ГАЗИНФОРМ СЕРВИС

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

Руководство пользователя
Часть 1

Администрирование

Санкт-Петербург, 2024

Аннотация

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

Руководство пользователя ПК «Efros DO» содержит сведения, необходимые пользователям для работы с персональной электронно-вычислительной машиной (ПЭВМ) пользователя в процессе выполнения доступных функций ПК «Efros DO».

Руководство состоит из следующих частей:

- часть 1 (данный документ) – содержит сведения, необходимые для настройки доступа пользователей ПК «Efros DO» к сетевым ресурсам и функциям, а также описание выполнения функций контроля работы объектов сети с использованием веб-интерфейса;
- часть 2 – содержит сведения, необходимые для настройки и конфигурирования функций контроля устройств;
- часть 3 – содержит сведения, необходимые для настройки и конфигурирования функций контроля доступа;
- часть 4 – содержит сведения, необходимые для настройки возможностей контроля целостности функционального модуля «Efros Integrity Check Compliance» («Efros ICC»);
- часть 5 – содержит сведения, необходимые для настройки агента «Efros Defence Operations».

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»

1.1 Назначение

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

- контроль конфигураций и топологии сети;
- оптимизация и настройка межсетевых экранов (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;
- защита DNS.

Доступность функциональных возможностей ПК «Efros DO» зависит от состава приобретенных лицензий на функциональные модули ПК «Efros DO»: «Efros Network Assurance» («Efros NA»), «Efros Firewall Assurance» («Efros FA»), «Efros Network Access Control» («Efros NAC»), «Efros Integrity Check Compliance» («Efros ICC»), «Efros Vulnerability Control» («Efros VC»), «Efros Network Flow Analysis» («Efros «NFA»), «Efros Change Manager» («Efros CM»), «Efros Secure DNS» («Efros DNS»).

Перечень видов лицензий ПК «Efros DO», их обозначение и краткое описание приведены в таблице 1.

Таблица 1 – Перечень видов лицензий ПК «Efros DO», их обозначение и краткое описание

Лицензия функционального модуля		**Описание**
Полное название	**Сокращенное название**	
NETWORK ASSURANCE	NA	Модуль контроля конфигураций и топологии сети
FIREWALL ASSURANCE	FA	Модуль оптимизации и настройки МЭ
CHANGE MANAGER	CM	Модуль анализа и управления объектами

Лицензия функционального модуля		Описание
Полное название	**Сокращенное название**	
		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
SECURE DNS	DNS	Модуль защиты DNS

Каждая лицензия на функциональный модуль имеет определенное количество доступных лицензий на оборудование.

При достижении лимита по количеству лицензий на оборудование добавление нового оборудования или назначение новых функций невозможно. Для того чтобы добавить новое оборудование, необходимо удалить ранее добавленное оборудование или назначенные функции либо приобрести дополнительную лицензию (подробное описание модели лицензирования функциональных модулей программного комплекса приведено в документе «Модель лицензирования» ПК «Efros DO»).

Доступность функциональных возможностей ПК «Efros DO» (разделов веб-интерфейса ПК «Efros DO»), в зависимости от приобретенной лицензии, приведена в таблице 2.

Таблица 2 – Функциональные возможности в зависимости от лицензии

Раздел веб-интерфейса	**Подраздел (вкладка меню)**	**Efros DO***	**Лицензии на функциональные модули**							
			Efros NA	**Efros FA**	**Efros ICC**	**Efros VC**	**Efros NFA**	**Efros NAC**	**Efros CM**	**Efros DNS**
Мониторинг		+								
Объекты сети		+								
	Объекты защиты (дерево устройств)	+								
	Объекты защиты (Контроль устройств)		+	+	+	+				

Раздел веб-интерфейса	Подраздел (вкладка меню)	Efros DO*	Лицензии на функциональные модули							
			Efros NA	Efros FA	Efros ICC	Efros VC	Efros NFA	Efros NAC	Efros CM	Efros DNS
	Объекты защиты (Контроль доступа)							+		
	Объекты защиты (Контроль трафика)						+			
	Объекты защиты (SNMP профили)	+								
	База знаний	+	+		+		+	+		
	Конечные точки							+		
	Карта сети	+								
	Векторы атак					+				
	Сканирование сети	+								
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							+		

Раздел веб-интерфейса	Подраздел (вкладка меню)	Efros DO*	Лицензии на функциональные модули							
			Efros NA	Efros FA	Efros ICC	Efros VC	Efros NFA	Efros NAC	Efros CM	Efros DNS
	Загружаемые ACL							+		
	Наборы команд							+		
	Разрешенные протоколы							+		
	Разрешенные MAC-адреса							+		
	Словари							+		
	Гостевые порталы							+		
Агенты								+		
	Агенты							+		
	Наборы политик							+		
	Профили настроек							+		
	Установка и обновление							+		
Защита DNS										+
	Черный и белый списки									+
	Правила IDS/IPS									+
	Защита DNS-трафика									+
	Серверы пересылки									+
Центр задач		+								
Отчеты		+								
События		+								
	Центр задач	+								
	Объекты сети		+	+	+	+	+	+		
	Аудит	+								
	Доступ в сеть							+		
	Доступ на оборудование							+		
	Системные события		+	+	+	+		+		+
Администриро-	Пользователи	+								

Раздел веб-интерфейса	Подраздел (вкладка меню)	Efros DO*	Лицензии на функциональные модули							
			Efros NA	Efros FA	Efros ICC	Efros VC	Efros NFA	Efros NAC	Efros CM	Efros DNS
вание	Лицензии	+								
	Сертификаты (Доверенные)	+								
	Сертификаты (Системные)	+								
	Сертификаты (Изданные)							+		
	Сертификаты (Шаблоны)	+								
	Сертификаты (Запросы на сертификат)	+								
	Планировщик	+								
Настройки		+								
	TACACS+ и RADIUS							+		
	Источники данных							+		
	Модули		+	+	+	+				
	База уязвимостей					+				
	Хранение данных	+								
	Хранение данных (Контроль устройств)		+	+	+	+				
	Хранение данных (Контроль доступа)							+		
	Хранение данных (Контроль трафика)						+			
	Хранение данных (Общее)	+								
	Хранение данных (База знаний)	+	+		+		+	+		
	Хранение данных (Агенты)							+		
	Почтовые серверы	+								
	Импорт данных							+		

Раздел веб-интерфейса	Подраздел (вкладка меню)	Efros DO*	Лицензии на функциональные модули							
			Efros NA	Efros FA	Efros ICC	Efros VC	Efros NFA	Efros NAC	Efros CM	Efros DNS
	База знаний	+								
	Внешние системы	+								
	Иерархия серверов	+								
*разделы и функциональные возможности, отмеченные знаком «+», входят в базовый набор лицензии на любой функциональный модуль										

1.2 Функциональные возможности программы

ПК «Efros DO» реализует следующие функциональные возможности:

- единая точка доступа (веб-интерфейс) к функциям комплекса и модулям интеграции;
- получение, обработка, интеграция и хранение данных, полученных из событий по объектам защиты (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 администраторов комплекса на сервере ПК «Efros DO» с использованием идентификаторов и паролей;
- ведение списка администраторов 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;
- передача событий безопасности для дальнейшей обработки (SIEM-системы);
- импорт сущностей из сторонних систем согласно заданному шаблону в формате

.csv;

- интеграция со сканерами уязвимостей «MaxPatrol 8», «RedCheck» и «SafeERP Pentest»;
- управление ролями пользователей комплекса;
- построение иерархии серверов;
- функции модуля контроля конфигураций и топологии сети «Efros NA»;
- функции модуля оптимизации и настройки МЭ «Efros FA»;
- функции модуля контроля целостности и проверки соответствия хостов и конечных точек «Efros ICC»;
- функции модуля анализа уязвимостей и построения векторов атак «Efros VC»;
- функции модуля сбора статистики по потокам данных в сети «Efros NFA»;
- функции модуля разграничения и контроля доступа в сети «Efros NAC»;
- функции модуля анализа и управления объектами защиты в разделе «Центр задач» «Efros CM»;
- функции модуля защиты DNS «Efros DNS».

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 (ОЗ, конечные точки, вектора атак):
   - просмотр ОЗ, клиентского оборудования (конечных точек сети);
   - инвентаризация параметров сети и управление несконфигурированными ОЗ (добавление/удаление ОЗ);
   - работа с базой знаний по ОЗ;
   - ведение списка конечных точек сети;
   - просмотр карты сети ОЗ;
   - построение векторов атак;
   - сканирование сети.
2) Контроль устройств:
   - настройка доступа к устройствам/группам устройств;

— проверка безопасности;
— проверка МЭ;
— настройка профилей отчетов;
— 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 активным сетевым оборудованием (АСО)/группами АСО;
— управление сетевыми пользователями/группами сетевых пользователей, имеющих доступ к АСО;
— настройка политик доступа;
— настройка условий доступа;
— настройка профилей оборудования;
— настройка профилей авторизации;
— загрузка ACL;
— редактирование набора команд;
— редактирование разрешенных протоколов аутентификации;
— управление разрешенными MAC-адресами;
— ведение словарей атрибутов;
— создание и управление гостевыми порталами.

4) Управление агентами «Efros Defence Operations» (агент ПК «Efros DO» или агент):
— учет установленных агентов на контролируемых конечных точках;
— настройка политик безопасности и контроля целостности;
— управление профилями настроек агентов;
— работа с инсталляционными пакетами для установки и обновления агентов и дополнительных модулей.

5) Защита DNS:
— управление черным и белым списками;

— настройка правил IDS/IPS;

— настройка защиты DNS-трафика;

— настройка серверов пересылки.

6) Управление заявками в разделе «Центр задач».

7) Управление отчетами для ОЗ.

8) Просмотр и экспорт событий.

9) Администрирование:

— управление пользователями/группами пользователей;

— управление лицензиями на подключаемые модули;

— ведение списка корневых, серверных и клиентских сертификатов, создание запросов на сертификаты;

— настройка планировщика задач и событий.

10) Управление настройками:

— настройка подключения к сервисам протоколов TACACS+ и RADIUS;

— настройка источника данных (LDAP, Active Directory, профили сертификатов);

— управление модулями встроенных и пользовательских типов устройств;

— настройка сервера обновлений для базы уязвимостей;

— управление хранением данных;

— настройка почтовых серверов;

— импорт данных;

— настройка DNS-сервера для базы знаний;

— настройка внешних систем (внешние серверы RADIUS, внешняя система аутентификации, SMS-провайдеры);

— построение иерархии серверов.

11) Мониторинг:

— визуализация процессов, обеспечивающих ИБ, с помощью встроенных и гибко настраиваемых схем в графическом виде с текстовым пояснением.

В ПК «Efros DO»:

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

2) Установлены внешние модули, отвечающие за активный аудит сетевого оборудования, серверных и клиентских операционных систем (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 syslog-сервера и отправки syslog-сообщений (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

— модуль взаимодействия со службами DNS по протоколу DNS.

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, контейнеров и прикладного программного обеспечения (ППО);
- контроль целостности файлов ОС, виртуализации, контейнеров и ППО;

— проверки соответствия безопасности ОС, виртуализации, контейнеров 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 набора 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+;
- гостевой портал;
- передача событий безопасности для дальнейшей обработки (SIEM-системы);
- интеграция с системой Cisco ACS\ISE (импорт пользователей АСО и списка сетевых устройств/конечных точек).

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 функциональную возможность ПК «Efros DO» по автоматизации управления жизненным циклом правил МЭ.

1.2.8 Модуль защиты DNS «Efros Secure DNS»

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

- блокировка доступа к нежелательным сайтам;
- обнаружение и предотвращение атак на DNS-трафик.

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 базе данных (БД) автоматически создается учетная запись пользователя с ролью встроенного системного администратора «GlobalAdministrator» и логином «SuperAdmin».

2 Работа со списком сущностей

Списки сущностей в комплексе: виджеты, объекты сети, отчеты, пользователи выполнены в виде дерева или таблицы. В качестве примера приведен подраздел «Объекты защиты» (рис. 1).

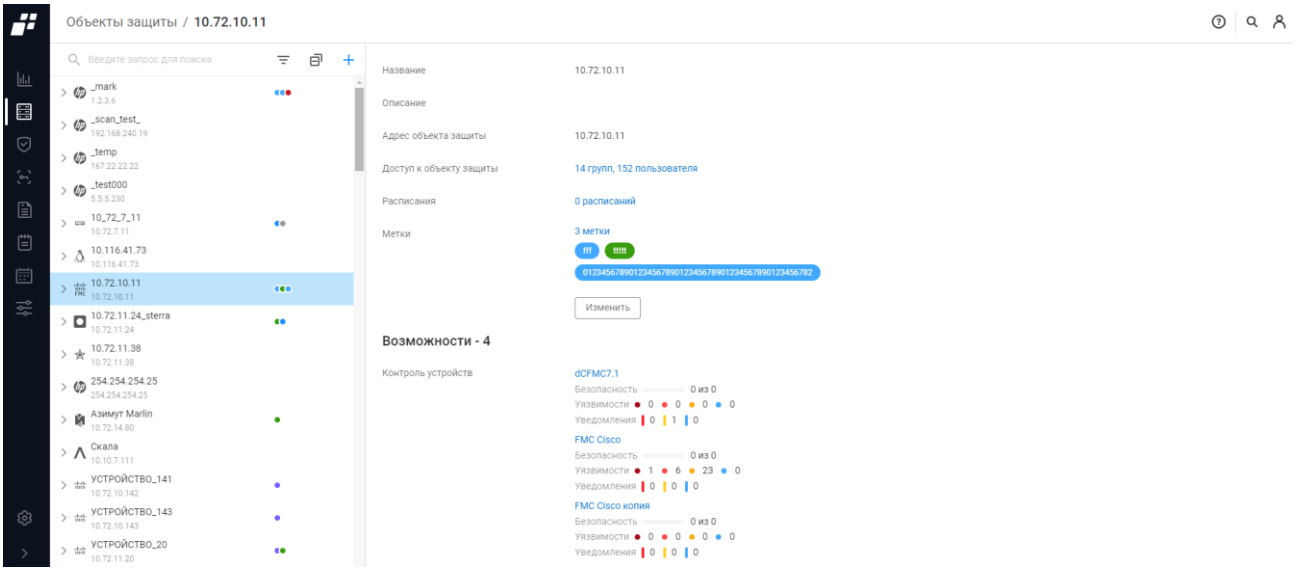


Рисунок 1 – Подраздел «Объекты защиты»

Над деревом (таблицей) в зависимости от типа сущности могут быть доступны:

- поле поиска (Введите запрос для поиска) для поиска записи в списке. Поиск выполняется по мере ввода символов;
- кнопка « + » для перехода на страницу создания сущности[1];
- кнопка « » для сворачивания или разворачивания дерева;
- кнопка «Фильтр» (Фильтр или) для фильтрации списка сущностей;
- кнопка «Колонки» ( ) для изменения отображения колонок на странице;
- индивидуальные для дерева/списка кнопки (подробнее описание кнопок приведено в разделах документа ниже).

2.1 Выбор сортировки записей таблиц

По умолчанию список сущностей отсортирован в порядке убывания даты и времени внесения последних изменений в данные сущности – в алфавитном порядке.

Пользователь имеет возможность задать другой тип сортировки, выбрав заголовок

[1] Название кнопки зависит от типа создаваемой сущности

требуемого столбца таблицы. В заголовке отобразится знак « », сортировка всех строк таблицы выполнена по убыванию значений выбранного столбца. Для изменения направления сортировки необходимо повторно выбрать заголовок столбца. В заголовке отобразится знак « ».

2.2 Поиск данных в таблицах (дереве) сущностей

Для поиска в списке сущностей требуемых записей необходимо ввести в поле поиска последовательность символов из искомой записи. Поиск выполняется по мере ввода символов, в списке отобразятся записи сущностей, в данных которых содержатся введенные символы.

