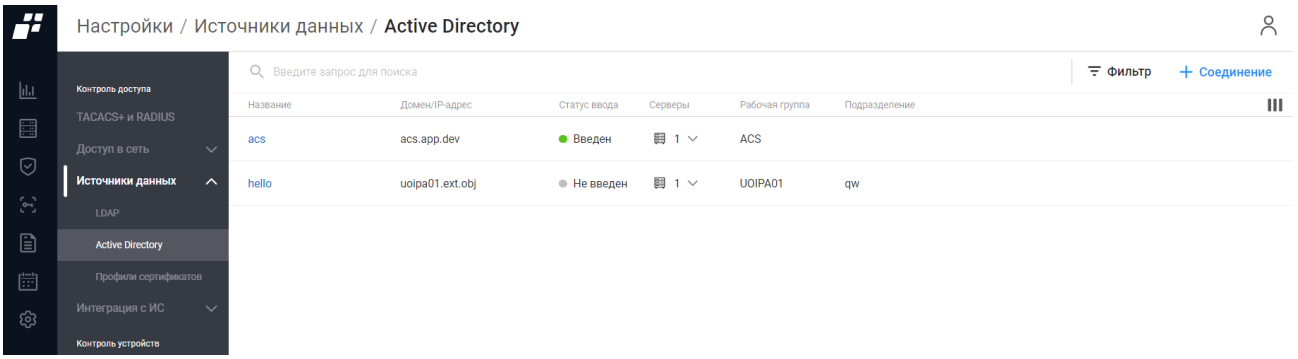


Рисунок 111 – Вкладка «Active Directory»

На странице список источников реализован в виде таблицы. Для каждой записи списка отображаются следующие данные:

- наименование устанавливаемого соединения;
- имя или IP-адрес домена, к которому подключается сервер ПК «Efros DO»;
- статус ввода ПК «Efros DO» сервера в домен;
- количество серверов аутентификации;
- имя рабочей группы;
- учетная запись сервера ПК «Efros DO» в определенном подразделении.

Над списком соединений располагаются:

- поле поиска (Введите запрос для поиска) для поиска искомой записи в списке;
- кнопка «Соединение» (+ Соединение) для создания нового LDAP соединения;
- кнопка «Фильтр» (Фильтр) для фильтрации источников данных;
- кнопка «Колонки» ( ) для изменения отображения колонок на странице.

При наведении курсора на строку с настройкой, в правой части строки появляется кнопка «Удалить» ( ) для удаления настройки.

10.3.2.1 Создание нового соединения Active Directory

Для выполнения настройки подключения к серверу аутентификации необходимо:

1) Нажать на кнопку «Соединение» (+ Соединение).
2) Откроется окно «Создание Active Directory соединения» (см. рис. 112). Состав и описание полей страницы приведены в таблице 48.

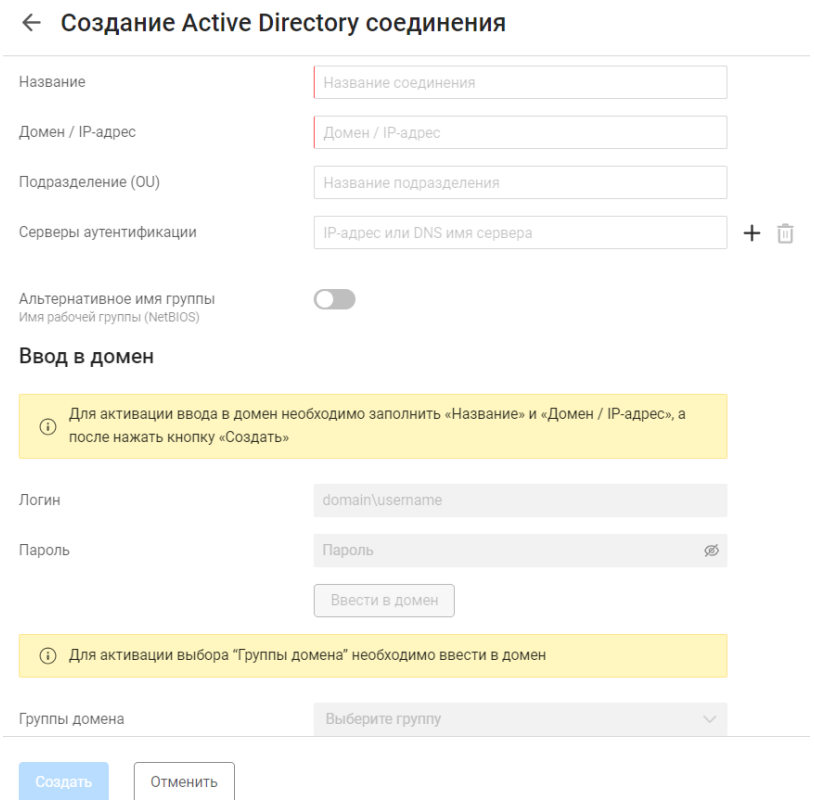


Рисунок 112 – Страница «Создание Active Directory соединения»

Таблица 48 – Состав и описание полей страницы «Создание Active Directory соединения»

Поле	Описание
Поле «Название»	Поле для ввода названия соединения. Параметры ввода текста: от 1 до 50 символов. Допустимые символы: буквы латинского алфавита, цифры, «_», «–»
Поле «Домен/ IP-адрес»	Поле для ввода имени или IP-адреса домена, к которому подключается сервер ПК «Efros DO». Параметры ввода текста: от 1 до 50 символов. Допустимые символы: буквы латинского алфавита, цифры, «_», «–»
Поле «Подразделение (OU)»	Поле для ввода учетной записи сервера ПК «Efros DO» в определенном подразделении. Строка OU читается сверху вниз без относительных уникальных имен и разделяется символом «/». Например, «Computers/Servers/Unix». Параметры ввода текста: от 1 до 50 любых символов
Поле «Серверы аутентификации»	Поле для ввода IP-адреса или DNS имени сервера аутентификации. Параметры ввода текста: 50 символов. Допустимые символы: буквы латинского алфавита, цифры,

Поле	Описание
	«_», «–»
Поле «Альтернативное имя группы»	Альтернативное имя группы. Параметры ввода текста: от 1 до 15 символов. Допустимые символы: буквы латинского алфавита, цифры и символы «-», «.», «_». Поле не может начинаться с "."
Блок «Ввод в домен»	
Поле «Логин»	Поле для введения логина пользователя, настраивающего подключение. Параметры ввода текста: от 1 до 256 любых символов
Поле «Пароль»	Поле для введения пароля пользователя, настраивающего подключение. Параметры ввода текста: от 1 до 500 любых символов
Кнопка «Ввести в домен»	Ввод сервера в домен
Поле «Группы домена»	Поле с раскрывающимся списком групп. Активируется после ввода в домен
Элементы управления	
Создать	При нажатии кнопки выполняется сохранение внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу без сохранения внесенных данных

3) Ввести в поля вкладки требуемые значения.
4) Нажать кнопку «Ввести в домен». Будет запущен процесс ввода сервера в домен.
5) После получения сообщения об успешном завершении ввода сервера в домен:
   — все параметры подключения к серверу аутентификации станут недоступны для внесения изменений;
   — в поле «Статус сервера» отобразится текст «Введен»;
   — кнопка «Ввести в домен» заменится на кнопку «Вывести из домена». Администратор будет иметь возможность вывода сервера ПК из домена.

Вывод сервера ПК из домена выполняется после нажатия кнопки «Вывести из домена» и ввода в окне, аналогичном окну ввода в домен (см. рис. 112). При этом параметры подключения, установленные ранее, не удаляются и могут быть применены для повторного ввода сервера в домен или изменены.

10.3.2.2 Редактирование соединения Active Directory

Для редактирования подключения пользователю необходимо:

1) Выбрать в блоке нужное подключение и нажать на его имя. Откроется страница редактирования выбранного подключения AD.
2) Внести требуемые изменения в поля страницы.

3) Нажать кнопку «Сохранить».

Для удаления соединения пользователю необходимо:

1) Нажать в строке удаляемого соединения кнопку «Удалить» ( ).
2) Нажать в открывшемся окне подтверждения кнопку «Удалить». Соединение будет удалено.

10.3.3 Профили сертификатов

Данный подраздел предназначен для ведения (создание/удаление/редактирование) списка профилей сертификатов, используемых при настройке политик аутентификации в политиках доступа устройств (рис. 113).

После установки и первичной настройки комплекса используются самоподписанные корневой и серверный сертификаты (далее – сертификаты «по умолчанию»). Удаление сертификатов «по умолчанию» недоступно пользователю.