Для отмены заданного правила поиска и отображения в таблице всех записей необходимо нажать кнопку «Очистить» (✕).

2.3 Фильтрация

В разделах ПК «Efros DO» реализована возможность фильтрации событий, отчетов, заявок и других списков. Фильтровать данные можно по выбранным параметрам или по периоду создания элементов.

2.3.1 Фильтрация по выбранным параметрам

Для фильтрации с выбором требуемых параметров необходимо выполнить следующие действия:

1) Нажать кнопку « Фильтр » или « ». Откроется окно фильтрации. Состав полей окна для разных подразделов раздела «Контроль устройств» отличается. На рис. 2 приведен пример окна фильтрации в дереве типов устройств, подраздел «Проверки безопасности».
2) Задать требуемые параметры фильтрации. Для раскрывающихся списков доступен множественный выбор значений параметра.
3) Нажать кнопку «Применить». Окно фильтрации закроется, на странице отобразятся данные, соответствующие заданным параметрам фильтрации.

Для внесения изменений в заданные правила фильтрации необходимо повторно открыть окно фильтрации, задать новые правила и нажать кнопку «Применить». Для очищения поля параметра – нажать в поле кнопку « ».

Для отмены заданных правил фильтрации и отображения на странице всех данных необходимо повторно открыть окно фильтрации и нажать кнопку «Сбросить».

2.3.2 Фильтрация по периоду

Для фильтрации данных в дереве (таблицах) по периоду необходимо:

— нажать кнопку «Выбор периода» (Выбор периода). Откроется окно выбора

параметров начала и окончания периода;

— выбрать требуемые даты и время (час, минуту) начала и окончания периода;
— нажать кнопку «Применить».

Окно выбора периода свернется, на странице над таблицей отобразится период, соответствующий заданным параметрам фильтрации.

Для отмены заданных правил фильтрации и отображения всех данных в дереве (таблицах) необходимо установить курсор в поле выбора периода и нажать в открывшемся окне выбора периода кнопку «Сбросить».

2.4 Настройка отображаемых колонок в таблицах списков сущностей

Для настройки состава отображаемых колонок в списках сущностей необходимо нажать кнопку «Колонки» (). Откроется окно выбора колонок таблицы. На рис. 2 приведен пример окна для списка конечных точек, подраздел «Конечные точки».

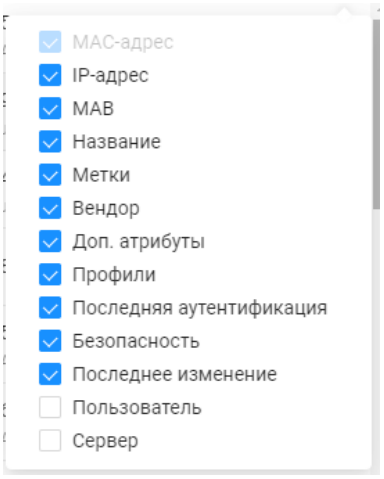


Рисунок 2 – Окно выбора колонок для списка конечных точек

В окне отображаются строки с наименованиями всех колонок таблицы. Им соответствуют поля для флага. Наличие в поле флага означает, что столбец выбран для отображения в таблице. Колонка, строка которого неактивна, не доступен для изменения его видимости в таблице.

Для настройки состава отображаемых в списке колонок необходимо установить/отменить флаг. Состав колонок изменяется по мере установки/отмены флагов.

Кроме того, в окне выбора колонок пользователь может настроить последовательность расположения колонок в таблице. При наведении курсора на строку с названием колонки слева от поля для флага отображается символ «». Перетаскиванием символа выбирается требуемое положение в списке колонок.

2.5 Копирование/изменение параметров сущностей

Копирование сущности в списке может быть выполнено одним из следующих способов:

1) Способ 1:
   - навести курсор на строку с сущностью;
   - нажать кнопку «•••»;
   - выбрать пункт «Создать копию»;
   - в открывшемся окне отредактировать необходимые параметры и нажать кнопку «Создать».
2) Способ 2:
   - навести курсор на строку с сущностью;
   - в правой части строки появится кнопка «  »;
   - в открывшемся окне внести требуемые параметры и нажать кнопку «Создать».

Изменение параметров сущности может быть выполнено одним из следующих способов:

1) Способ 1:
   - навести курсор на строку с сущностью;
   - нажать кнопку «•••»;
   - выбрать пункт «Изменить»;
   - в открывшемся окне отредактировать необходимые параметры и нажать кнопку «Сохранить».
2) Способ 2:
   - навести курсор в таблице на название сущности;
   - нажать на сущность. Откроется страница с параметрами сущности;
   - внести требуемые изменения;
   - нажать кнопку «Сохранить».

После копирования или внесения изменений после нажатия кнопки «Создать» или «Сохранить» автоматически запускается процесс проверки заполненности всех обязательных полей и уникальности копируемой/изменяемой сущности.

При обнаружении недопустимых значений под полем появится подсказка красного цвета с информацией для корректного заполнения поля и кнопка «Создать»/«Сохранить» будет недоступна. При дублировании информации в верхней части страницы появится сообщение, что поле должно содержать уникальную информацию. Пользователю необходимо корректно заполнить поля страницы, кнопка «Создать»/«Сохранить» станет доступной.

2.6 Удаление сущностей

Удаление сущностей выполняется вручную. Для удаления доступны только те записи списков ПК «Efros DO», которые не использованы в карточках других. При попытке удаления таких сущностей, удаление выполнено не будет, отобразится

соответствующее сообщение.

Удаление одной сущности из списка может быть выполнено одним из следующих способов:

1) Способ 1:
   - навести курсор на строку с сущностью;
   - нажать кнопку «»;
   - выбрать пункт «Удалить»;
   - в открывшемся окне подтверждения нажать кнопку «Удалить».
2) Способ 2:
   - навести курсор на строку с сущностью;
   - в правой части строки появится кнопка «  »;
   - нажать кнопку и далее в открывшемся окне подтверждения нажать кнопку «Удалить».

В результате будет запущен процесс удаления сущности.

В случае возникновения ошибки в процессе удаления сущность из списка не будет удалена.

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. 3).
4) Ввести в поле «Логин» имя учетной записи пользователя в одном из форматов: логин; домен\логин; логин@домен (в формате UPN).
5) Ввести в поле «Пароль» пароль пользователя.
6) Нажать кнопку «Подключиться».
7) При наличии двухфакторной аутентификации ввести проверочный код.

В случае некорректного ввода данных появится сообщение об ошибке под кнопкой «Подключиться». Полный перечень возможных ошибок приведен в разделе 12.

Рисунок 3 – 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 раздела «Мониторинг» (рис. 4). 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. 5).

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

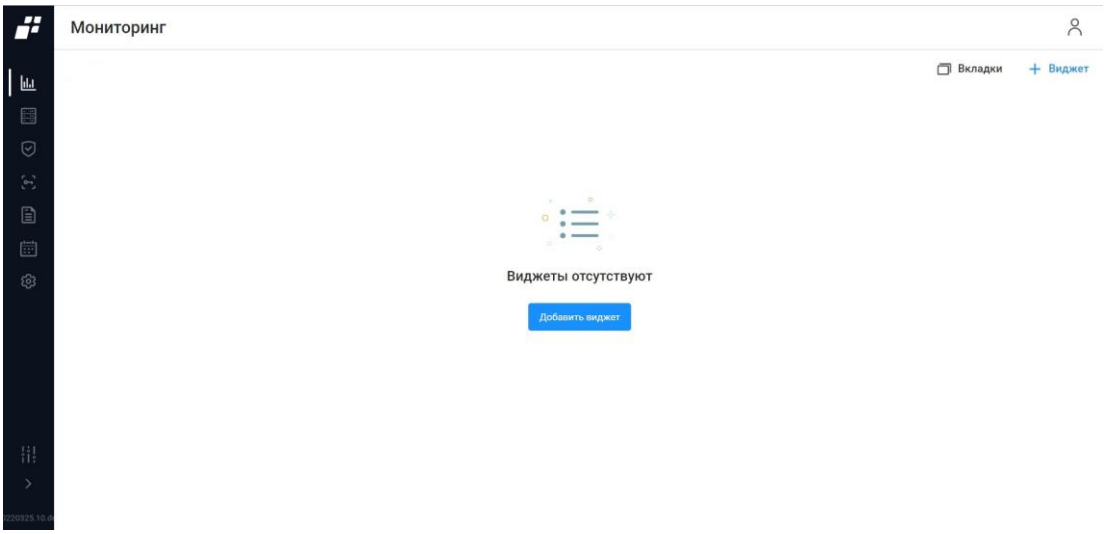


Рисунок 4 – Раздел «Мониторинг»

Рисунок 5 – 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 «Справка» (), по нажатию которой на отдельной странице браузера открывается справочная система ПК «Efros DO»;
— кнопка «Поиск» (), по нажатию которой открывается поле поиска для быстрого перехода в требуемый раздел/подраздел ПК «Efros DO». По мере ввода в поле символов отображается список разделов и подразделов ПК «Efros DO», название которых содержит введенные символы. Пользователю необходимо выбрать в списке строку требуемого раздела/подраздела;
— кнопку «Аккаунт» (), по нажатию которой открывается меню (рис. 6), содержащее:
а) логин и роль текущего пользователя (доступен только для просмотра);
б) блок с настройками оформления страниц приложения – 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;

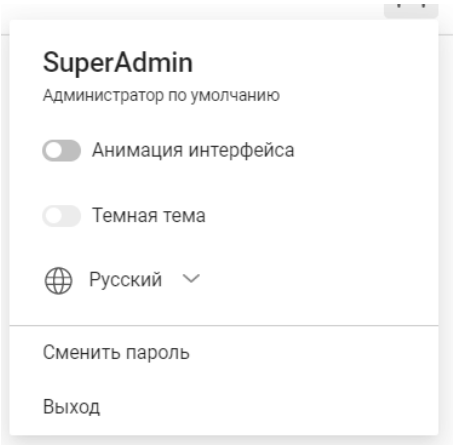


Рисунок 6 – Меню «Аккаунт»

в) поле выбора языка приложения (русский/английский). По умолчанию задан русский язык;
г) кнопка «Сменить пароль» для перехода в окно смены пароля;
д) кнопка «Выход», по нажатию которой выполняется выход из веб-

приложения и открывается страница авторизации пользователя (см. рис. 3);

2) Панель главного меню, содержащая:

— наименование активного в текущий момент времени сервера (отображается только при наличии настроенной иерархии серверов комплекса и при наличии у текущего пользователя прав доступа к данным нескольких серверов иерархии;

— доступные пользователю разделы для работы с комплексом;

— строку управления отображением панели главного меню. В развернутом состоянии панели строка имеет вид в соответствии с рис. 7, в свернутом отображаются пиктограммы, обозначающие разделы. Выбор пиктограммы позволяет перейти на страницу соответствующего раздела и раскрыть меню без разворачивания панели главного меню.

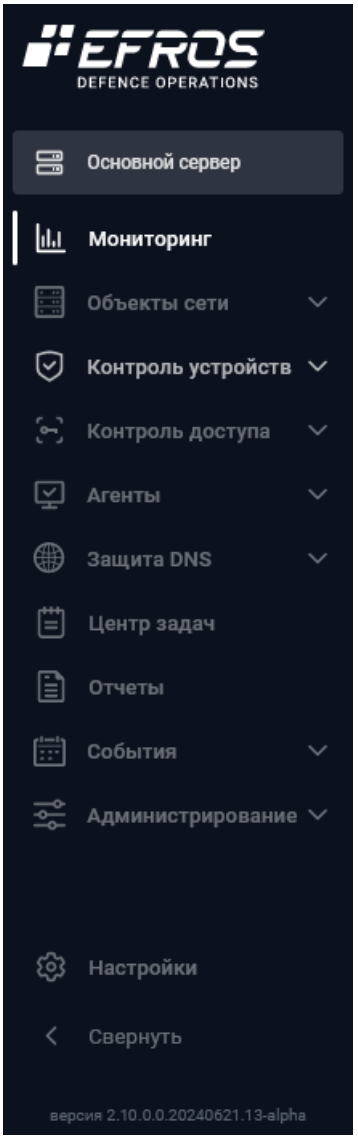


Рисунок 7 – Меню в развернутом виде

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

При наличии в комплексе настроенной иерархии (подробнее см. подраздел 11.10) и, если пользователю назначены права доступа к различным серверам иерархии, то в рабочей области страницы будут отображаться данные сервера, выбранного пользователем в текущий момент времени в качестве активного. По умолчанию выбран основной сервер. Для смены активного сервера пользователю необходимо установить курсор в строке меню с наименованием активного сервера и выбрать в открывшемся окне (рис. 8) требуемый сервер. Окно содержит значение «Основной сервер» и строки с наименованиями подчиненных серверов, доступных пользователю.

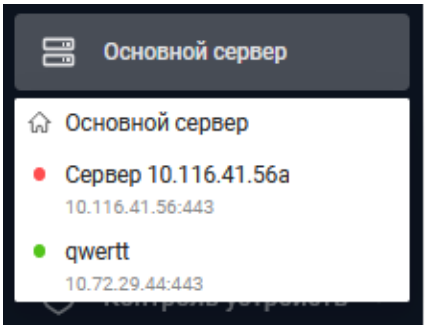


Рисунок 8 – Окно выбора активного сервера

При успешном завершении переключения на выбранный сервер отобразится соответствующее сообщение, при возникновении ошибки отобразится сообщение об ошибке с текстом ошибки. В журнале событий комплекса будет зафиксирован факт успешного или неуспешного переключения пользователя на другой сервер (основной или подчиненный).

Работа с комплексом выполняется пользователями с использованием веб-интерфейса разделов комплекса, описание которых приведено в разделах 4 – 11 руководства.

4 Раздел «Мониторинг»

Раздел «Мониторинг» представляет собой вкладки, состоящие из интерактивных отчетов (виджетов) в реальном времени по всем параметрам комплекса (рис. 9).

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» зависят от наличия хотя бы одной лицензии на функциональные модули.

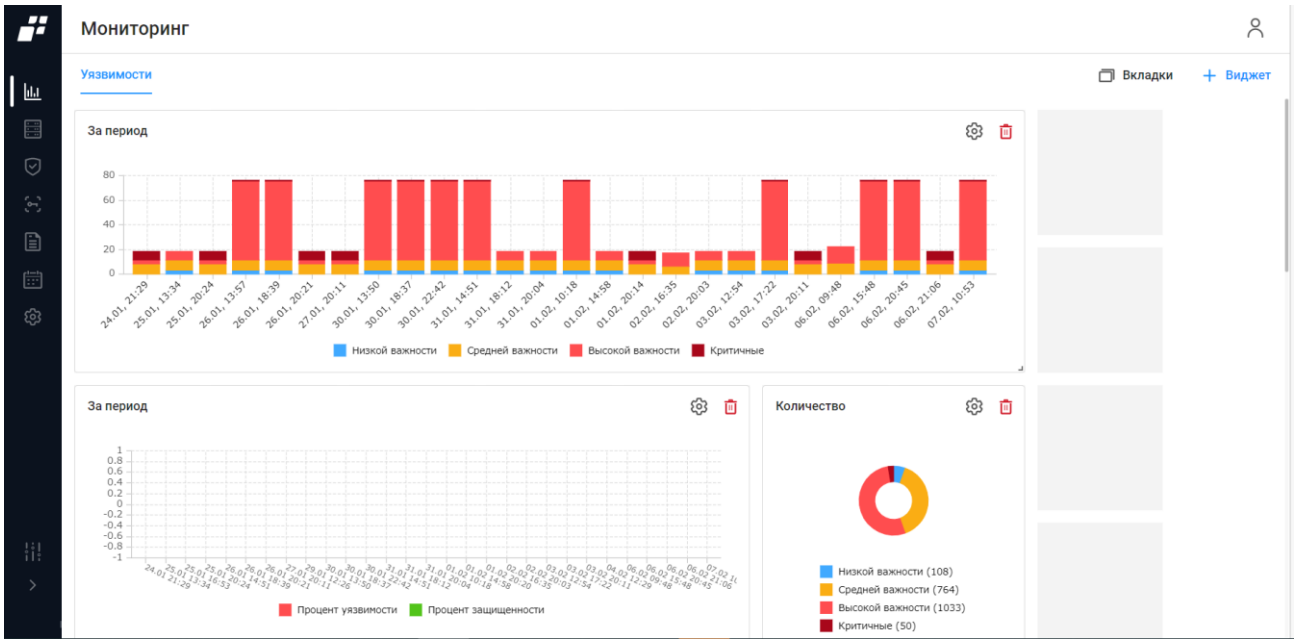


Рисунок 9 – Раздел «Мониторинг»

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);
- кнопка «Виджет» (Виджет).