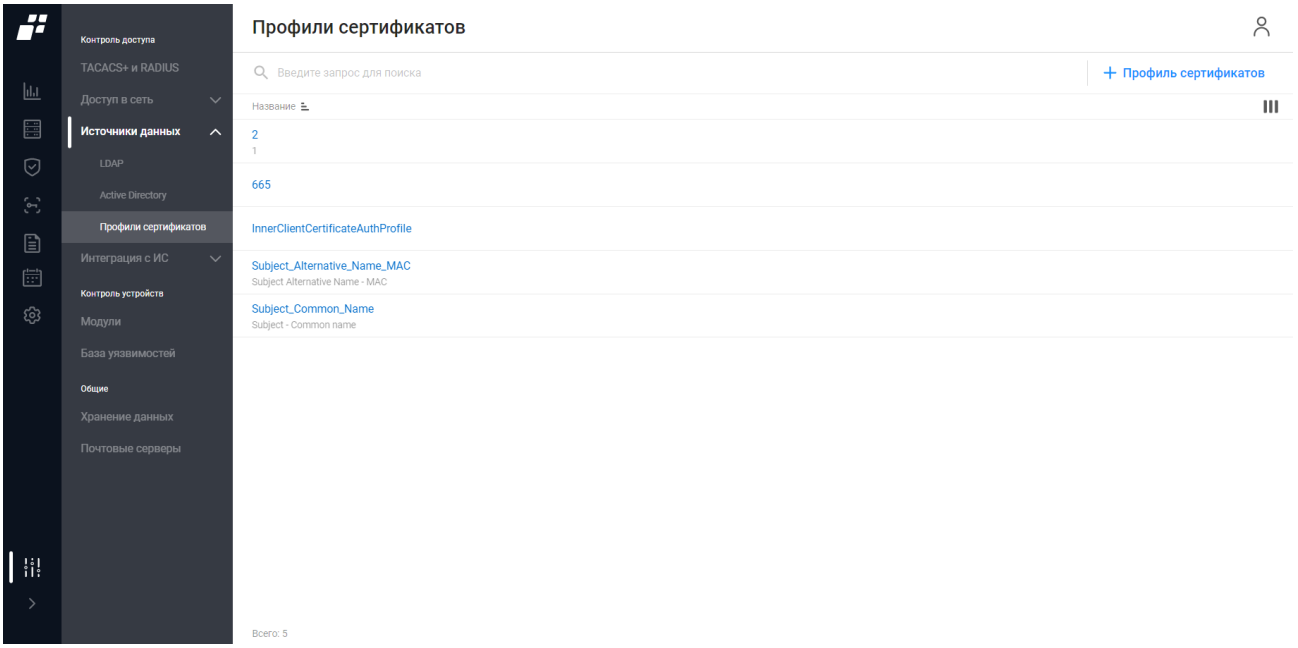


Рисунок 113 – Вкладка «Профили сертификатов»

На странице список профилей сертификатов реализован в виде таблицы. Для каждой записи списка отображаются следующие данные:

— название профиля сертификата;

— описание профиля сертификата.

Над списком профилей располагаются:

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

— кнопка «Профиль сертификатов» (+ Профиль сертификатов);

— кнопка «Колонки» ( ) для изменения отображения колонок на странице.

При наведении курсора на строку с настройкой, в правой части строки появляется

кнопка «Удалить» ( ) для удаления настройки.

10.3.3.1 Создание нового профиля сертификата

Для создания профиля сертификата пользователю необходимо:

1) Нажать на кнопку «Профиль сертификатов» (+ Профиль сертификатов).
2) Откроется окно «Создание профиля сертификатов» (см. рис. 114). Состав и описание полей окна приведены в таблице 49.

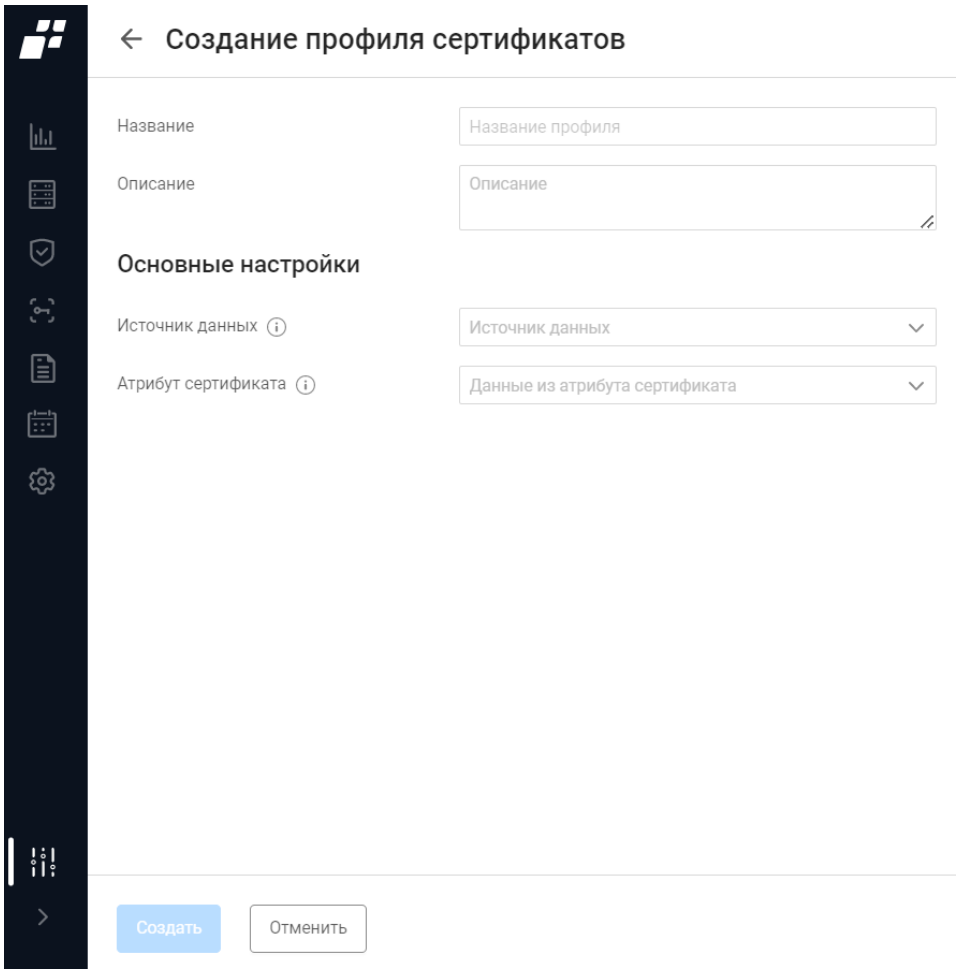


Рисунок 114 – Окно «Создание профиля сертификатов»

Таблица 49 – Состав и описание полей окна «Создание профиля сертификатов»

Поле	Описание
Поле «Название»	Текстовое поле для ввода названия профиля сертификата. Параметры ввода текста: от 1 до 50 символов. Допустимые символы: буквы латинского алфавита, цифры, «_», «–»
Поле «Описание»	Текстовое поле для ввода описания профиля сертификата. Параметры ввода текста: от 1 до 250 символов. Допустимые символы: буквы латинского алфавита, цифры,

Поле	Описание
	«_», «–»
Основные настройки	
Поле «Источник данных»	Поле с раскрывающимся списком источников данных
Поле «Атрибут сертификата»	Поле с раскрывающимся списком: — «Subject-CommonName»; — «Subject»; — «Subject Alternative Name – EMAIL»; — «Subject Alternative Name – UPN»; — «Subject Alternative Name – DNS»
Элементы управления	
Создать	При нажатии кнопки выполняется сохранение внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу без сохранения внесенных данных

3) Ввести в поля вкладки требуемые значения.
4) Нажать кнопку «Создать».

10.3.3.2 Редактирование профиля сертификата

Для редактирования подключения пользователю необходимо:

1) Выбрать в списке нужный профиль сертификата и нажать на имя. Откроется страница редактирования выбранного профиля сертификата.
2) Внести требуемые изменения в поля страницы.
3) Нажать кнопку «Сохранить».

Для удаления профиля пользователю необходимо:

1) Нажать в строке удаляемого соединения кнопку «Удалить» ( ).
2) Нажать в открывшемся окне подтверждения кнопку «Удалить».

10.4 Модули

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

Данный подраздел предоставляет пользователю комплекса информацию о всех внешних модулях, подключенных к ПК.

Модули соединяют сервер с устройствами по различным коммуникационным протоколам и бывают следующие:

- модули сетевые;
- модули виртуализации;
- модули операционных систем;
- модули сервисные;
- модули приложения;
- пользовательские модули.

10.4.1 Просмотр установленных модулей

На странице список модулей реализован в виде таблицы (рис. 115).

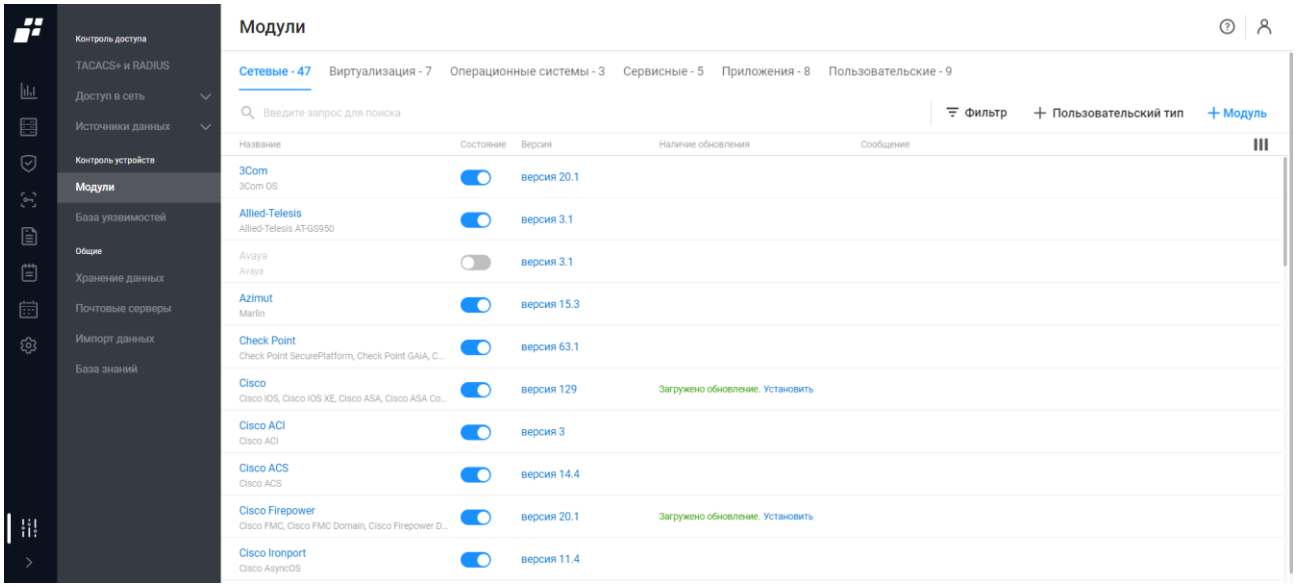


Рисунок 115 – Вкладка «Сетевые»

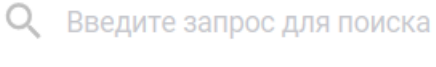
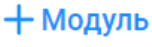
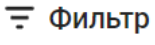
Для каждой записи списка отображаются следующие данные[8]:

- название модуля – доступна сортировка по имени модуля в алфавитном порядке;
- состояние модуля (подключен/отключен);

[8] Для пользовательских модулей отображаются только название и состояние

— версия модуля;
— наличие обновления;
— краткое сообщение.

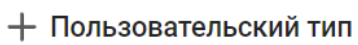
Над списком доступны следующие функции:

— поле поиска () для поиска искомой записи в списке;
— кнопка «Добавить модуль» () для добавления нового модуля;
— кнопка «Пользовательский тип» () для добавления пользовательского типа сетевого устройства;
— кнопка «Фильтр» () для фильтрации списка модулей;
— кнопка «Колонки» () для изменения отображения колонок на странице.

Состав и описание вкладок «Виртуализация», «Операционные системы», «Сервисные», «Приложения», «Пользовательские» подраздела «Модули» аналогичен составу вкладки «Сетевые».

10.4.2 Добавление пользовательского типа сетевого устройства

Для добавления пользовательского типа сетевого устройства для подключения к комплексу отдельных типов устройств администратору необходимо:

1) В заголовке любой вкладки «Модули» нажать кнопку «Пользовательский тип» ().
2) Откроется окно «Создание пользовательского типа сетевого устройства» (рис. 116). Состав и описание полей окна «Создание пользовательского типа сетевого устройства» приведены в таблице 50.

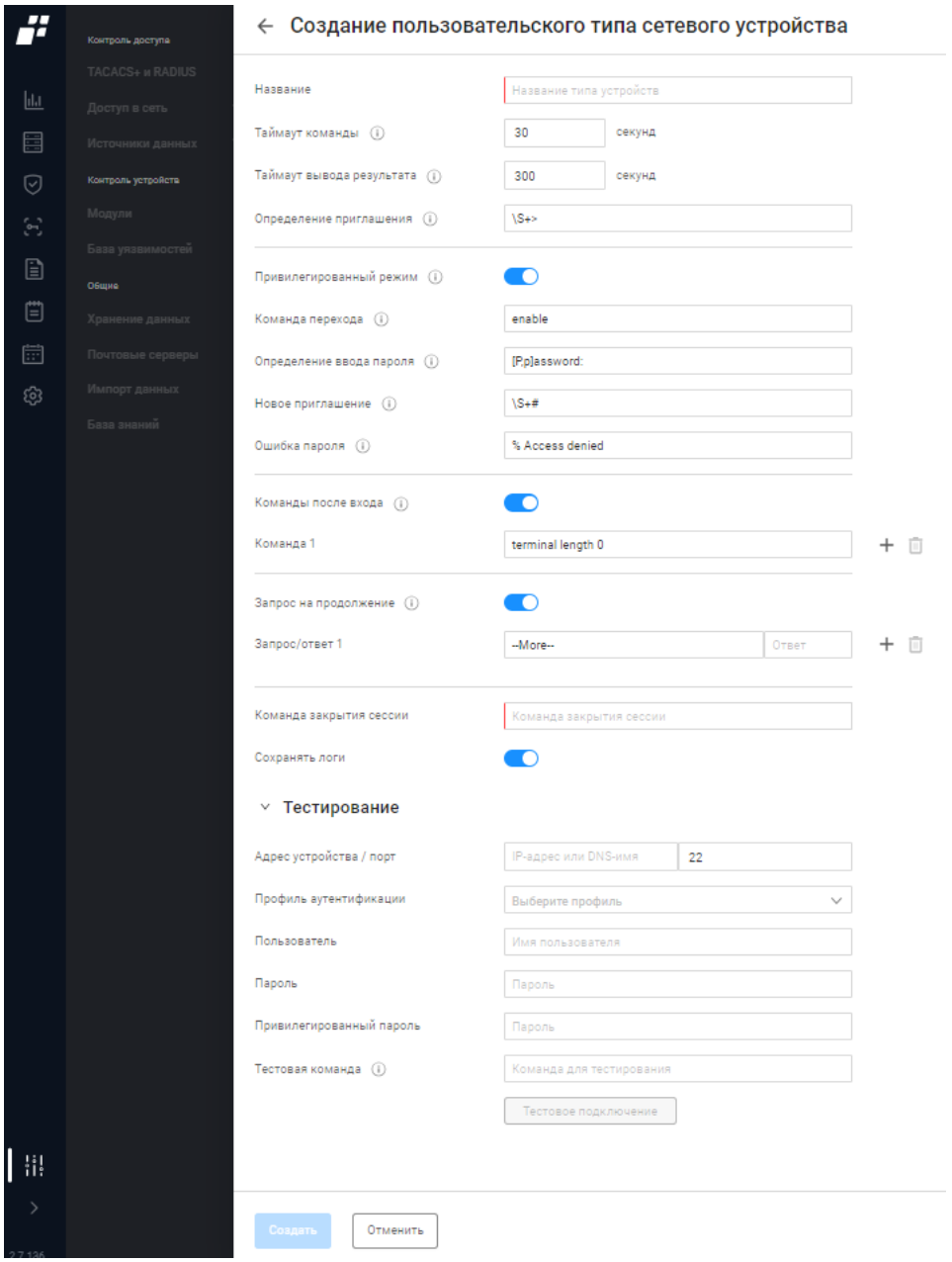


Рисунок 116 – Окно «Создание пользовательского типа сетевого устройства»

Таблица 50 – Состав и описание полей окна «Создание пользовательского типа сетевого устройства»

Поле	Описание
Поле «Название»	Текстовое поле для ввода названия пользовательского типа сетевого устройства. Параметры ввода текста: от 1 до 255 любых символов
Поле «Таймаут команды»	Время ожидания ответа при выполнении команд на устройстве (секунд)
Поле «Таймаут	Время ожидания вывода результата при запросе

Поле	Описание
вывода результата»	конфигурации устройства (секунд)
Поле «Определение приглашения»	Регулярное выражение для определения вида приглашения. Параметры ввода текста: от 1 до 255 любых символов
Поле «Привилегированный режим»	Переключатель с двумя положениями: — «Включен» ( ) – включает привилегированный режим и дополнительные поля настройки режима; — «Выключен» ( ) – выключает привилегированный режим и дополнительные поля настройки режима. По умолчанию переключатель установлен в положение «Включен» и поля для ввода параметров работы в привилегированном режиме отображаются в окне
Блок полей для работы в привилегированном режиме	
Поле «Команда перехода»	Команда перехода в привилегированный режим. Значение по умолчанию: enable. Параметры ввода текста: от 1 до 250 любых символов
Поле «Определение ввода пароля»	Регулярное выражение для определения приглашения ввода пароля при переходе в привилегированный режим. Параметры ввода текста: от 1 до 255 любых символов
Поле «Новое приглашение»	Регулярное выражение для определения вида приглашения в привилегированном режиме. Если приглашение не меняется, то поле оставляется пустым
Поле «Ошибка пароля»	Регулярное выражение для определения ошибки пароля. Параметры ввода текста: от 1 до 250 любых символов
Поле «Команды после входа»	Переключатель с двумя положениями: — «Включен» ( ) – включает отображение полей дополнительного набор команд; — «Выключен» ( ) – выключает отображение полей дополнительного набор команд. По умолчанию переключатель установлен в положение «Включен» и поля для ввода команд Команда 1..N (см. ниже) отображаются в окне
Блок полей для добавления дополнительных команд	
Поле «Команда 1..N»	Поля для ввода дополнительных команд для настройки устройства.

Поле	Описание
	Параметры ввода текста: от 1 до 250 любых символов
Поле «Запрос на продолжение»	Переключатель с двумя положениями: — «Включен» () – включает отображение полей с запросами на продолжение; — «Выключен» () – выключает отображение полей с запросами на продолжение. По умолчанию переключатель установлен в положение «Включен» и поля для ввода запросов/ответов Запрос/ответ 1..N (см. ниже) отображаются в окне
Поле «Запрос/ответ 1…N»	Поля для ввода регулярных выражений запросов и соответствующих ответов. По умолчанию, если поле на заполнено, то будет отправляться «пробел». Параметры ввода текста: от 1 до 250 любых символов
Поле «Команда закрытия сессии»	Текстовое поле ввода команды. Параметры ввода текста: от 1 до 255 любых символов
Сохранять логи	Переключатель с двумя положениями: — «Включен» () – включает сохранение логов сессии; — «Выключен» () – выключает сохранение логов сессии
Группа полей «Тестирование»	
Поле «Адрес устройства / порт»	IP-адрес или доменное имя устройства
Поле «Профиль аутентификации»	Раскрывающийся список созданных профилей аутентификации в комплексе. Профиль аутентификации содержит в себе имя учетной записи (логин) и пароль, которые будут использоваться при аутентификации на контролируемом устройстве
Поле «Пользователь»	Логин пользователя для аутентификации на устройстве
Поле «Пароль»	Пароль пользователя для аутентификации на устройстве
Поле «Привилегированный пароль»	Пароль пользователя для осуществления входа на устройство в привилегированном режиме. Поле отображается на вкладке только при включенном

Поле	Описание
	переключателе «Привилегированный режим»
Поле «Тестовая команда»	Команда для тестирования загрузки конфигурации с устройства. Например, «show version» – отображение текущей версии для устройств типа Cisco IOS. Поле обязательно для заполнения
Элементы управления	
Кнопка «Добавить» (+)	При нажатии кнопки добавляется новое поле для дополнительной команды/запроса/ответа
Кнопка «Удалить» (🗑)	При нажатии кнопки удаляется добавленное поле для дополнительной команды/запроса/ответа
Кнопка «Тестовое подключение»	По нажатию кнопки выполняется проверка подключения и выполнения заданной команды
Создать	При нажатии кнопки выполняется сохранение внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу без сохранения внесенных данных

3) Заполнить все необходимы параметры и нажать кнопку «Создать».