4.1 Добавление новой вкладки и виджета

Для добавления вкладки необходимо выполнить следующие действия:

1) Нажать кнопку «Вкладки» (Вкладки).
2) Откроется окно «Вкладки» (рис. 10). Необходимо указать название вкладки и нажать кнопку «Сохранить».

При необходимости добавления нескольких вкладок – нажать кнопку « + », при необходимости удалить вкладку – нажать кнопку « 🗑 ». Слева в строке вкладки отображается символ «⠿». Перетаскиванием символа выбирается требуемое положение вкладки на странице раздела «Мониторинг».

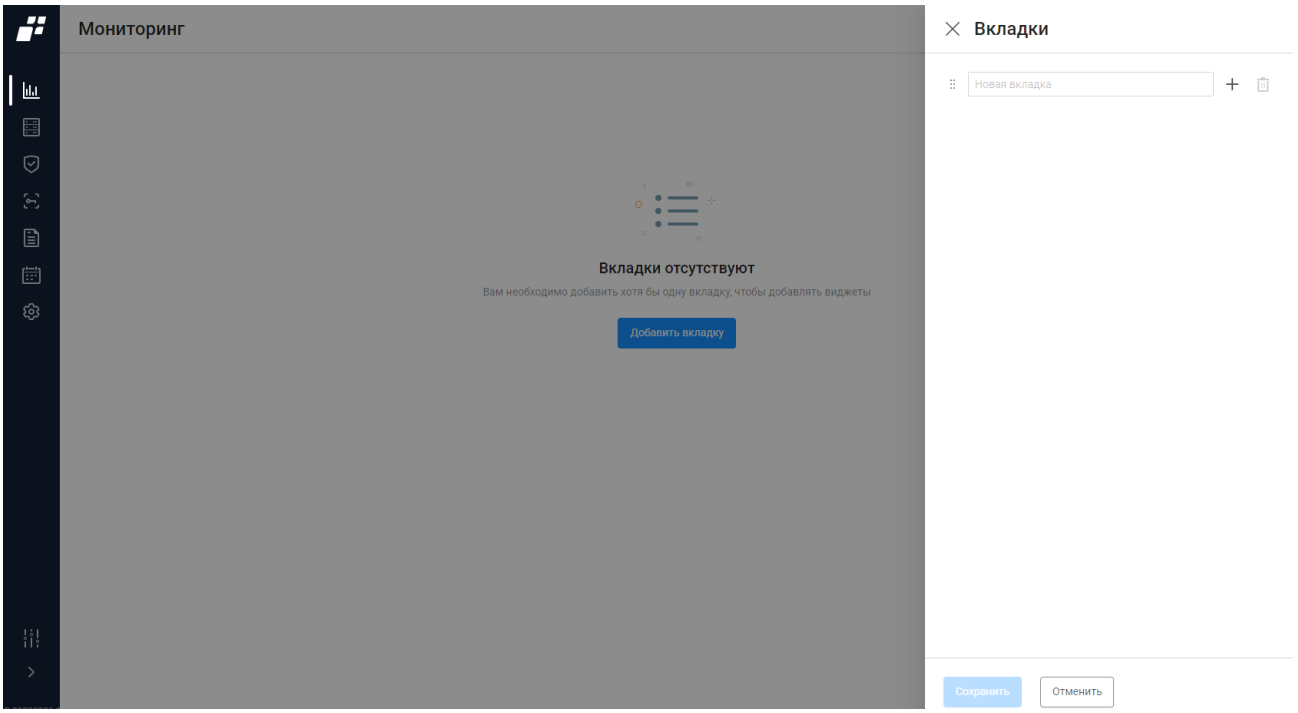


Рисунок 10 – Окно «Вкладки»

Для добавления нового виджета необходимо:

1) В созданной вкладке нажать кнопку «Виджет» (+ Виджет).
2) Откроется окно «Библиотека виджетов» (рис. 11). Состав и описание виджетов приведены в таблице 3.

Возможность добавления виджета и информация, отображаемая на нем, зависит от типа установленной лицензии. Доступность информации на виджетах в зависимости от типа лицензии приведена в таблице 4.

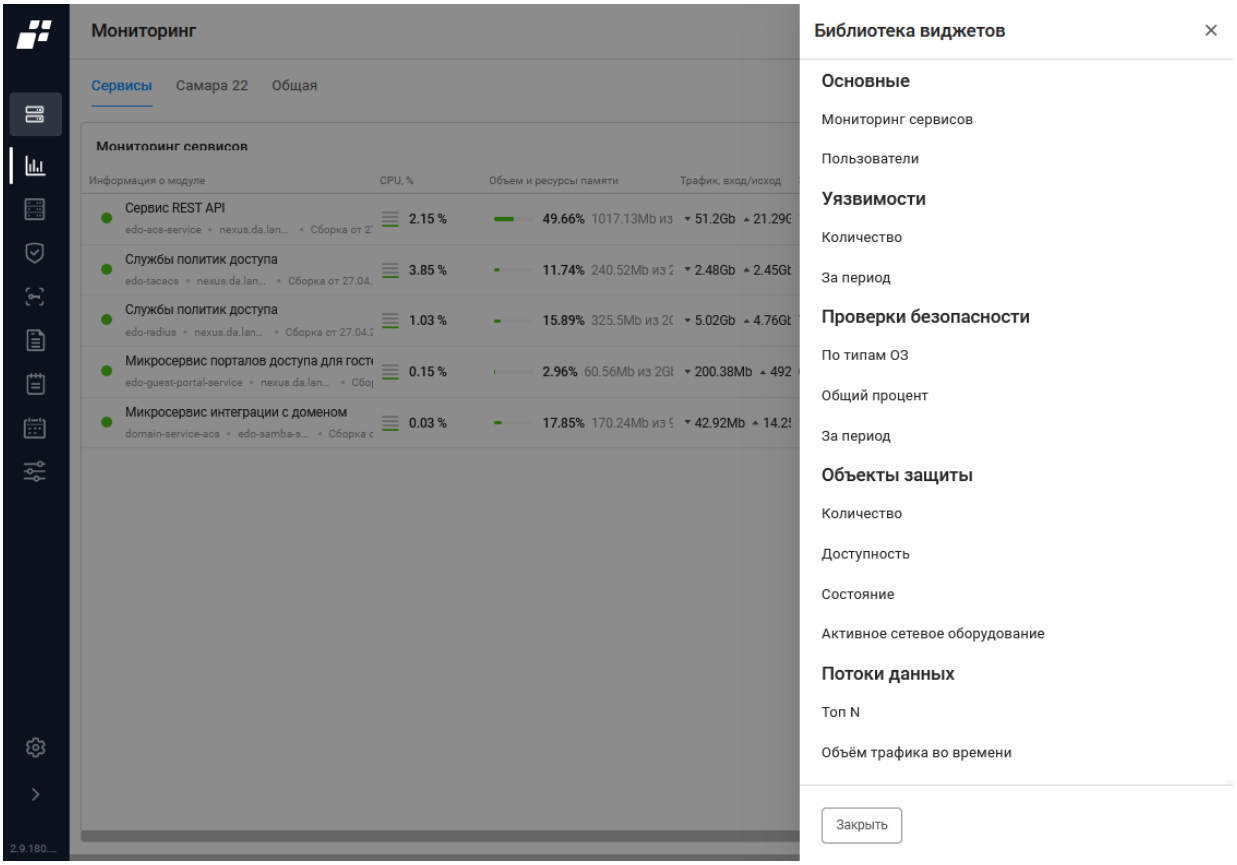


Рисунок 11 – Окно «Библиотека виджетов»

Таблица 3 – Состав и описание виджетов раздела «Мониторинг»

Виджет	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 (типов устройств) с выявленными уязвимостями за период – приводятся сведения о количестве ОЗ для каждой степени критичности уязвимостей за определенный шаг

Виджет	Описание
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; — 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

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

Виджет	Описание
	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 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)

Таблица 4 – Доступность информации на виджетах в зависимости от типа лицензии

Лицензия / Виджет	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		+	+	+	+		

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

3) Выбрать строку требуемого виджета. Откроется окно добавления виджета (рис. 13). Состав параметров зависит от типа виджета.

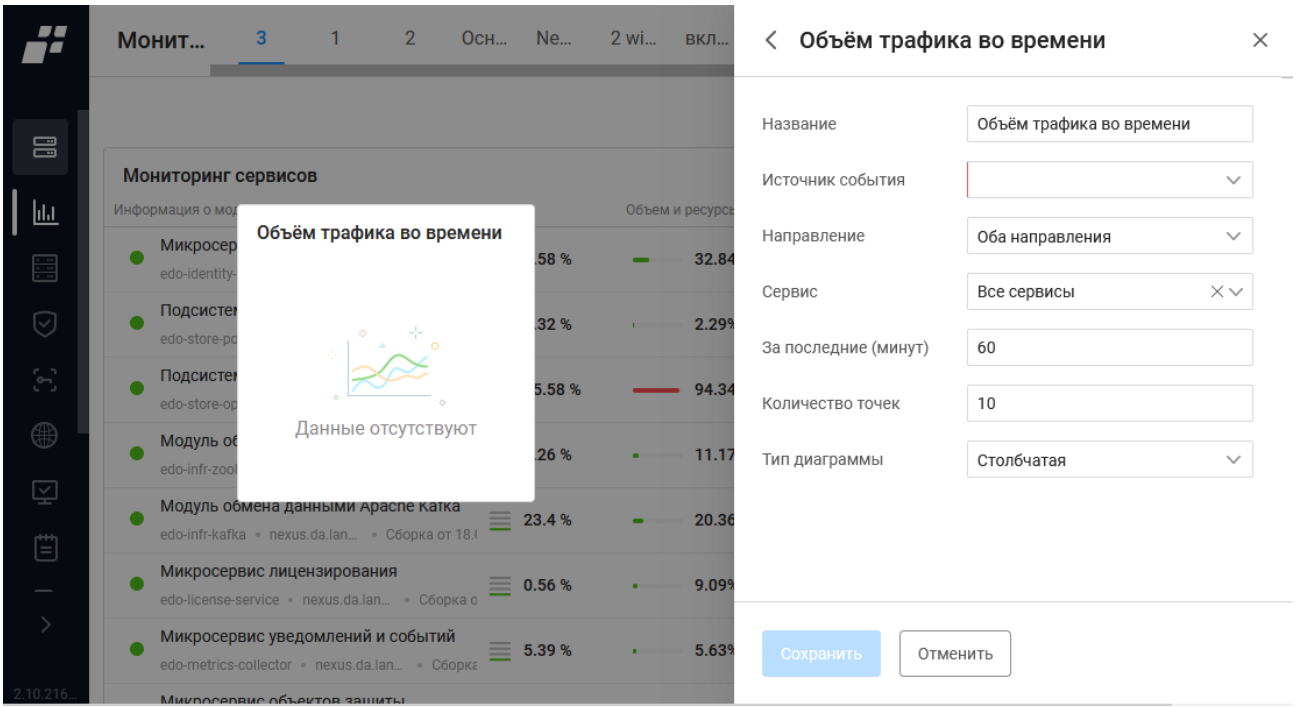


Рисунок 12 – Окно добавления виджета

4) Указать требуемые параметры виджета и нажать кнопку «Сохранить». На странице раздела «Мониторинг» в выбранной в перечислении 1 вкладке добавится виджет с указанным названием.

При наведении курсора на поле виджета в виджете отображаются кнопки (рис. 13):

— «Настройка» (⚙) – для перехода в окно настройки параметров виджета (аналогично окну создания виджета). Окно содержит дополнительно кнопку удаления виджета;

— «Переместить» (⠿) – для перемещения виджета в требуемое положение на странице вкладки.

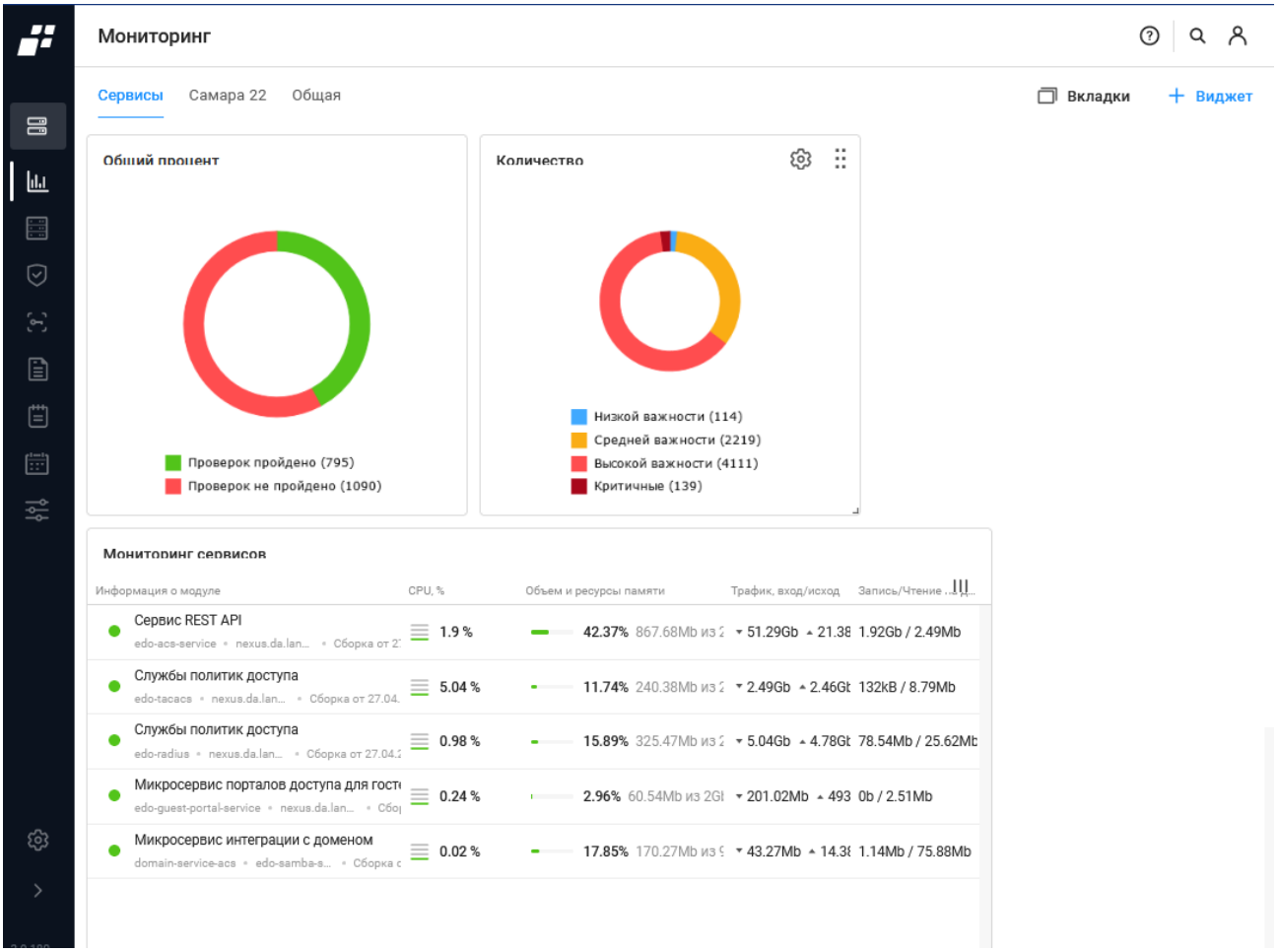


Рисунок 13 – Раздел «Мониторинг» с выбранными виджетами

4.2 Удаление вкладки и виджета

Для удаления вкладок необходимо выполнить следующие действия:

1) Нажать кнопку «Вкладки» (Вкладки). Откроется окно «Вкладки» (см. рис. 10).
2) В строке удаляемых вкладок нажать кнопу «Удалить» ( ). В строках вкладок отобразится кнопка «Восстановить» (Восстановить).
3) Отменить удаление ошибочно удаленных вкладок, нажав соответствующие им кнопки «Восстановить» (Восстановить).
4) Нажать кнопку «Сохранить». Состав вкладок раздела «Мониторинг» будет изменен.