Пользовательский модуль доступен, как и другие модули, для редактирования настроек, отключения/подключения и удаления.

10.4.3 Фильтрация модулей

Для фильтрации модулей необходимо нажать кнопку «Фильтр» (Фильтр). Откроется окно фильтрации, приведенное на рис. 117. Состав полей окна и правила их заполнения приведены в таблице 51

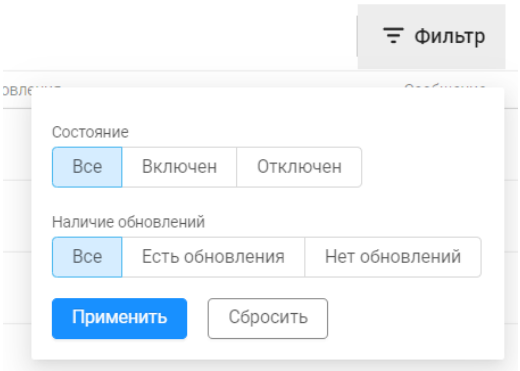


Рисунок 117 – Окно фильтрации списка АСО

Таблица 51 – Состав и описание полей окна фильтрации модулей

Поле	Описание
Поле «Состояние»	Поле с тремя вариантами выбора состояния модулей: — «Все»; — «Включен»; — «Отключен»
Поле «Наличие обновлений»	Поле с тремя вариантами выбора: — «Все»; — «Есть обновления»; — «Нет обновлений». Поле отсутствует в фильтре для пользовательских модулей
Элементы управления	
Сбросить	При нажатии кнопки окно фильтрации закрывается без применения введенных настроек
Применить	При нажатии кнопки окно фильтрации закрывается, введенные настройки фильтрации применяются

Далее необходимо отметить необходимые параметры фильтрации и нажать кнопку «Сохранить». После чего окно фильтрации закроется, а в таблице отобразятся записи с оборудованием, соответствующие заданным параметрам фильтрации;
Для отмены заданных правил фильтрации и отображения в таблице всех записей необходимо повторно нажать на кнопку «Фильтр» и далее нажать кнопку «Сбросить».

10.4.4 Настройка модуля

Для настройки модуля необходимо нажать на название-ссылку любого модуля. Откроется окно настройки, см. рис. 118:

— выбрать установкой флага «Разрешить сохранение логов»;
— нажать кнопку «Сохранить».

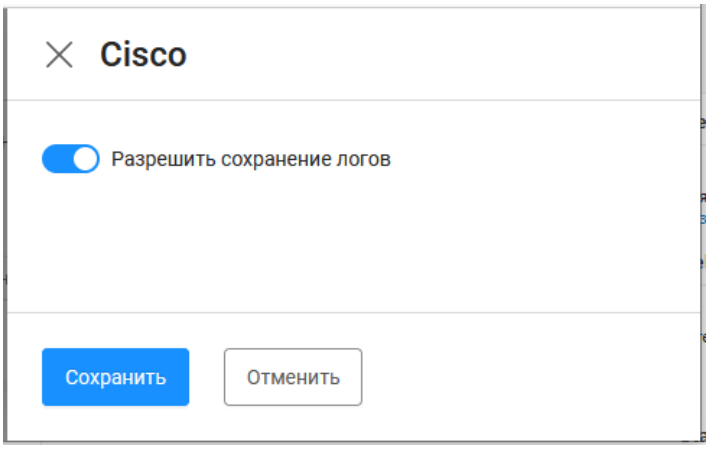


Рисунок 118 – Окно настройки

10.5 База уязвимостей

Подраздел «База уязвимостей» доступен при наличии лицензии на функциональный модуль «Efros VC».

Данный подраздел предоставляет пользователю информацию об общем количестве уязвимостей, выявленных на устройствах, и времени обнаружения (рис. 119).

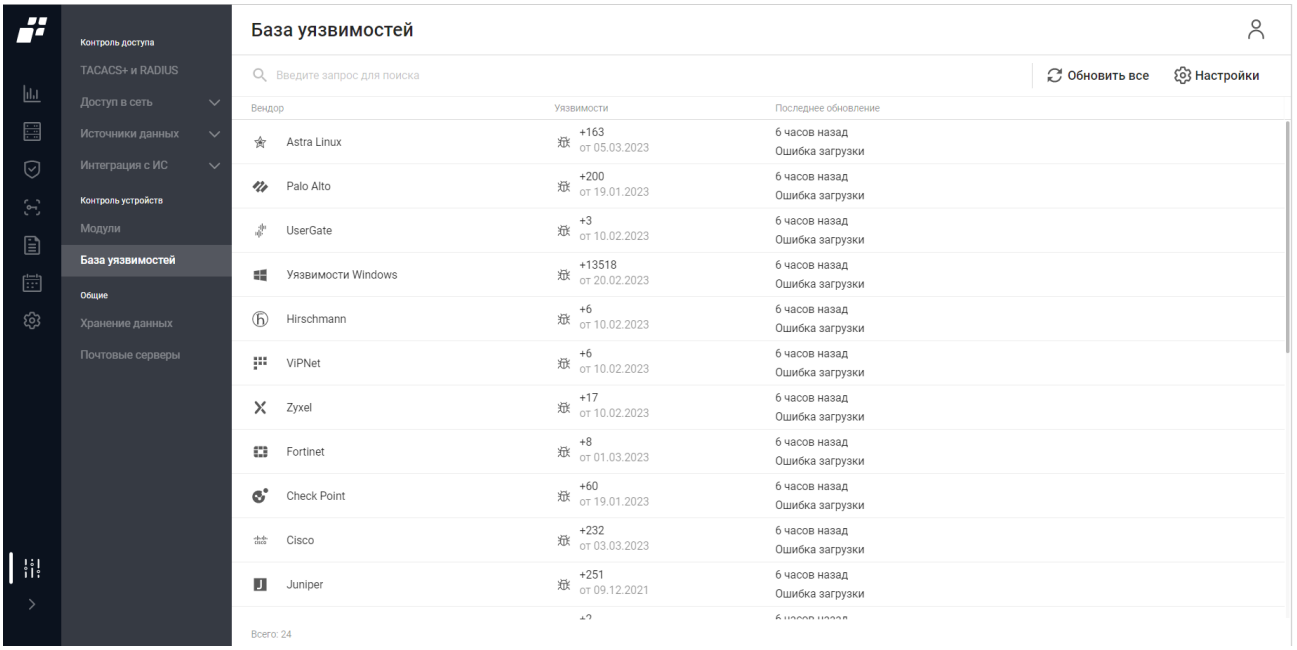


Рисунок 119 – Подраздел «База уязвимостей»

На странице список модулей реализован в виде таблицы.
Для каждой записи списка отображаются следующие данные:

- вендор;
- количество уязвимостей, выявленных вендором;
- время последнего обновления базы данных уязвимостей.

Над списком располагаются:

- поле поиска (Введите запрос для поиска) для поиска искомой записи в списке;
- кнопка «Обновить все» (Обновить все) для обновления всех баз уязвимостей;
- кнопка «Настройки» (Настройки) для настройки базы уязвимостей.

При наведении курсора на строку с базой, в правой части строки появляется кнопка «Обновить» ( ) для обновления только выбранной базы уязвимостей.

10.5.1 Настройка базы уязвимостей

Для выполнения настройки базы уязвимостей пользователю необходимо:

1) Нажать на кнопку «Настройки» (Настройки).
2) Откроется окно «Настройка сервера обновлений» (см. рис. 120). Состав и описание полей окна приведены в таблице 52.

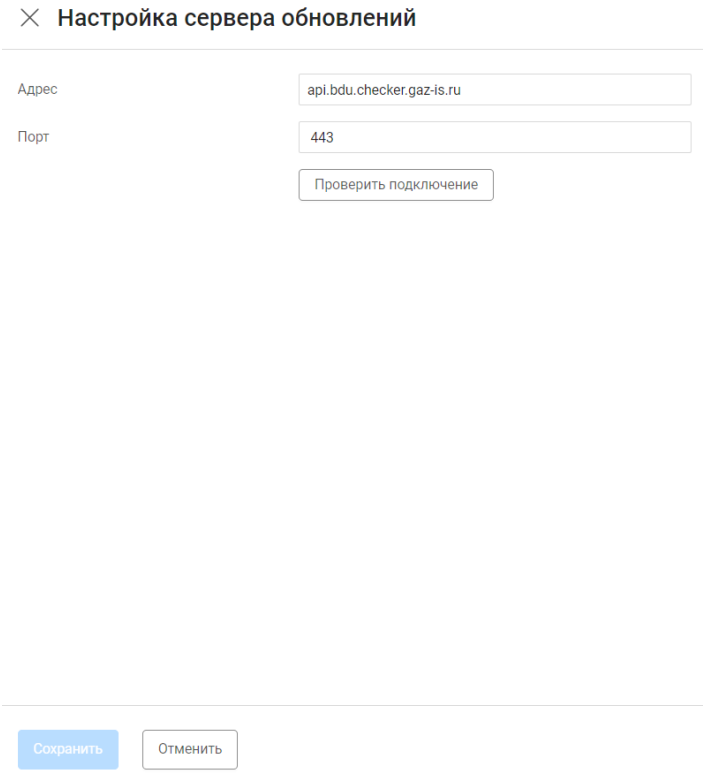


Рисунок 120 – Окно «Настройка сервера обновлений»

Таблица 52 – Состав и описание полей окна «Настройка сервера обновлений»

Поле	Описание
Поле «Адрес»	Поле для введения адреса сервера, на котором расположена база данных уязвимостей
Поле «Порт»	Порт обмена данными с сервером, на котором распложена БДУ. После установки значений адреса и порта необходимо проверить подключение комплекса к серверу БДУ, нажав кнопку «Проверить соединение»
Кнопка «Проверить соединение»	В случае корректно установленных параметров рядом с кнопкой «Проверить подключение» появится надпись *«Успешно»*
Элементы управления	
Сохранить	При нажатии кнопки выполняется сохранение внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу без

Поле	Описание
	сохранения внесенных данных

3) Ввести значения параметров в соответствующие поля.
4) Нажать кнопку «Сохранить».

Введенные значения будут сохранены в БД ПК «Efros DO», будет запущен процесс обновления конфигурационного файла сервиса.

10.6 Хранение данных

Отображаемые данные и доступная функциональность подраздела «Хранение данных» зависит от наличия хотя бы одной лицензии на один из функциональных модулей: «Efros NA», «Efros NAC», «Efros VC», «Efros FA», «Efros NFA» или «Efros ICC».

Данный подраздел позволяет пользователю устанавливать сроки и объем хранения данных по устройствам, событиям и потокам данных для предотвращения переполнения БД комплекса.

На рисунке 121 приведена страница подраздела «Хранение данных».

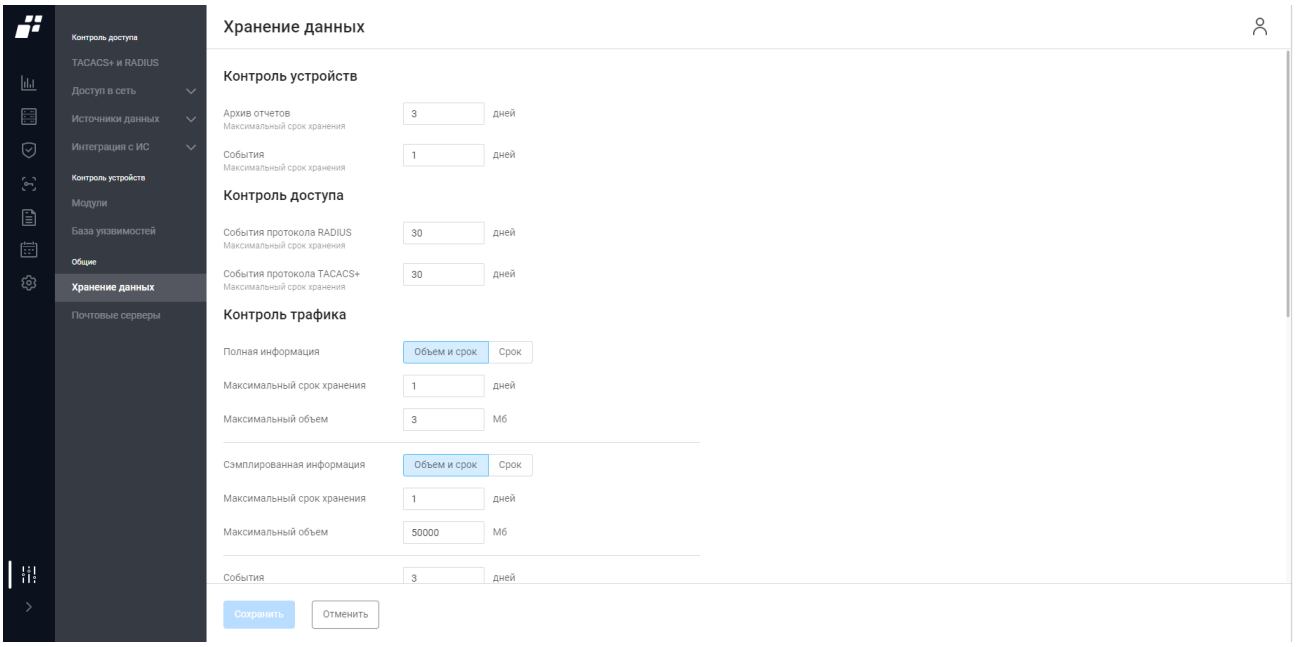


Рисунок 121 – Подраздел «Хранение данных»

Состав и описание полей страницы приведены в таблице

Таблица 53.

Таблица 53 – Состав и описание полей подраздела «Хранение данных»

Поле	Описание
Группа полей «Контроль устройств»	
Поле «Архив отчетов»	Поле для заполнения количества дней хранения отчета
Поле «События»	Поле для заполнения количества дней хранения отчета
Группа полей «Контроль доступа»	
Поле «События доступа на оборудование»	Поле для заполнения количества дней хранения отчета
Поле «События доступа в сеть»	Поле для заполнения количества дней хранения отчета
Группа полей «Контроль трафика»	
Поле «Полная информация»	Переключатель с двумя вариантами: — *«Объем и срок» – архив хранится определенное время. — «Срок» – архив хранится определенное время. *При выборе поля «Объем и срок» появляются поля «Максимальный срок хранения» в днях и «Максимальный объем» в Мб
Поле «Сэмплированная информация»	Переключатель с двумя вариантами: — *«Объем и срок» – архив хранится определенное время. — «Срок» – архив хранится определенное время. *При выборе поля «Объем и срок» появляются поля «Максимальный срок хранения» в днях и «Максимальный объем» в Мб
Поле «События»	Указывается максимальный срок хранения событий в днях
Поле «Счетчики утилизации интерфейсов»	Переключатель с двумя вариантами: — *«Объем и срок» – архив хранится определенное время. — «Срок» – архив хранится определенное время *При выборе поля «Объем и срок» появляются поля «Максимальный срок хранения» в днях и «Максимальный объем» в Мб
Группа полей «Общее»	
Поле «Срабатывание планировщика»	Поле для заполнения количества дней хранения отчета событий планировщика

Поле	Описание
Поле «События по ОЗ»	Переключатель с двумя вариантами: — *«Объем и срок» – архив хранится определенное время. — «Срок» – архив хранится определенное время *При выборе поля «Объем и срок» появляются поля «Максимальный срок хранения» в днях и «Максимальный объем» в Мб
Поле «Системные события»	Поле для заполнения количества дней хранения отчета по системным событиям
Поле «Аудит действий пользователя»	Переключатель с двумя вариантами: — *«Объем и срок» – архив хранится определенное время; — «Срок» – архив хранится определенное время. *При выборе поля «Объем и срок» появляются поля «Максимальный срок хранения» в днях и «Максимальный объем» в Мб
Элементы управления	
Сохранить	При нажатии кнопки выполняется сохранение внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу без сохранения внесенных данных

10.7 Почтовые серверы

Отображаемые данные и доступная функциональность подраздела зависит от наличия хотя бы одной из лицензий.

Данный подраздел позволяет пользователю настраивать параметры отправки почтовых сообщений.

На рисунке 122 приведена страница подраздела «Почтовые серверы».

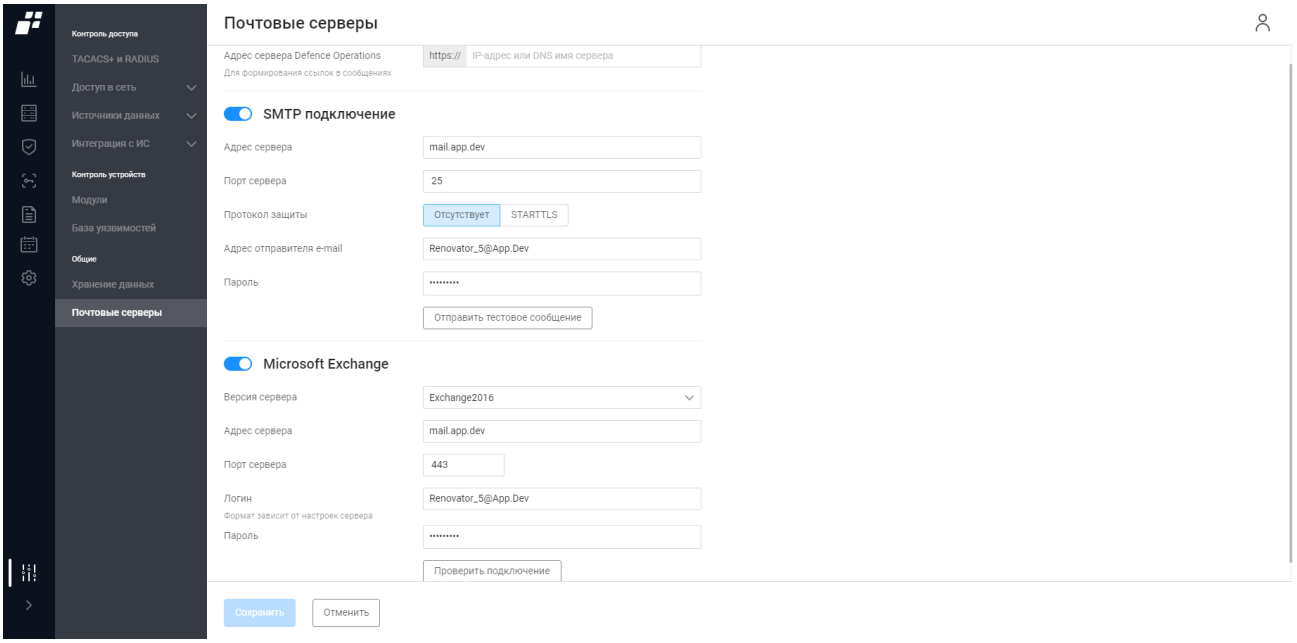


Рисунок 122 – Подраздел «Почтовые серверы»

Состав и описание полей страницы приведены в таблице 54.