Для удаления виджета с вкладки необходимо выполнить следующие действия:

1) Перейти в разделе «Мониторинг» на требуемую вкладку.

2) Навести курсор на требуемый виджет и нажать в нем кнопку «Настройка» ( ).

3) Нажать в открывшемся окне настройки параметров виджета (рис. 14) кнопку «Удалить».

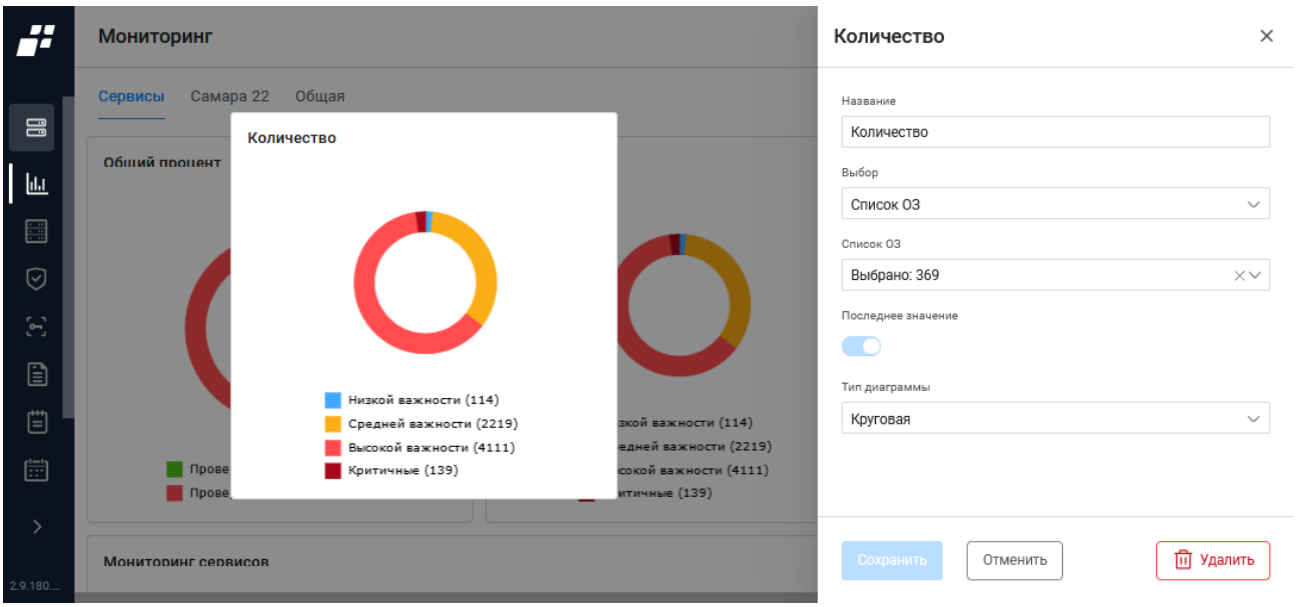


Рисунок 14 – Окно настройки параметров виджета

5 Раздел «Объекты сети»

Раздел «Объекты сети» содержит агрегированную информацию, характеризующую объект сети в части конфигурирования, авторизации и аутентификации.

Раздел состоит из следующих подразделов:

- «Объекты защиты»;
- «База знаний»;
- «Конечные точки»;
- «Карта сети»;
- «Векторы атак»;
- «Сканирование сети».

5.1 Объекты защиты

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

Подраздел «Объекты защиты» 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. 15), позволяет выполнять следующие действия с ОЗ:

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

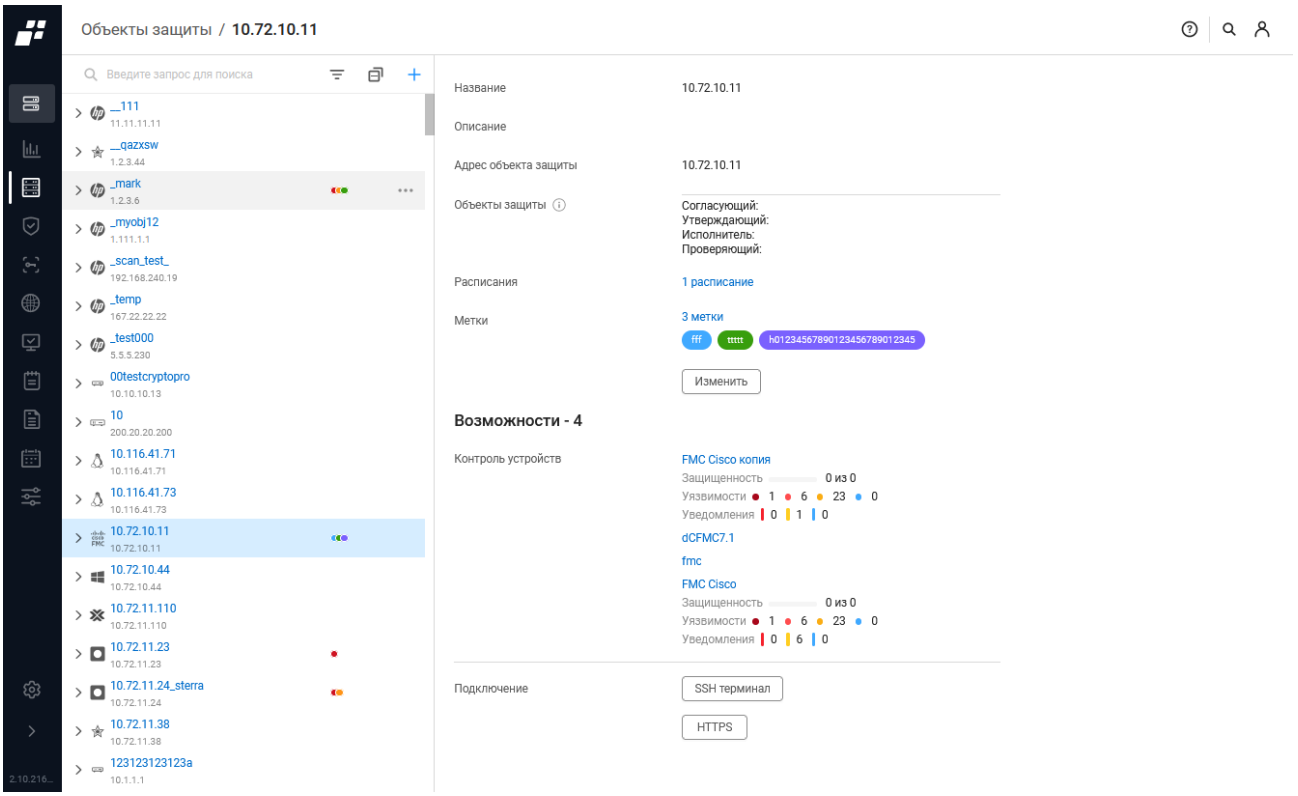


Рисунок 15 – Подраздел «Объекты защиты»

Страница содержит следующие элементы:

- дерево ОЗ – иерархический список сконфигурированных ОЗ, контролируемых 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»;
- поле «Подключение» с кнопками для подключения к ОЗ (для поддерживаемых ОЗ типов подключения, например, «SSH терминал», «HTTPS»).

5.1.1 Дерево объектов защиты

Над деревом ОЗ располагаются:

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

В строке первого уровня дерева отображаются:

- иконка производителя, название и адрес ОЗ;
- цветные кружки-метки[4], при наведении на них курсора всплывают подсказки с текстом меток;
- кнопка «Контекстное меню» ( ). По нажатию кнопки открывается контекстное меню, которое позволяет выполнить с ОЗ следующие действия:
  - «Изменить» – внести изменения в параметры ОЗ (см. п. 5.1.1.6);
  - «Добавить возможность «Контроль устройств» (см. п. 5.1.1.4);
  - «Добавить возможность «Контроль доступа» (см. п. 5.1.1.3);
  - «Добавить возможность «Потоки данных» (см. п. 5.1.1.5);
  - «Добавить вложенный объект защиты» (см. п. 5.1.1.2);
  - «Удалить».

Состав активных пунктов меню «Добавить возможность <название возможности>» зависит от типа ОЗ.

При нажатии в строке ОЗ кнопки « » раскрывается список второго уровня – зависимости от назначенных ОЗ возможностей. Могут отображаться строки с иконками:

- « » – обозначает возможность «Контроль устройств»;
- « » – обозначает возможность «Контроль доступа»;
- « » – обозначает возможность «Потоки данных».

Цвет подсветки строки с ОЗ (рис. 16) обозначает следующее:

- зеленый – выполнение операции;
- желтый – обнаружено событие контроля (например, не пройдена проверка устройства);
- красный:
  - при выполнении операции на устройстве возникла ошибка;

[4] Метки – это ключевые слова, которые используются для выделения объектов сети из общего списка, упрощения поиска объектов, объединения объектов в логические категории

- 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.

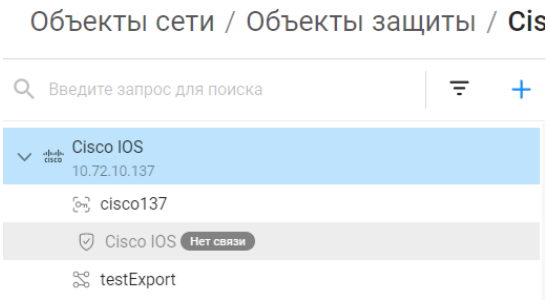


Рисунок 16 – Пример подсветки строки с ОЗ

Контекстное меню устройства на втором и последующих уровнях в зависимости от назначенной возможности позволяет выполнить следующие действия с устройством:

1) С возможностью «Контроль устройств»:
— изменить;
— загрузить конфигурации;
— принять все изменения;
— конфигурировать (если тип устройства поддерживает такую операцию);
— включить сервисный режим;
— удалить.

2) С возможностью «Контроль доступа»:
— изменить;
— удалить.

3) С возможностью «Потоки данных»:
— изменить;
— создать копию;
— удалить.

При выборе устройства с назначенной возможностью:

1) «Контроль устройств» – отображаются следующие вкладки[5]:
— «Статус»;
— «Отчеты»;
— «События»;
— «Архив».
2) «Контроль доступа» – отображается описание ОЗ.
3) «Потоки данных» – отображаются следующие вкладки:
— «Настройки»;
— «Срабатывания».

Добавление ОЗ может быть выполнено следующими способами:

— в разделе «Объекты защиты» через дерево ОЗ;
— в разделе «Контроль устройств» (более подробно см. документ «Руководство 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. 17). Заполнить поля в окне необходимыми параметрами и нажать кнопку «Создать». Состав и описание полей окна приведены в таблице 5.

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 в его строке кнопку «Контекстное меню» (•••). Выбрать «Добавить вложенный ОЗ».
3) Откроется окно «Создание объекта защиты» (см. рис. 17). Заполнить поля окна необходимыми параметрами и нажать кнопку «Создать». Состав и описание полей окна приведены в таблице 5.

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

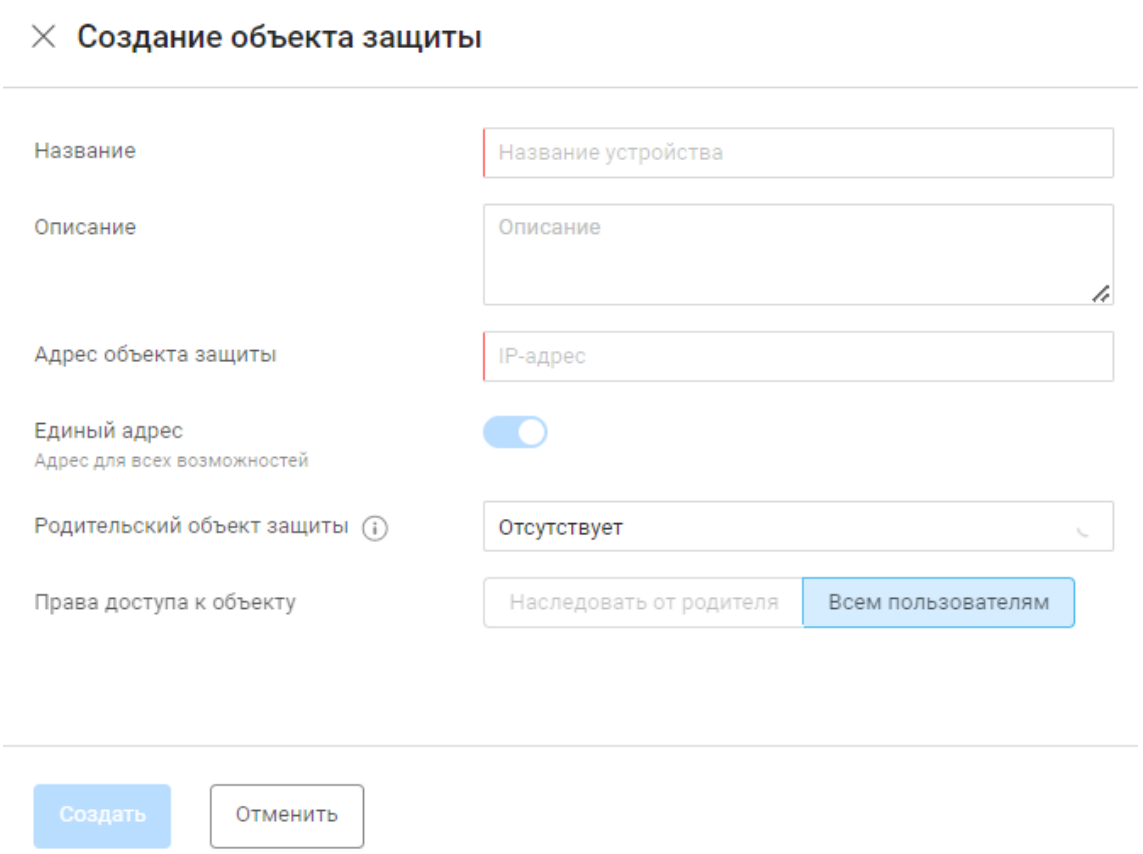


Рисунок 17 – Окно «Создание объекта защиты»

Таблица 5 – Состав и описание полей окна добавления ОЗ

Поле	Описание
Поле «Название»	Текстовое поле для ввода названия ОЗ. Параметры ввода текста: от 1 до 50 любых символов
Поле «Описание»	Текстовое поле для ввода описания ОЗ. 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 переключатель в положении «Включен»
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	Поле позволяет редактировать уровень доступа к ОЗ

Поле	Описание
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 во вкладке «Настройки» (см. п. 5.1.1.6)	

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) Нажать в его строке кнопку «Контекстное меню» (•••). Выбрать возможность «Контроль доступа».
3) Откроется страница «Создание возможности “Контроль доступа”» (рис. 18). Состав и описание полей вкладки «Свойства» приведены в таблице 6.
4) Заполнить поля страницы необходимыми параметрами. Страница состоит из следующих вкладок:

— «Свойства» – вкладка активна по умолчанию;

— «Группы».

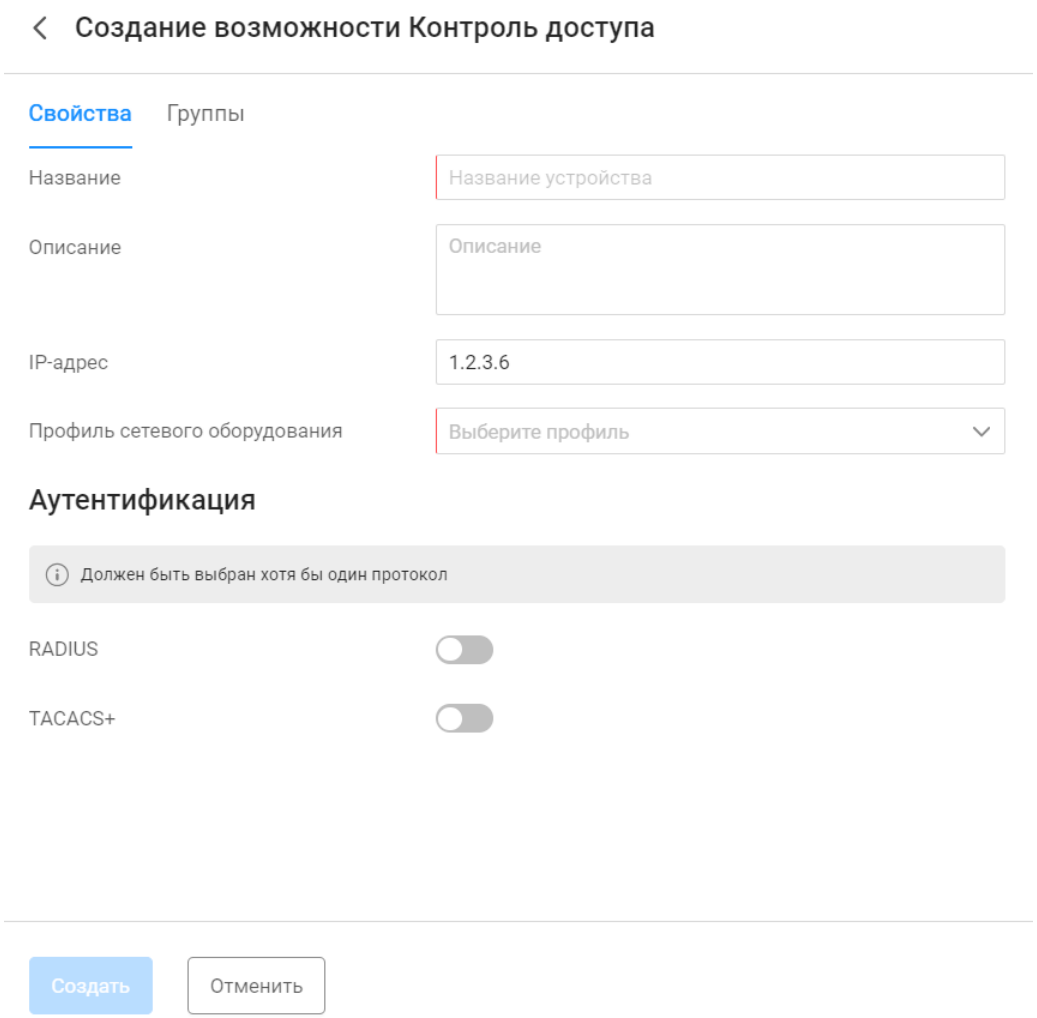


Рисунок 18 – Страница «Создание возможности “Контроль доступа”»

Таблица 6 – 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»)
Группа переключателей «Аутентификация»	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

Поле	Описание
	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

5) Перейти на вкладку «Группы» (рис. 19). Состав и описание полей вкладки «Группы» приведены в таблице 7. Добавить ОЗ при необходимости установкой флагов в требуемых строках в одну или несколько групп.

6) Нажать кнопку «Создать».

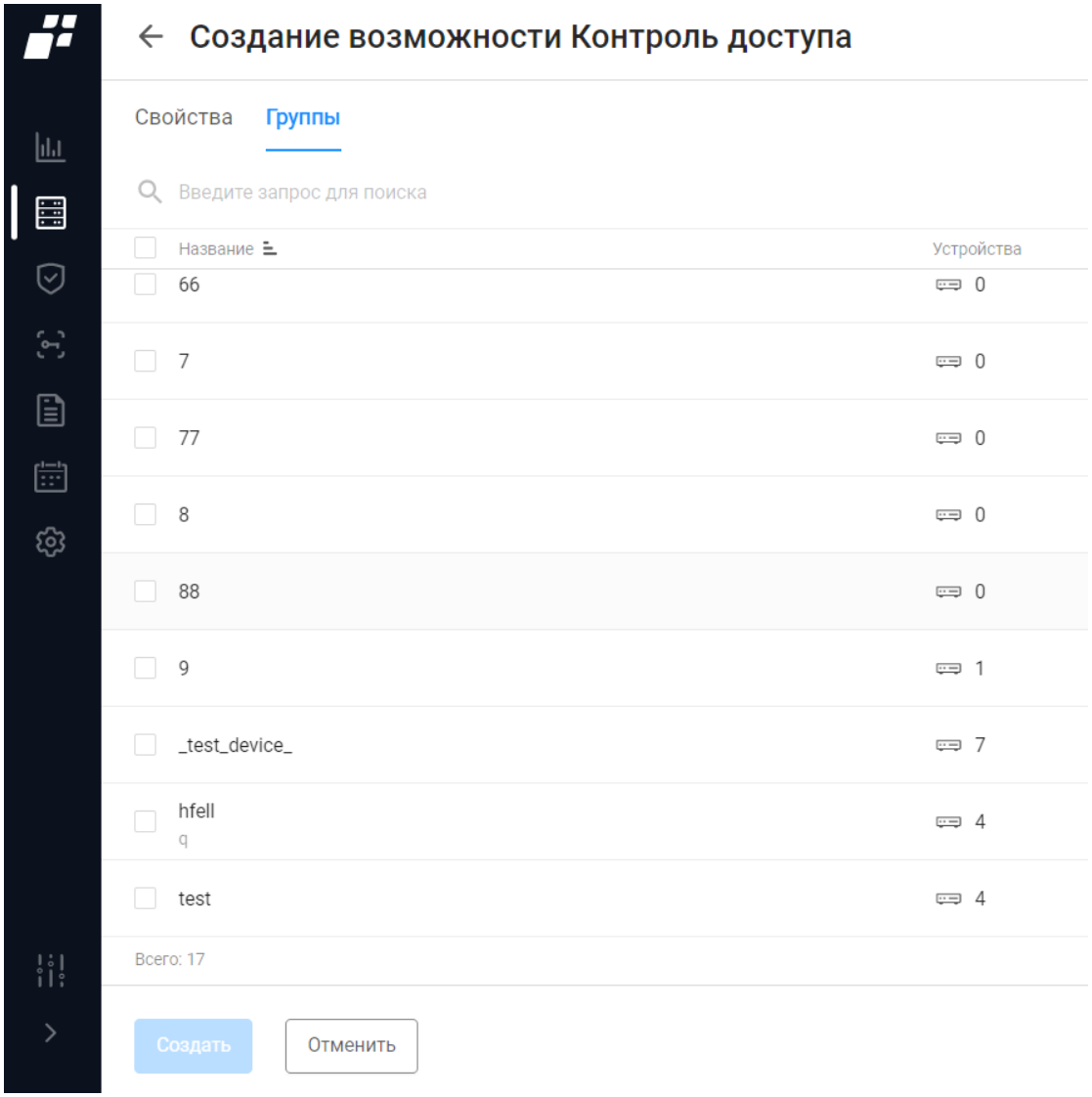


Рисунок 19 – Вкладка «Группы»

Таблица 7 – 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

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) Нажать в его строке кнопку «Контекстное меню» (•••). Выбрать возможность «Контроль устройств».
3) Откроется страница «Создание возможности “Контроль устройств”» (рис. 20). Состав и описание полей вкладки «Свойства» приведены в таблице 8.
4) Заполнить поля соответствующими параметрами. Страница состоит из следующих вкладок:

— «Свойства» – вкладка активна по умолчанию;

— «Расписания».

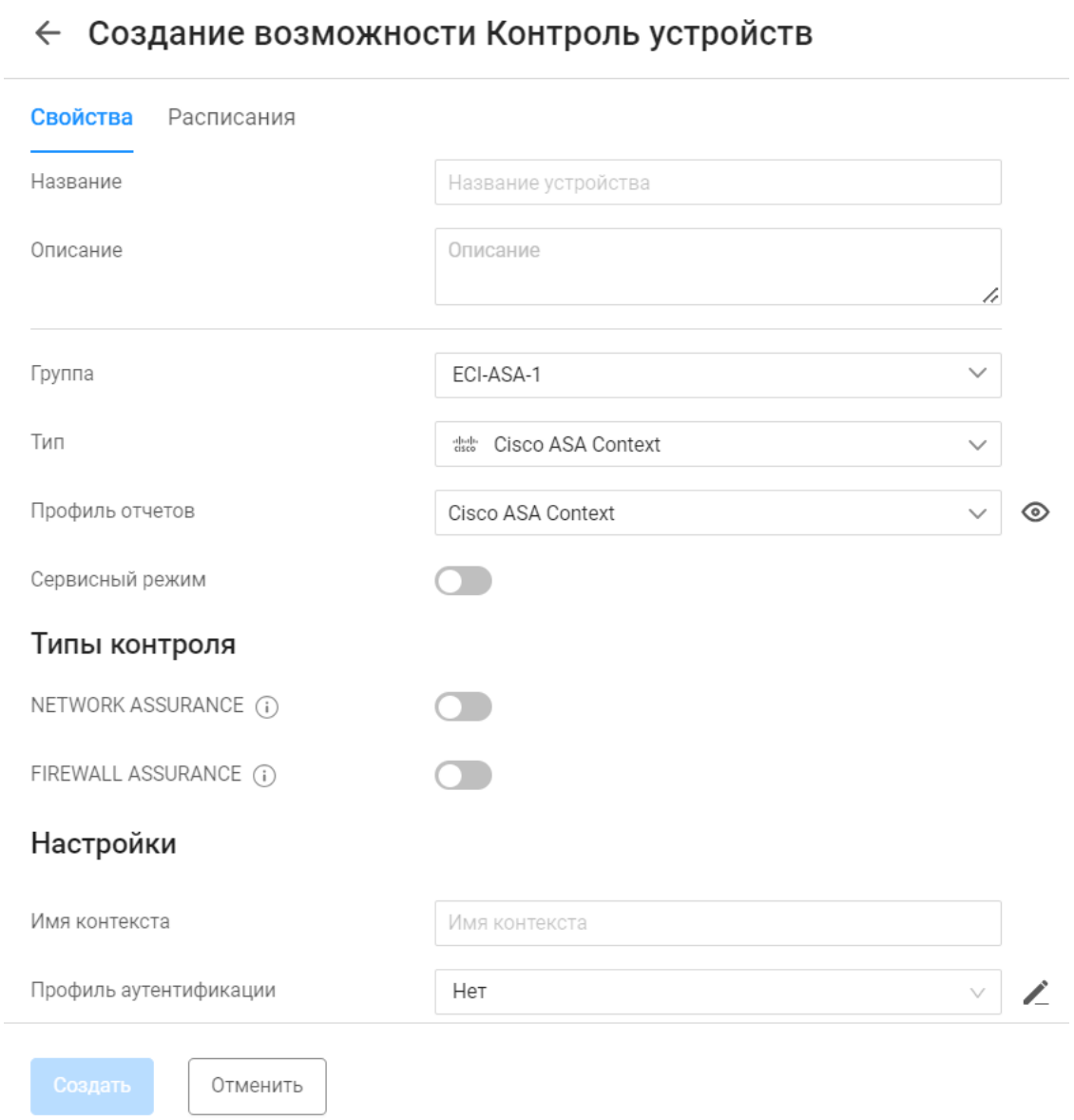


Рисунок 20 – Страница «Создание возможности “Контроль устройств”»

Таблица 8 – Состав и описание полей вкладки «Свойства» для возможности «Контроль устройств»

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
Поле «Группа»	Раскрывающийся список доступных для выбора групп ОЗ
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	Раскрывающийся список профилей отчетов параметров контроля

Поле	Описание
отчетов»	устройств. Поле становится доступно после выбора типа устройства. По нажатию кнопки «Просмотреть» (👁) раскрывается список отчетов, входящих в профиль, с заданным для них в профиле типом использования. Отчеты сгруппированы по категориям «Конфигурации» и «Проверки» (более подробно см. документ «Руководство пользователя. Часть 2. Контроль устройств»)
Поле «Сервисный режим»	Переключатель: — «Активен» () – сервисный режим активен. Устройство не опрашивается по заданному расписанию. В автоматическом режиме доступность устройства не проверяется. Обновление данных выполняется только по запросу пользователя; — «Неактивен» ()
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 поля	Состав полей с дополнительными параметрами подключения зависит от типа устройства, выбранного 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

5) Перейти на вкладку «Расписания» (рис. 21). На вкладке «Расписания» отображаются только те расписания, у которых выбран статус использования «Вкл.» (более подробно описано в подразделе 10.4). Состав и описание полей вкладки «Расписания» приведены в таблице 9.