Таблица 54 – Состав и описание полей подраздела «Почтовые серверы»

Поле	Описание
Поле «Адрес сервера Defence Operations»	Поле для указания DNS-имени или IP-адреса сервера ПК «Efros DO»
Группа полей «SMTP подключение»	
Поле «SMTP подключение»	Переключатель для включения/отключения блоков настройки SMTP подключения
Поле «Адрес сервера»	Адрес почтового сервера
Поле «Порт сервера»	Порт выбранного выше почтового сервера
Протокол защиты	Переключатель для выбора протокола: — «Отсутствует»; — «STARTTLS»

Поле	Описание
Поле «Fingerprint ключа сервера»	Переключатель для включения/отключения сбора информации об удаленном сервере. Поле отображается, если выбран протокол STARTTLS
Поле «Адрес отправителя e–mail»	Почта отправителя сообщения
Поле «Пароль»	Пароль отправителя сообщения
Кнопка «Отправить тестовое сообщение»	Позволяет проверить настройки подключения путем отправки сообщения на указанную выше почту
Группа полей «Microsoft Exchange»	
Поле «Microsoft Exchange»	Переключатель для включения/отключения блоков настройки Microsoft Exchange
Поле «Версия сервера»	Окно с раскрывающимся списком версий сервера Exchange
Поле «Адрес сервера»	Адрес выбранной выше версии сервера
Поле «Порт сервера»	Порт выбранного выше сервера
Поле «Логин»	Логин пользователя
Поле «Пароль»	Пароль пользователя
Поле «Максимальный размер вложений»	Максимальный суммарный размер вложений, прикрепленных к сообщению
Кнопка «Проверить подключение»	При нажатии кнопки выполняется проверка успешности установления соединения с введенными параметрами к указанному серверу
Элементы управления	
Сохранить	При нажатии кнопки выполняется сохранение внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу без сохранения внесенных данных

10.8 Импорт данных

Отображаемые данные и доступная функциональность в подразделе «Импорт данных» зависят от наличия лицензии на функциональный модуль «Efros NAC».

Данный подраздел позволяет пользователю импортировать необходимые данные исключая ввод их вручную (рис. 123).

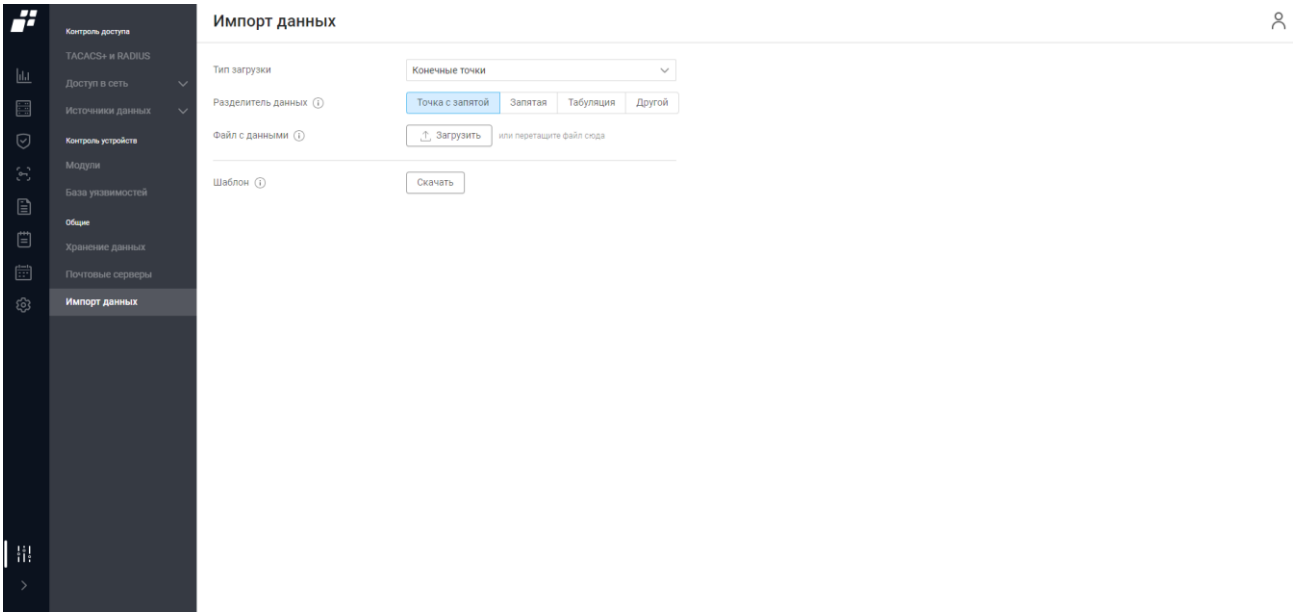


Рисунок 123 – Подраздел «Импорт данных»

Состав и описание полей страницы приведены в таблице 54.

Таблица 55 – Состав и описание полей подраздела «Импорт данных»

Поле	Описание
Поле «Тип загрузки»	Раскрывающийся список с выбором типа загружаемых данных: — «MAB»; — «Конечные точки»; — «Сетевые пользователи»; — «Сетевые устройства»
Поле «Разделитель данных»	Разделитель полей для загружаемого CSV-файла или шаблона. Переключатель: — «Точка с запятой»; — «Запятая»; — «Табуляция»; — «Другой». При выборе «Другой» в поле «Пользовательский разделитель» необходимо указать разделитель данных

Поле	Описание
Поле «Файл с данными»	Поле для загрузки заполненного шаблона необходимыми данными
Поле «Шаблон»	Экспорт файла шаблона в формате csv для заполнения необходимыми данными

Для импорта данных пользователю необходимо выполнить следующие шаги:

1) Выбрать тип загрузки данных из предлагаемых вариантов (рис. 124)

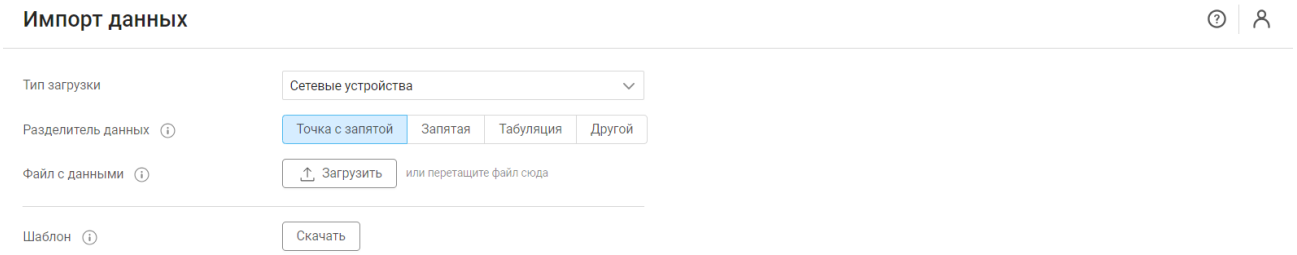


Рисунок 124 – Выбор типа загрузки

2) Скачать шаблон на локальную ЭВМ.
3) Заполнить шаблон необходимыми данными и загрузить.
4) Или загрузить готовый файл с данными.

Загружаемый файл должен соответствовать следующим требованиям:

1. Допустимый формат файла csv.
2. Размер файла не должен превышать 50 Мб.
3. Структура файла (строки заголовков) соответствует последней версии шаблона для выбранного типа загрузки (при необходимости сверить и откорректировать заголовки в шаблоне и пользовательском файле).
4. В файле должна присутствовать хотя бы одна строка с данными для импорта.
5. Атрибуты должны содержать корректные значения.

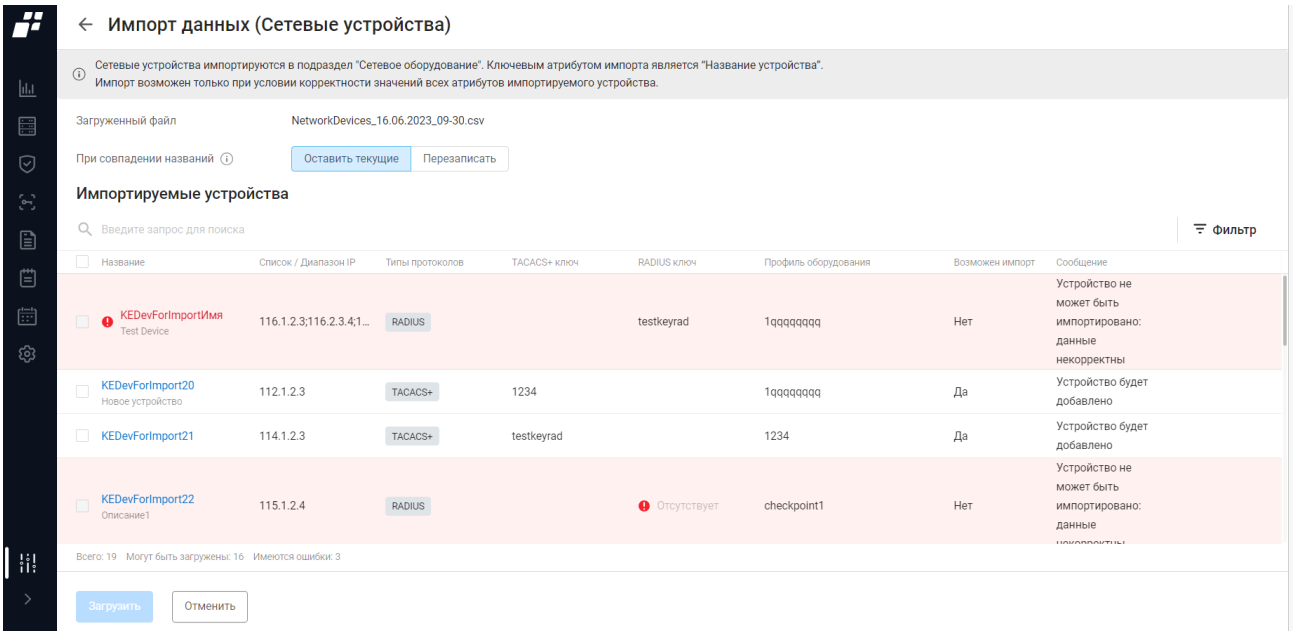


Рисунок 125 – Выбор типа загрузки

5) Список данных отобразится на странице в виде таблицы. Состав и описание полей страницы приведены в таблице 56.

Строки устройств, требующие корректировки, подсвечены красным.