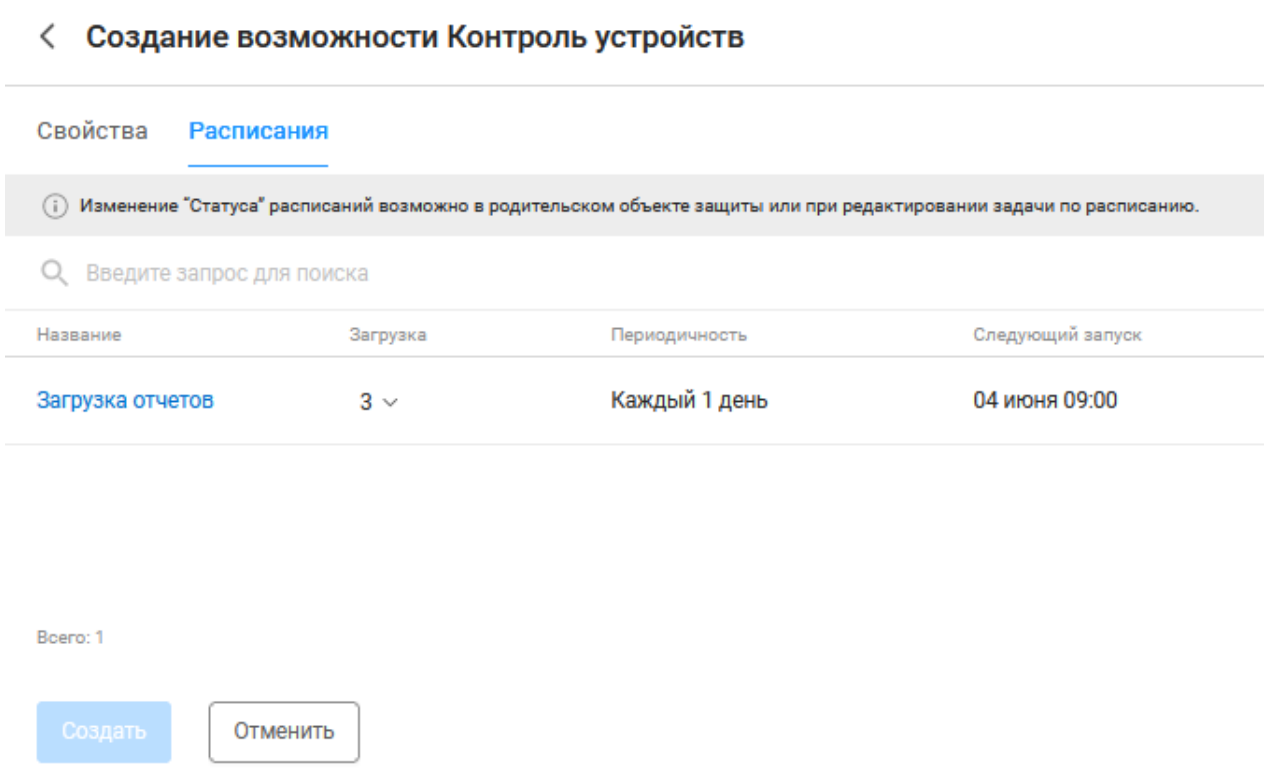


Рисунок 21 – Вкладка «Расписания»

Таблица 9 – Состав и описание полей вкладки «Расписания»

Поле	Описание
Поле «Название»	Название и описание расписания
Поле «Загрузка»	Раскрывающийся список включенных в расписании для загрузки категорий отчетов. Возможны следующие категории: — «Конфигурации»; — «Проверки безопасности»; — «Уязвимости»
Поле «Периодичность»	Период срабатывания расписания
Поле «Следующий запуск»	Дата и время следующего срабатывания расписания
Элементы управления	
Создать	При нажатии кнопки окно возможности закрывается, возможность отображается у ОЗ
Отменить	При нажатии кнопки окно создания возможности закрывается без применения введенных данных

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) Нажать в его строке кнопку «Контекстное меню» (•••). Выбрать «Потоки данных».
3) Откроется страница «Создание возможности “Триггер потока данных”» (рис. 22). Заполнить поля страницы необходимыми параметрами и нажать кнопку «Сохранить». Состав и описание полей страницы приведены в таблице 10.

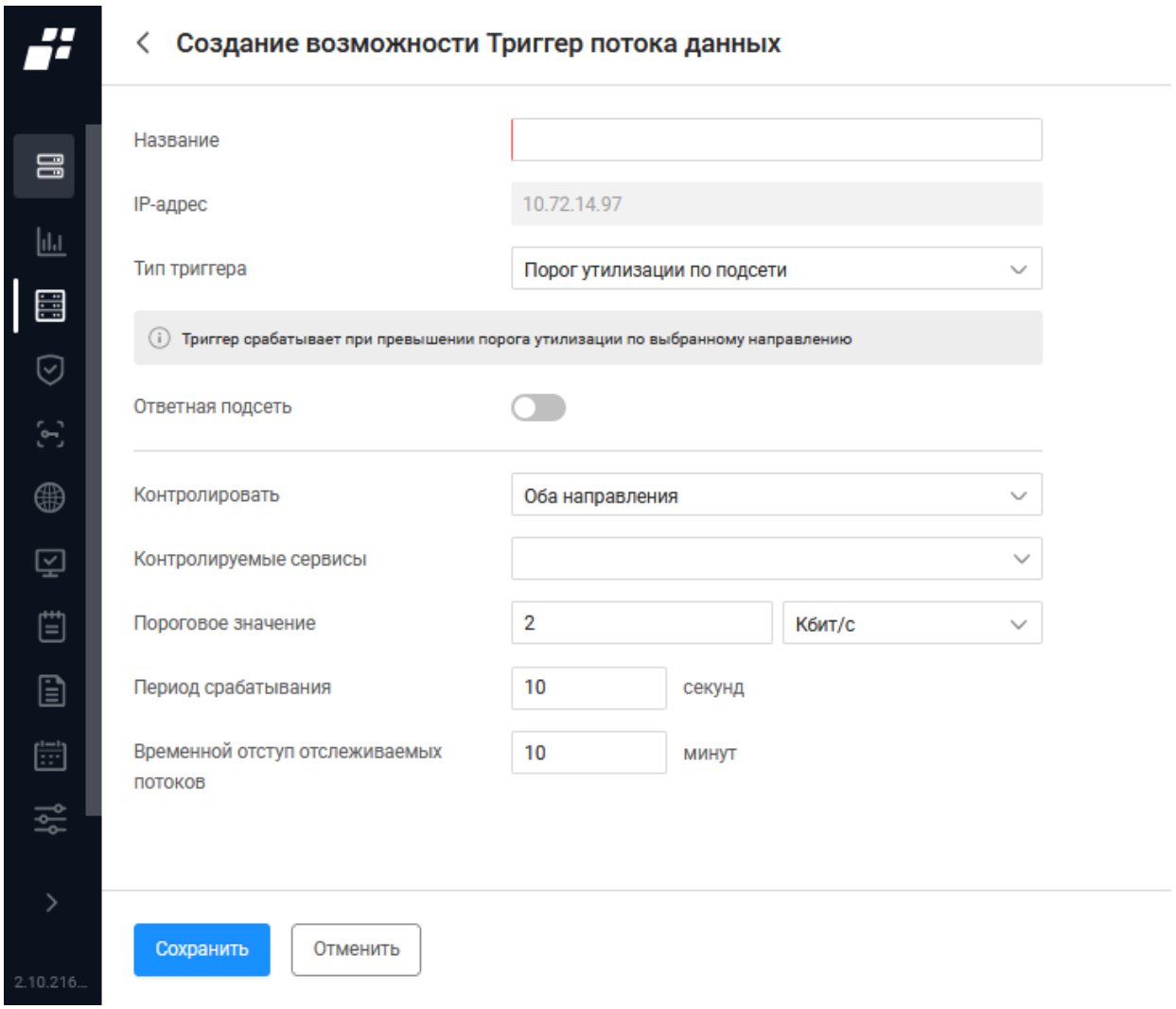


Рисунок 22 – Страница «Создание возможности “Триггер потока данных”»

Таблица 10 – Состав и описание полей страницы «Создание возможности Триггер потока данных»

Поле	Описание
Поле «Название»	Текстовое поле для ввода названия 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 поля	Состав полей с дополнительными параметрами настройки возможности зависит от выбранного типа триггера в поле «Тип триггера»
Элементы управления	
Сохранить	При нажатии кнопки создается возможность «Триггер потока данных» у ОЗ
Отменить	При нажатии кнопки выполняется переход на страницу ОЗ без сохранения внесенных данных

5.1.1.6 Изменение параметров ОЗ

Для изменения параметров ОЗ пользователю необходимо выполнить следующие действия:

1) В дереве ОЗ выделить необходимый ОЗ. Нажать в его строке кнопку «Контекстное меню» (•••). Выбрать пункт «Изменить». Откроется страница редактирования параметров ОЗ с активной вкладкой «Настройки» (рис. 23).
2) Внести при необходимости изменения в параметры ОЗ (название, IP-адрес и др.), для чего нажать кнопку «Изменить объект защиты», в открывшемся окне (аналогично окну создания ОЗ) внести требуемые изменения и нажать кнопку «Сохранить».
3) Внести при необходимости изменения в состав меток ОЗ, для чего:

— нажать ссылку в поле «Метки»;

— в открывшемся окне (рис. 24) добавить, при необходимости, новую метку, нажав кнопку «Метка» (+ Метка), заполнив поля открывшегося окна (выбрать цвет метки и ввести ее название) и нажав кнопку «Создать»;

— выбрать установкой флагов требуемые метки;

— нажать кнопку «Сохранить».

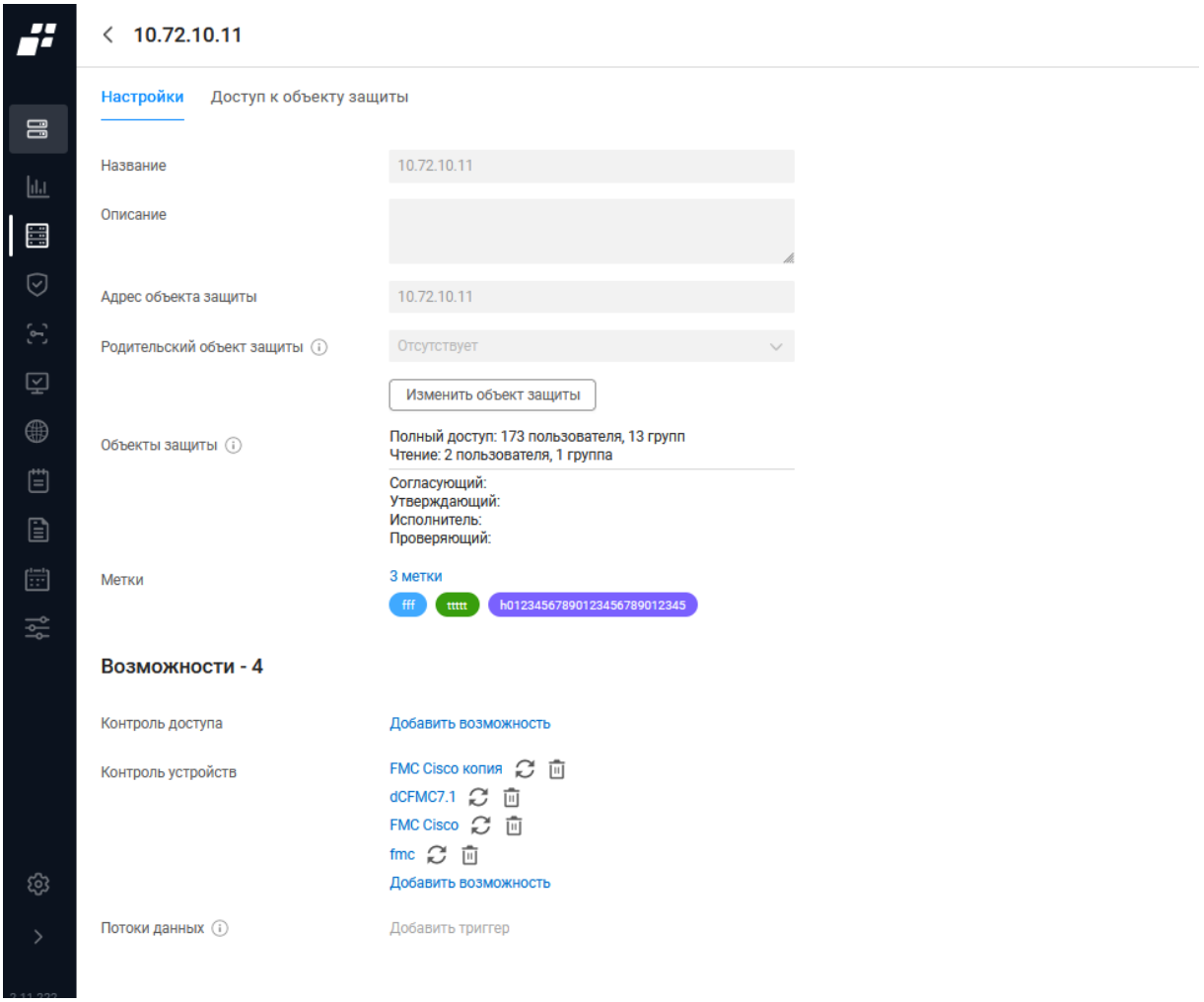


Рисунок 23 – Страница редактирования параметров ОЗ с активной вкладкой «Настройки»

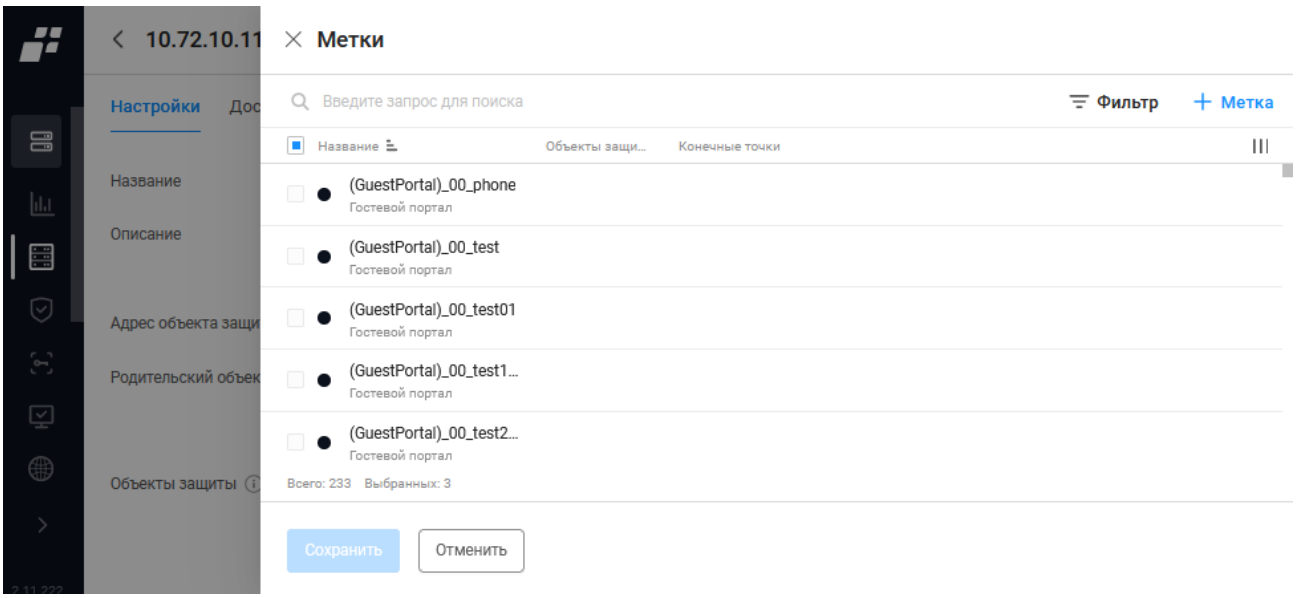


Рисунок 24 – Окно создания/выбора меток ОЗ

4) Просмотреть параметры имеющихся возможностей ОЗ и внести в них требуемые изменения. Для внесения изменений в параметры одной из возможностей – нажать ссылку-название возможности, на открывшейся странице возможности просмотреть параметры, внести требуемые изменения в соответствии с пунктами 5.1.1.3, 5.1.1.4, 5.1.1.5 и нажать кнопку «Сохранить».

5) Внести изменения в состав возможностей ОЗ. Для добавления возможности – нажать в поле типа добавляемой возможности ссылку «Добавить возможность» и далее в зависимости от типа возможности выполнить действия пунктов 5.1.1.3, 5.1.1.4 или 5.1.1.5. Существующие возможности – обновить, нажав кнопку «Обновить» (), или удалить, нажав кнопку «Удалить» (), в строке возможности.

6) Перейти на вкладку «Доступ к объекту защиты» (рис. 25) и отредактировать доступ к ОЗ, для чего установить флаг в полях требуемых пользователей (отмечены пиктограммой «») или групп пользователей (отмечены пиктограммой «») и выбрать в отобразившемся над списком пользователей поле «Права доступа» требуемое значение «Отсутствует», «Чтение», «Полный» (полный доступ) или «Наследовать» (от родительского ОЗ). Повторить действия для всех требуемых пользователей.