Таблица 56 – Состав и описание полей подраздела «Импорт данных»

Поле	Описание
Поле «Загруженный файл»	Название загруженного файла с данными
Поле «При совпадении названий»	Переключатель: — «Оставить текущие» – из файла с данными в БД комплекса будут добавлен только новые сетевые устройства; — «Перезаписать» – данные существующих сетевых устройств будут заменены данными из файла импорта
Поле «Импортируемые устройства»	Сетевые устройства с данными по каждому устройству
Элементы управления	
Поле поиска (Введите запрос для поиска)	Для поиска искомой записи в списке
Кнопка «Фильтр» (Фильтр)	Для фильтрации данных в загруженной таблице

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

6) Необходимо выполнить корректировку данных у объектов.
7) Необходимо определить, оставить текущие данные у устройств (в список устройств комплекса будут добавлены только новые устройства) или перезаписать данные устройств в комплексе данными устройств из файла (в список устройств комплекса будут добавлены новые устройства, а также обновятся данные уже существующих устройств при наличии их в файле).
8) Нажать кнопку «Загрузить».

10.9 База знаний

Отображаемые данные и доступная функциональность в подразделе «База знаний» зависит от наличия хотя бы одной лицензии на функциональные модули.

Данный подраздел позволяет настраивать источники сканирования, которые осуществляют систематический сбор сведений о сетевых ресурсах путем пассивного и активного сканирования сети с помощью протоколов и утилит. На рисунке 126 приведена страница подраздела «База знаний».

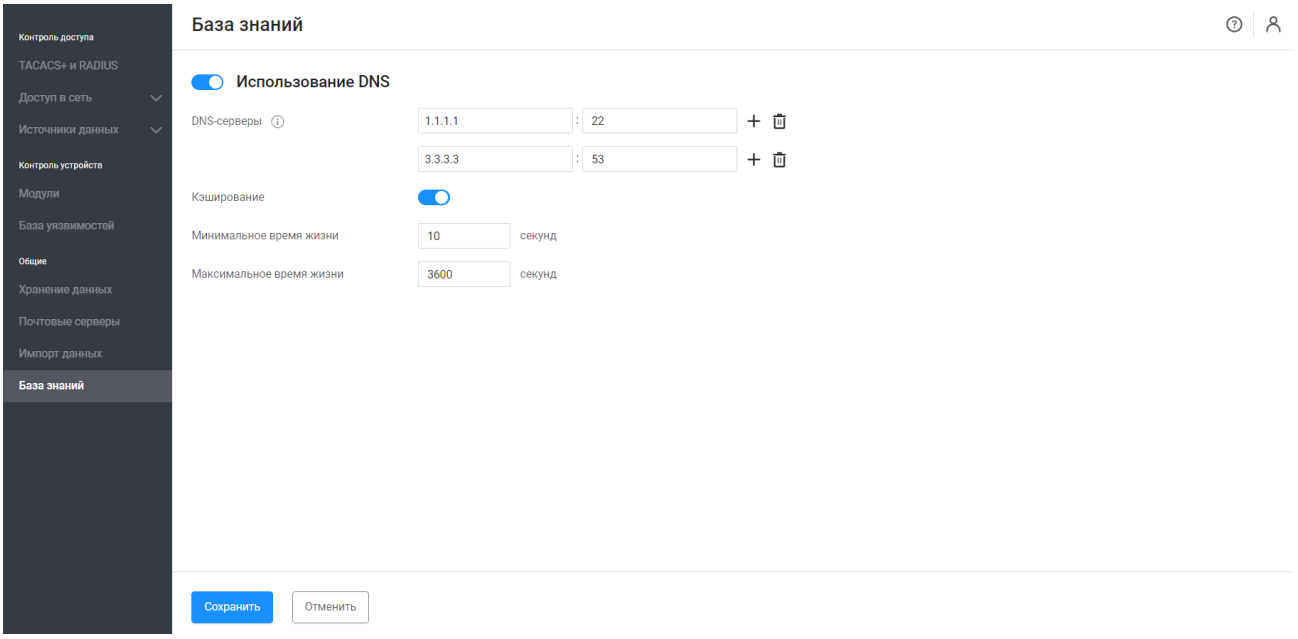


Рисунок 126 – Подраздел «База знаний»

Состав и описание полей страницы приведены в таблице 54.

Таблица 57 – Состав и описание полей подраздела «База знаний»

Поле	Описание
Группа полей «Использование DNS»	
Поле «Использование DNS»	Переключатель. При включении появляются дополнительные поля для добавления DNS-серверов
Поле «DNS-серверы»	Список DNS-серверов, которые будут использоваться для получения доменных имен по IP-адресам. Допустимый формат для адреса сервера: 0-255.0-255.0-255.0-255. Допустимый формат для порта: целочисленное значение в диапазоне от 1 до 65535
Поле «Кэширование»	Переключатель. При включении появляются дополнительные поля для настройки кэширования
Поле «Минимальное	Поле для указания количества секунд хранения кэша

Поле	Описание
время жизни»	
Поле «Максимальное время жизни»	Поле для указания количества секунд хранения кэша
Элементы управления	
Сохранить	При нажатии кнопки выполняется сохранение внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу без сохранения внесенных данных

11 Сообщения об ошибках пользователю

11.1 Ошибки при идентификации

Сообщения об ошибках идентификации будут направлены пользователю в следующих случаях:

- «Неверный логин или пароль» – в случае, если введена неправильная пара логин /пароль или попытка входа под несуществующей записью;
- «Ваша сессия устарела, требуется повторный вход» – в случае, если бездействие пользователя больше времени, указанного в параметре «Блокировка пользователя, при неактивности»;
- «Пользователь заблокирован» – в случае, если осуществляется попытка входа под заблокированным пользователем.

В первом случае пользователю необходимо ввести корректные данные и повторить попытку запуска. В случае, если запись не существует – необходимо обратиться к системному администратору ПК. Во втором случает подождать указанное в параметре «Блокировка пользователя, при неактивности» время и повторить попытку аутентификации. В третьем случае необходимо обратиться к системному администратору ПК.

Кроме того, после нескольких подряд неуспешных попыток аутентификации в комплексе учетная запись пользователя автоматически блокируется на заданный в подразделе «Пользователи» период времени. На странице выводится сообщение: «Пользователь заблокирован из–за превышения количества попыток ввода пароля на {количество_минут} мин». Количество неуспешных попыток запуска также настраивается. Более подробно смотри документ «Руководство пользователя. Часть 1. Администрирование».

Пользователь может повторить попытку входа через указанный в сообщении период времени. Если новая попытка входа повторно неуспешная, то пользователю необходимо обратиться к системному администратору комплекса для уточнения своих данных (логина и пароля).

11.2 Ошибки при создании/редактировании сущности

Если при заполнении полей страницы создания/редактирования сущности комплекса не было заполнено хотя бы одно из обязательных полей или поле заполнено некорректно, то поле будет выделено красной рамкой и под полем отобразится соответствующее сообщение. В этом случае пользователю необходимо заполнить поле корректно и продолжить работу с сущностью.

При попытке создать дубликат уже имеющейся сущности в верхней части страницы добавления отобразится соответствующее сообщение: «Поле {название поля} должно быть уникальным» Пользователю необходимо корректно заполнить поля страницы и повторно нажать кнопку «Создать/Сохранить». Пользователь не может ввести цифровые значения, которые меньше минимально заданного или больше максимально заданного.

Другие виды сообщений при создании/редактировании сущности:

- «Неверный формат поля» – в случае, если пользователь ввел некорректные данные: например, формат поля числовой, пользователь вводит буквенные символы;
- «Пароль может содержать только: латинские буквы обоих регистров, цифры, спец. символы (! @ # & ( ) - _ [{ }] : ; ', ? / * ~ $ ^ + = < >)» – в случае, если при заведении пользователя в поле «Пароль» указывается недопустимый символ;
- «Поле должно быть корректным: '0-255.0-255.0-255.0-255' или '0-255.0-255.0-255.0-255/32'» – в случае, если формат данных в поле не соответствует требуемому значению;
- «Сохранить изменения? Имеются несохраненные параметры в разделе: {название раздела}» – в случае, если пользователь решил перейти со страницы создания/редактирования на другую вкладку/страницу;
- «Недостаточно прав для {название действия} {название сущности}» – в случае, если у пользователя нет требуемой привилегии для работы с сущностью;
- «Выбранный файл не соответствует формату» – в случае, если была попытка загрузки файла не соответствующего формата;
- иные, в зависимости от контекста выполняемых действий.

11.3 Ошибки, связанные с лицензией на ПК «Efros DO»

Ошибки, связанные с лицензией на комплекс:

- «Ключ лицензии неверный» – ошибка в вводе ключа лицензии;
- «Ключ активации неверный» – ошибка в вводе ключа активации;
- «Загружен некорректный файл лицензии» – ошибка в загрузке файла лицензии;
- «По введенному ключу лицензия уже активирована» – повторное использование ключа лицензии;
- «Ошибка удаления лицензии» – сбой при удалении лицензии.

При возникновении других ошибок пользователю рекомендуется обратиться к системному администратору комплекса.

12 Завершение работы ПК «Efros DO»

Для завершения работы с веб-интерфейсом комплекса необходимо в заголовке текущей страницы нажать кнопку «Выход» и закрыть вкладку используемого веб-браузера.