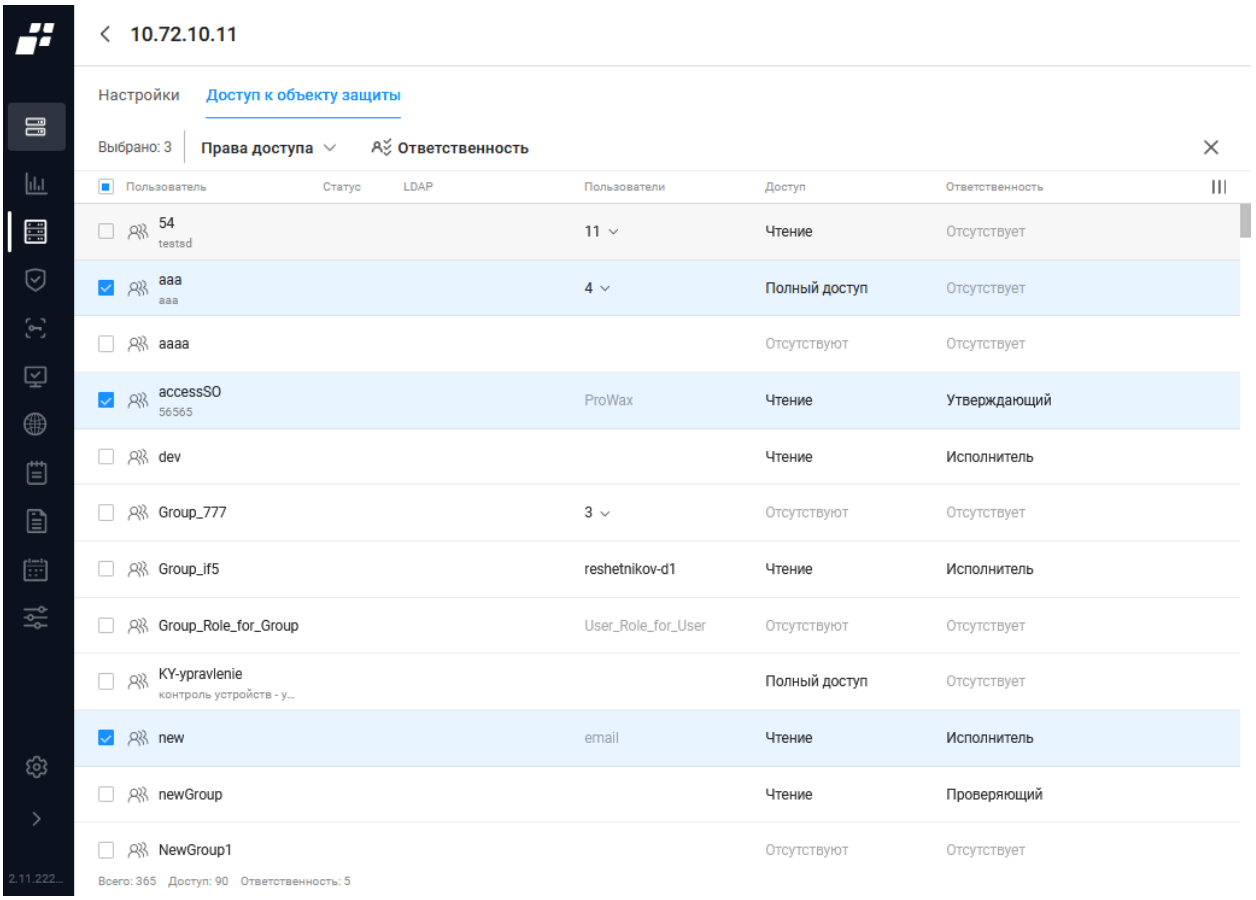


Рисунок 25 – Страница редактирования параметров ОЗ с активной вкладкой «Доступ к объекту защиты»

7) Назначить пользователям типы ответственности при работе с заявками по данному ОЗ, для чего установить флаг в полях требуемых пользователей (отмечены пиктограммой «») или групп пользователей (отмечены пиктограммой «») нажать отобразившуюся над списком пользователей кнопку «Ответственность». В открывшемся окне назначения пользователям типа ответственности выбрать установкой флага требуемые типы ответственности и нажать кнопку «Назначить». Повторить действия для всех требуемых пользователей.

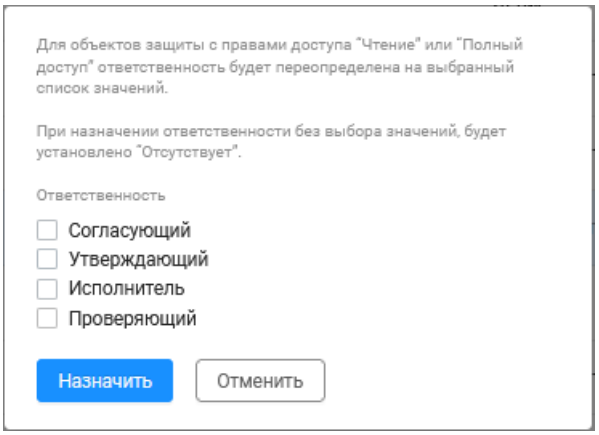


Рисунок 26 – Окно назначения пользователям типа ответственности

5.1.2 Блок «Информация об ОЗ»

Блок с описанием ОЗ (рис. 27) содержит следующую информацию:

- название устройства;
- описание устройства;
- адрес устройства;
- доступ к объекту защиты. Содержит данные о количестве пользователей и групп пользователей комплекса, имеющих полный доступ и доступ на чтение к ОЗ, а также количество пользователей, которым назначены типы ответственности при работе с заявками ОЗ «Согласующий», «Утверждающий», «Исполнитель» и/или «Проверяющий». Является ссылкой, при переходе по которой открывается окно редактирования параметров ОЗ. Во кладке «Доступ к объекту защиты» отображается список пользователей и групп пользователей комплекса для просмотра назначенного им типа доступа к ОЗ или типа ответственности при работе с заявками ОЗ. При наличии особых привилегий пользователь может редактировать доступ у группы пользователей и у каждого пользователя индивидуально (подробнее см. п. 5.1.1.6);
- расписания, назначенные ОЗ. Является ссылкой. При переходе открывается окно, в котором пользователь может поменять статус использования расписания: «вкл.»/«выкл.»;
- метки. Является ссылкой. При переходе открывается окно, в котором

пользователь может создать собственные метки для фильтрации ОЗ в дереве и выбрать из числа имеющихся меток требуемые метки;

— кнопка «Изменить» (Изменить). Позволяет пользователю перейти в окно редактирования ОЗ и внести требуемые изменения (см. п. 5.1.1.6).

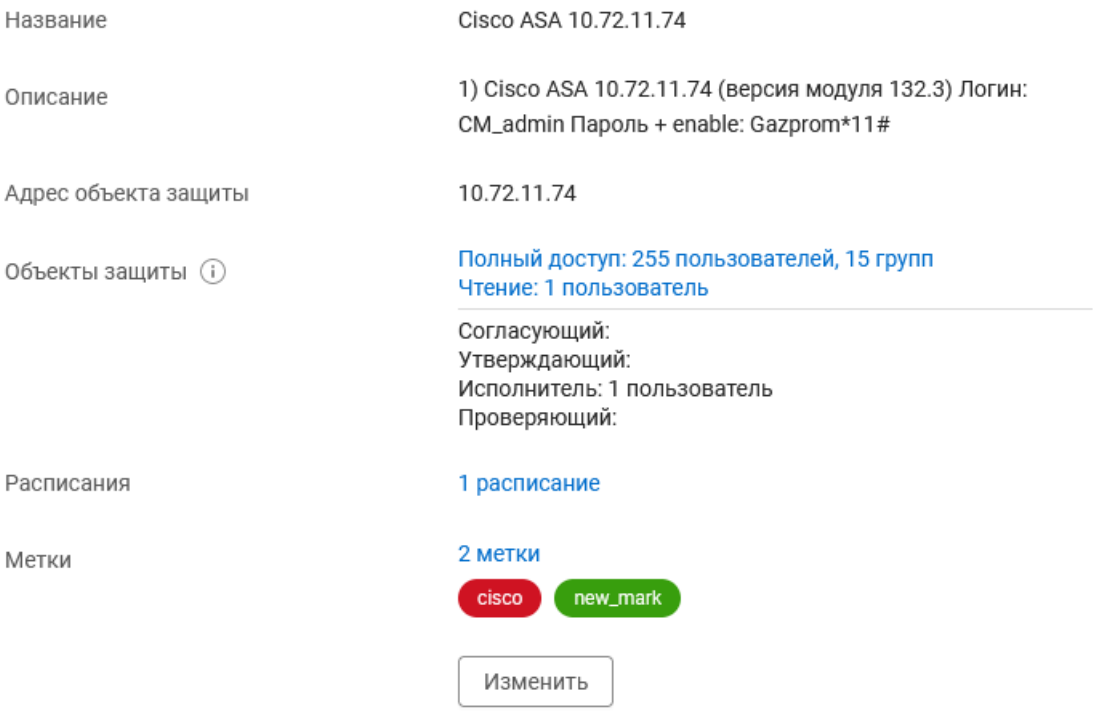


Рисунок 27 – Блок «Информация об ОЗ»

5.1.3 Блок «Возможности»

Блок «Возможности» содержит информацию о назначенных возможностях ОЗ (рис. 28). Назначить возможности ОЗ в данном блоке невозможно. При переходе по ссылке-названию устройства появляется доступ для просмотра и редактирования возможности.

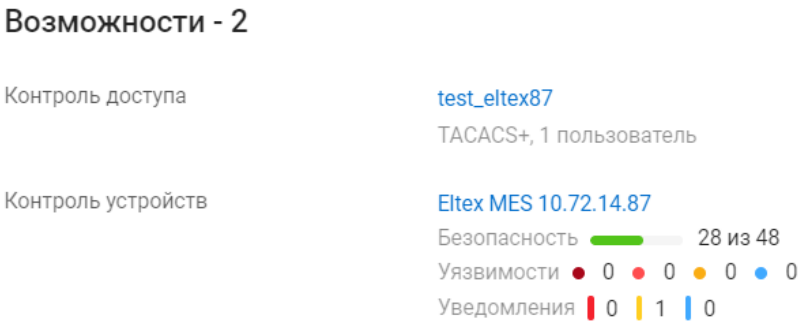


Рисунок 28 – Блок «Возможности»

5.2 База знаний

Отображаемые данные и доступная функциональность в подразделе «База знаний» зависят 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 используются следующие утилиты, протоколы и системы сканирования:

- возможность «Потоки»;
- атрибуты RADIUS;
- загрузка файла с данными формата .csv;
- UserAgent;
- протокол SNMP;
- сканер DHCP;
- сканер DNS;
- сканеры уязвимостей «MaxPatrol 8», «RedCheck» и «SafeERP Pentest».

Полученные данные хранятся в БД комплекса в виде результатов обработки данных в структурированной форме и используются для решения задач ИБ. В веб-интерфейсе ПК «Efros DO» данные отображаются в подразделе «База знаний» (рис. 29).

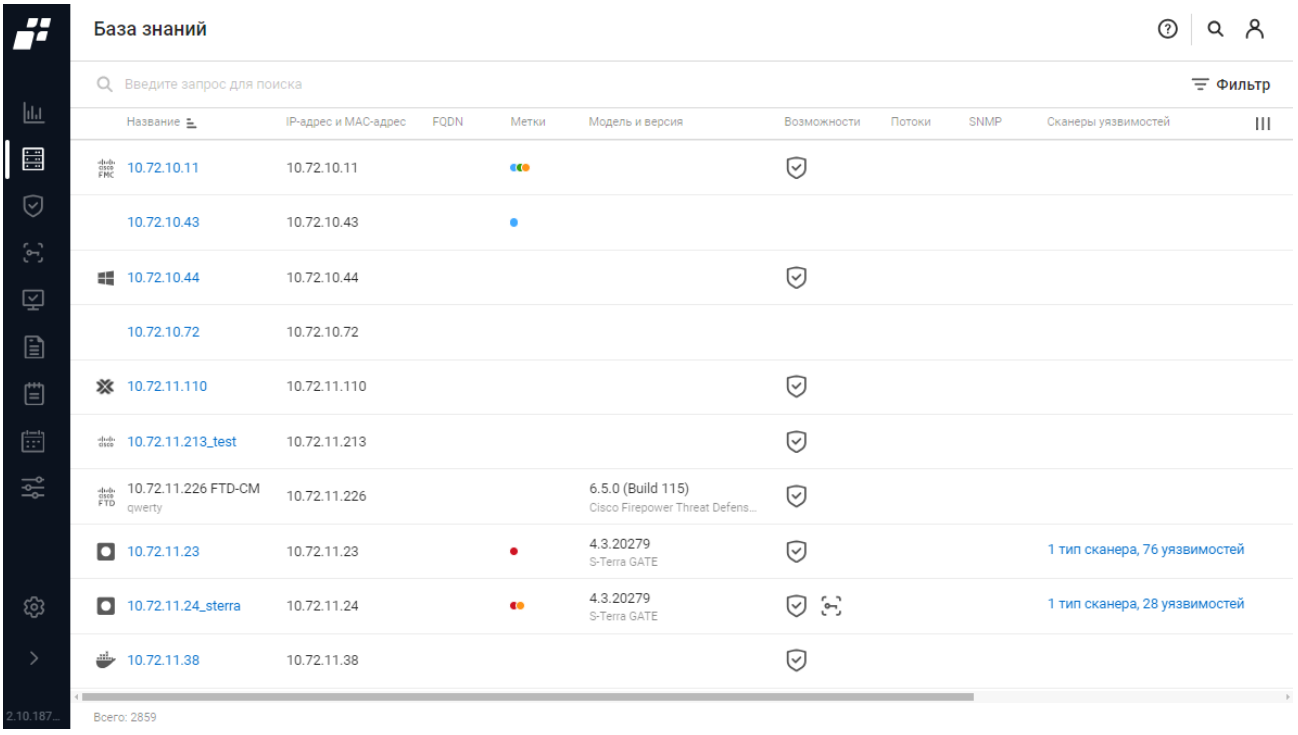


Рисунок 29 – Подраздел «База знаний»

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

- иконка производителя;
- название ОЗ. Является ссылкой. При переходе открывается окно редактирования объекта защиты (подробнее см. п. 5.1.1.6);
- IP-адрес и MAC-адрес устройства;
- доменное имя (FQDN);
- метки. При наведении на пиктограммы курсора открывается подсказка с текстом всех меток;
- модель и версия устройства (если они есть);
- пиктограммы назначенных возможностей (подробнее см. п. 5.1.1);
- интервал времени, прошедший с последнего выполненного пассивного сканирования NetFlow. Является ссылкой. При переходе открывается окно с описанием зафиксированных потоков данных;
- интервал времени, прошедший с последнего выполненного SNMP сканирования. Является ссылкой. При переходе открывается окно с результатами сканирования;
- количестве типов сканеров и количестве уязвимостей. Является ссылкой. При переходе открывается окно с перечнем обнаруженных уязвимостей (более подробно см. п. 5.2.1).

Над списком объектов сети располагаются:

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

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

5.2.1 Сканеры уязвимостей

Результаты сканирования ОЗ на наличие уязвимостей приведены в колонке «Сканеры уязвимостей» подраздела «База знаний». Значение является ссылкой, при нажатии на которую открывается соответствующее окно (рис. 30).

Настройка работы сканеров уязвимостей осуществляется в подразделе «Планировщик» при создании задачи по расписанию «Загрузить уязвимости со сканера» (подробнее см. п. 10.4.2.1).