Перечень сокращений

ACL	–	Access Control List
AD	–	Active Directory
AES	–	Advanced Encryption Standard
API	–	Application Programming Interface
CM	–	Change Manager
CN	–	Common Name
CoA	–	Change of Authorization
CPMI	–	Common Management Information Protocol
CRL	–	Certificate Revocation List
CSV	–	Comma-Separated Values
DES	–	Data Encryption Standard
DHCP	–	Dynamic Host Configuration Protocol
DNS	–	Domain Name System
EAP	–	Extensible Authentication Protocol
FAST	–	Flexible Authentication by Secure Tunneling
FQDN	–	Fully Qualified Domain Name
GTC	–	Generic Token Card
HTTP	–	HyperText Transfer Protocol
HTTPS	–	HyperText Transfer Protocol Secure
ICC	–	Integrity Check Compliance
ICMP	–	Internet Control Message Protocol
IIS	–	Internet Information Services
IP	–	Internet Protocol
IPFIX	–	Internet Protocol Flow Information Export
LDAP	–	Lightweight Directory Access Protocol
LDAPS	–	Lightweight Directory Access Protocol over SSL
MAB	–	MAC Authentication Bypass
MAC	–	Media Access Control
MD5	–	Message Digest 5
MSCHAPv2	–	Microsoft Challenge-Handshake Authentication Protocol v.2
NA	–	Network Assurance

NAC	–	Network Access Control
NFA	–	Network Flow Analysis
OCSP	–	Online Certificate Status Protocol
OU	–	Organization Unit
PEAP	–	Protected Extensible Authentication Protocol
RADIUS	–	Remote Authentication in Dial-In User Service
REST	–	Representational State Transfer
SAN	–	Subject Alternative Name
SCP	–	Secure Copy
SFTP	–	Secure File Transfer Protocol
SHA	–	Secure Hash Algorithm
SMTP	–	Simple Mail Transfer Protocol
SNMP	–	Simple Network Management Protocol
SP	–	Service Pack
SQL	–	Structured Query Language
SSH	–	Secure SHell
SSL	–	Secure Sockets Layer
SYSLOG	–	System Log
TACACS+	–	Terminal Access Controller Access Control System plus
TDS	–	Tabular Data Stream
TELNET	–	TELecommunication NETwork
TLS	–	Transport Layer Security
TTLS	–	Tunneled Transport Layer Security
UDP	–	User Datagram Protocol
URL	–	Uniform Resource Locator
VC	–	Vulnerability Control
XML-RPC	–	eXtensible Markup Language Remote Procedure Call
АСО	–	Активное сетевое оборудование
БД	–	База данных
БДУ	–	База данных уязвимостей
ГОСТ	–	Государственный стандарт
МЭ	–	Межсетевой экран
НКЦКИ	–	Национальный координационный центр по компьютерным

		инцидентам
ОЗ	–	Объект защиты
ОС	–	Операционная система
ПК	–	Программный комплекс
ППО	–	Прикладное программное обеспечение
СУБД	–	Система управления базами данных
ФСТЭК России	–	Федеральная служба по техническому и экспортному контролю России
ЭВМ	–	Электронно-вычислительная машина

Приложение А

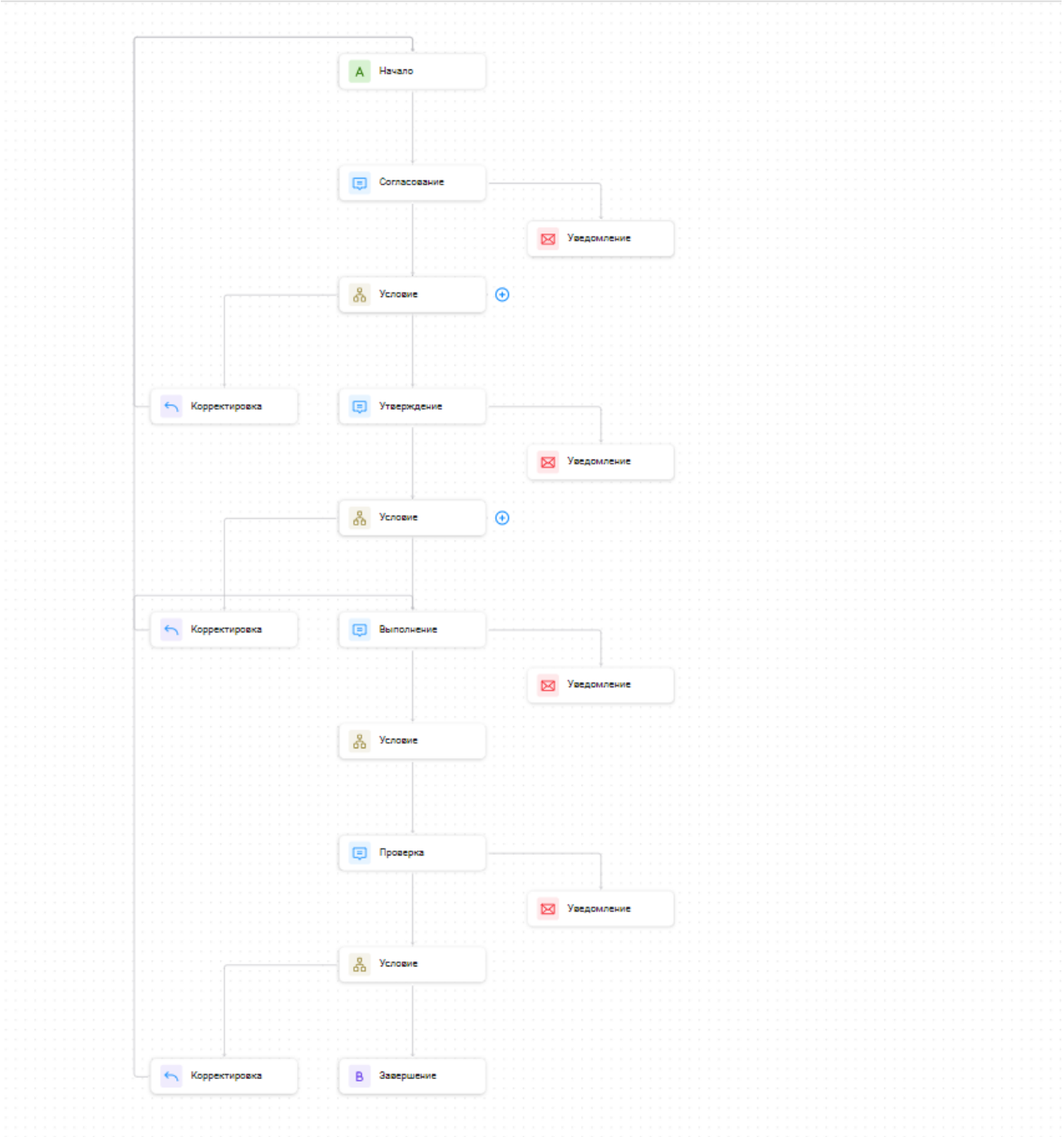


Рисунок 127 – Пример маршрута

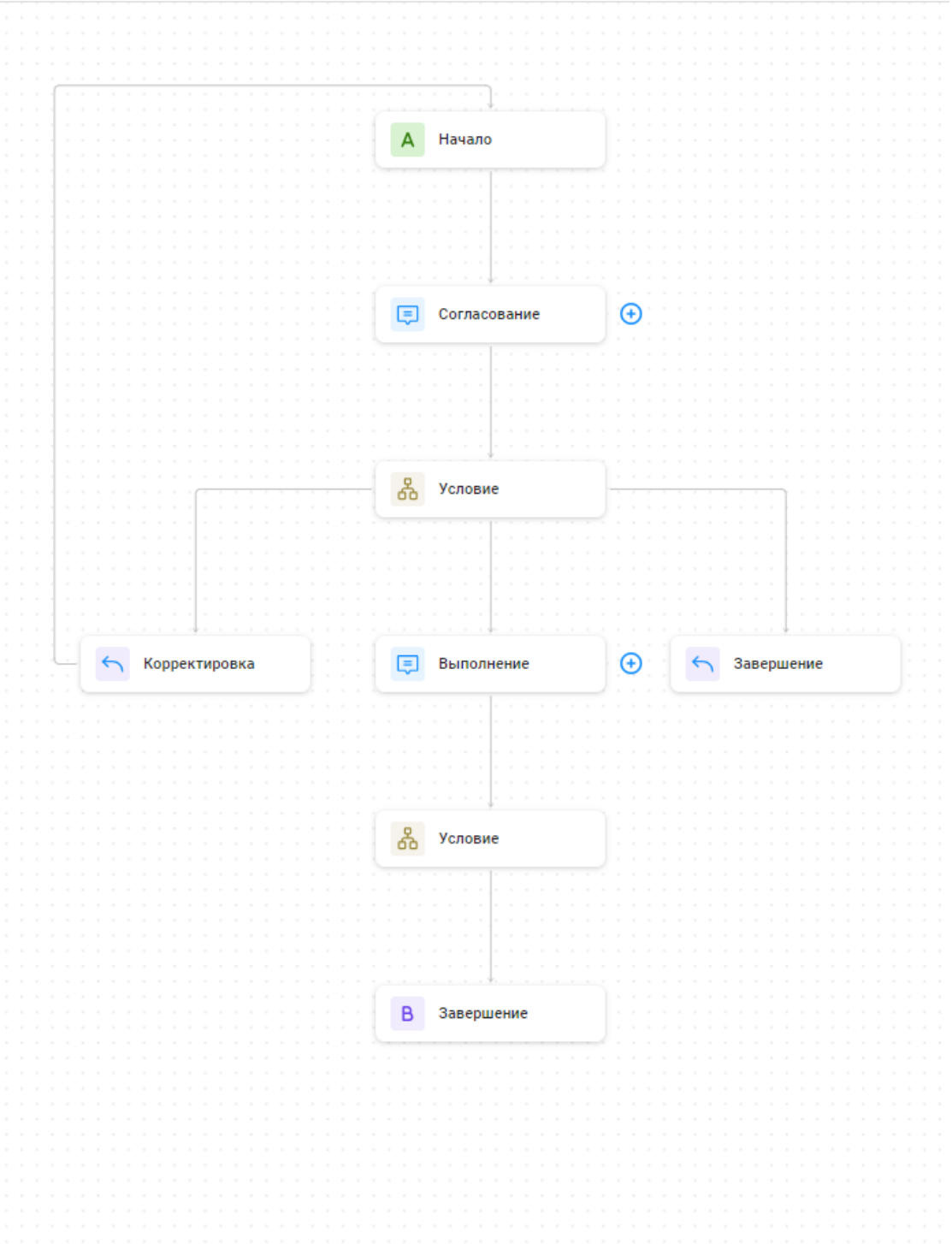


Рисунок 128 – Пример маршрута