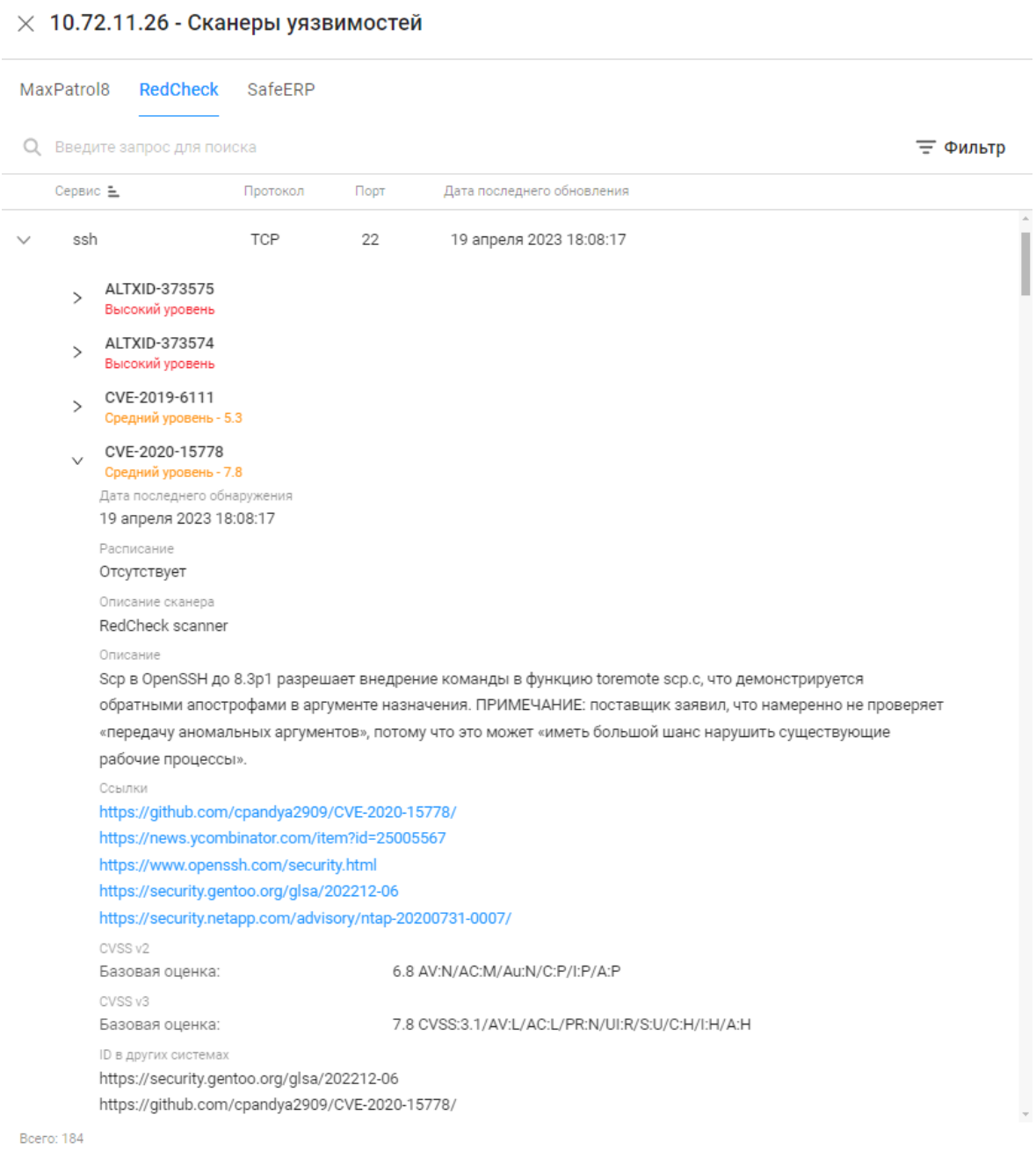


Рисунок 30 – Окно результатов сканирования ОЗ на наличие уязвимостей

Для ОЗ в заголовке указан IP-адрес и приведены вкладки примененных сканеров уязвимости:

- «MaxPatrol8»;
- «RedCheck»;
- «SafeERP».

В таблице с раскрывающимися списками приведена информация об уязвимостях, обнаруженных сканерами уязвимостей, с группировкой по названию сервиса, протоколу и порту. Для каждой сгруппированной строки указана дата последнего обновления.

Значение «N/A» применено, если в отчете сканирования нет данных о названии сервиса или протокола.

Строка таблицы содержит раскрывающийся перечень уязвимостей, со следующими данными:

- название уязвимости;
- уровень критичности:
  - «Критический уровень»;
  - «Высокий уровень»;
  - «Средний уровень»;
  - «Низкий уровень»;
  - «Доступна информация»;
  - «Недоступна информация».
- оценка из CVSS.

Раскрывающийся список с данными уязвимости содержит следующие поля:

- «Дата последнего обнаружения» – дата последнего сканирования, в котором была обнаружена уязвимость;
- «Расписание» – название задачи сканирования, обнаружившей уязвимость;
- «Описание сканера» – описание сканера из отчета сканирования;
- «Описание» – описание уязвимости;
- «Ссылки» – ссылки на другие источники информации об уязвимости;
- «Как исправить» – информация о способах устранения уязвимости;
- блок полей «CVSS v2»:
  - «Базовая оценка» – базовая оценка и базовый вектор CVSS2;
  - «Временная оценка» – временная оценка и временный вектор CVSS2.
- блок полей «CVSS v3»:
  - «Базовая оценка» – базовая оценка и базовый вектор CVSS3;
  - «Временная оценка» – временная оценка и временный вектор CVSS3.
- «ID в других системах» – идентификатор уязвимости в других системах.

Если в результате сканирования не было обнаружено уязвимостей, то на соответствующей вкладке сканера будет выведено сообщение «Уязвимости не обнаружены» и данные о времени последнего обновления информации.

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 из файла формата .csv (более подробно см. подраздел 11.7). Кроме этого, пользователь может создавать собственные конечные точки/группы конечных точек, просматривать данные, полученные о конечных точках в результате профилирования, управлять статусами 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. 31).

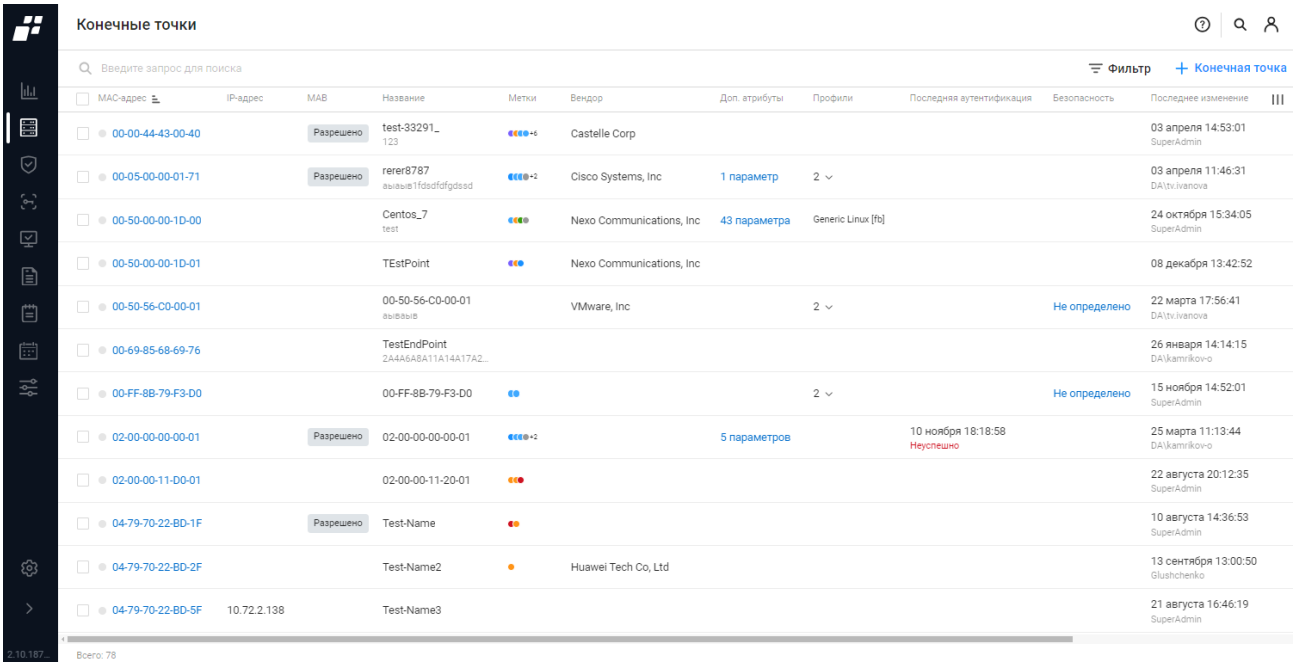


Рисунок 31 – Подраздел «Конечные точки»

Список конечных точек реализован в виде таблицы. 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 по которой открывается окно редактирования конечной точки;
- IP-адрес конечной точки;
- MAB – отображает информацию: запрещена или разрешена аутентификация устройств, подключаемых к сети по MAC-адресам;

— название конечной точки;
— метки – при наведении на пиктограммы курсора открывается подсказка с текстом всех меток конечной точки;
— вендор – производитель конечной точки согласно MAC-адресу;
— дополнительные атрибуты – динамически формируемый список параметров, получаемых от следующих источников:
  - RADIUS (данные аутентификации/аудита);
  - DHCP;
  - User-Agent;
  - Edo-Agent;
  - SNMP.
— профили – профиль конечной точки, полученный в результате ее классификации, или количество профилей, если их два и более (при установке в поле курсора раскрывается список всех профилей);
— последняя аутентификация – дата и время подключения, а также результат попытки подключения «Успешно», «Неуспешно»;
— безопасность – статус проверки требований политики безопасности на конечной точке. Возможные значения – «Соответствует», «Не соответствует», «Не определено». Пустое поле означает, что статус неизвестен, суппликант EDO на конечную точку не установлен, проверок не проводилось. Статус является ссылкой, при переходе по которой открывается окно проверки требований политики безопасности (более подробно см. п. 5.3.3)
— дата и время внесения последних изменений;
— пользователь – имя пользователя, содержащегося в запросе при попытке получения доступа к сети (по умолчанию в таблице не отображается);
— сервер – MAC-адрес сетевого устройства, содержащийся в запросе при попытке получения доступа к сети (через разделитель может присутствовать имя беспроводной сети) (по умолчанию в таблице не отображается).

Над списком с конечными точками располагаются:

— поле поиска (Введите запрос для поиска);
— кнопка «Фильтр» ( );
— кнопка «Конечная точка» (+ Конечная точка);
— кнопка «Колонки» ( ).

При установке флага в строках нескольких конечных точек над списком появляются следующие кнопки групповых действий:

— «Разрешить MAB» – разрешает аутентификацию устройств, подключаемых к сети по MAC-адресам;
— «Запретить MAB» – запрещает аутентификацию устройств, подключаемых к сети по MAC-адресам;

— «Добавить метки» – позволяет добавить пользовательские метки;
— «Создать копию» (Создать копию) – позволяет создать копию конечной точки;
— «Удалить» (Удалить) – позволяет удалить выбранную конечную точку.

При установке флага для одной конечной точки кнопка «Создать копию» (Создать копию) над таблицей отсутствует.

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

5.3.1 Профилирование конечной точки

Профилирование или определение профиля — это 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;
— атрибуты HTTP User-Agent, получаемые при открытии пользователем страницы подключения к гостевому порталу;
— атрибуты Edo-Agent, получаемые при установке на конечную точку агента ПК «Efros DO» и подключении к комплексу.

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

5.3.2 Добавление новой конечной точки вручную

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

1) Нажать кнопку «Конечная точка» (+ Конечная точка).
2) Откроется страница «Создание конечной точки сети» (рис. 32). Заполнить поля страницы необходимыми параметрами. Состав и описание полей вкладки «Основные» приведены в таблице 11.
3) На вкладке «Дополнительные атрибуты» отображается список источников профилирования и их параметры (атрибуты) в табличном виде. Данные на вкладке заполняются автоматически при выборе профиля и недоступны для

редактирования (рис. 33).

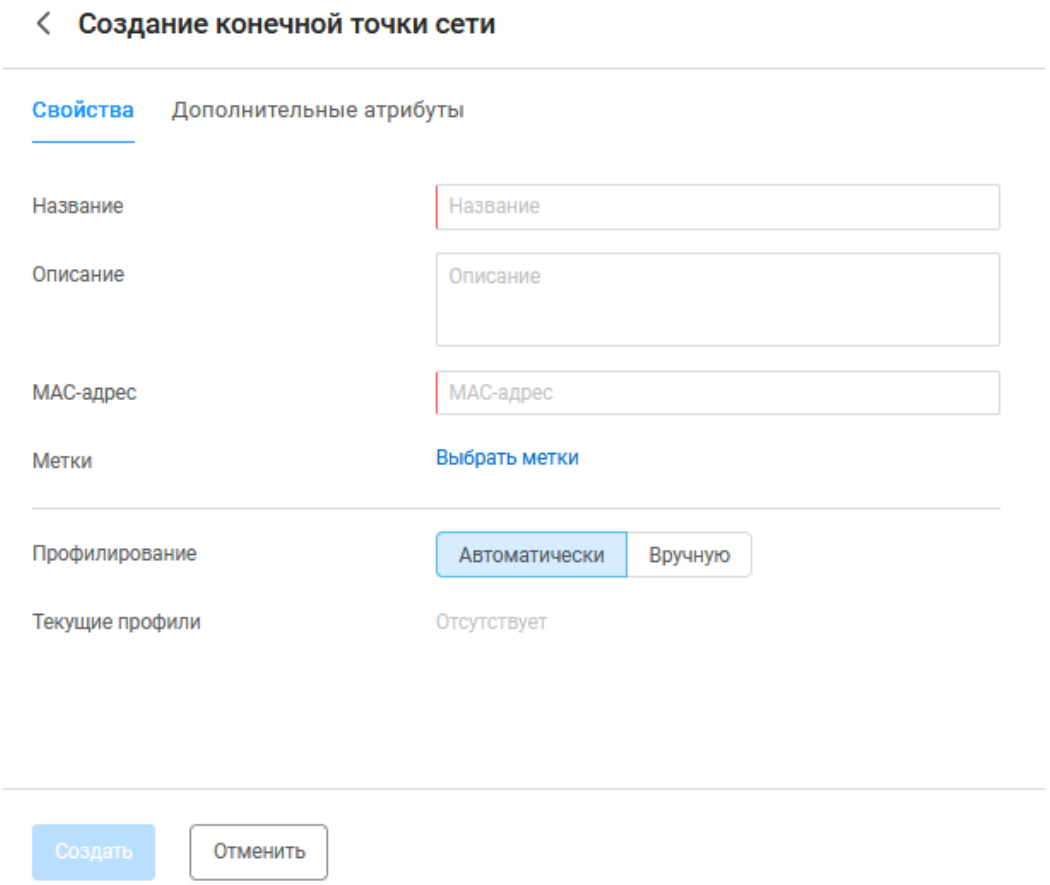


Рисунок 32 – Вкладка «Свойства»

Таблица 11 – Состав и описание полей вкладки «Свойства» страницы создания конечной точки

Поле	Описание
Поле «Название»	Текстовое поле для ввода названия конечной токи. Параметры ввода текста: от 1 до 50 символов. Допустимые символы: буквы латинского алфавита, цифры, «_», «–»
Поле «Описание»	Текстовое поле для ввода описания оконечной точки. 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 кнопки «Выбрать метки» открывается окно с метками, созданными пользователями комплекса ранее для ОЗ и конечных точек. Метки в окне разрешено создавать, редактировать и удалять Для назначения конечной точке необходимо выбрать установкой флагов требуемые метки и

Поле	Описание
	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 профилей необходимо нажать на ссылку «Выбрать профили», в открывшемся окне выбрать установкой флагов требуемые профили и нажать кнопку «Выбрать»
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

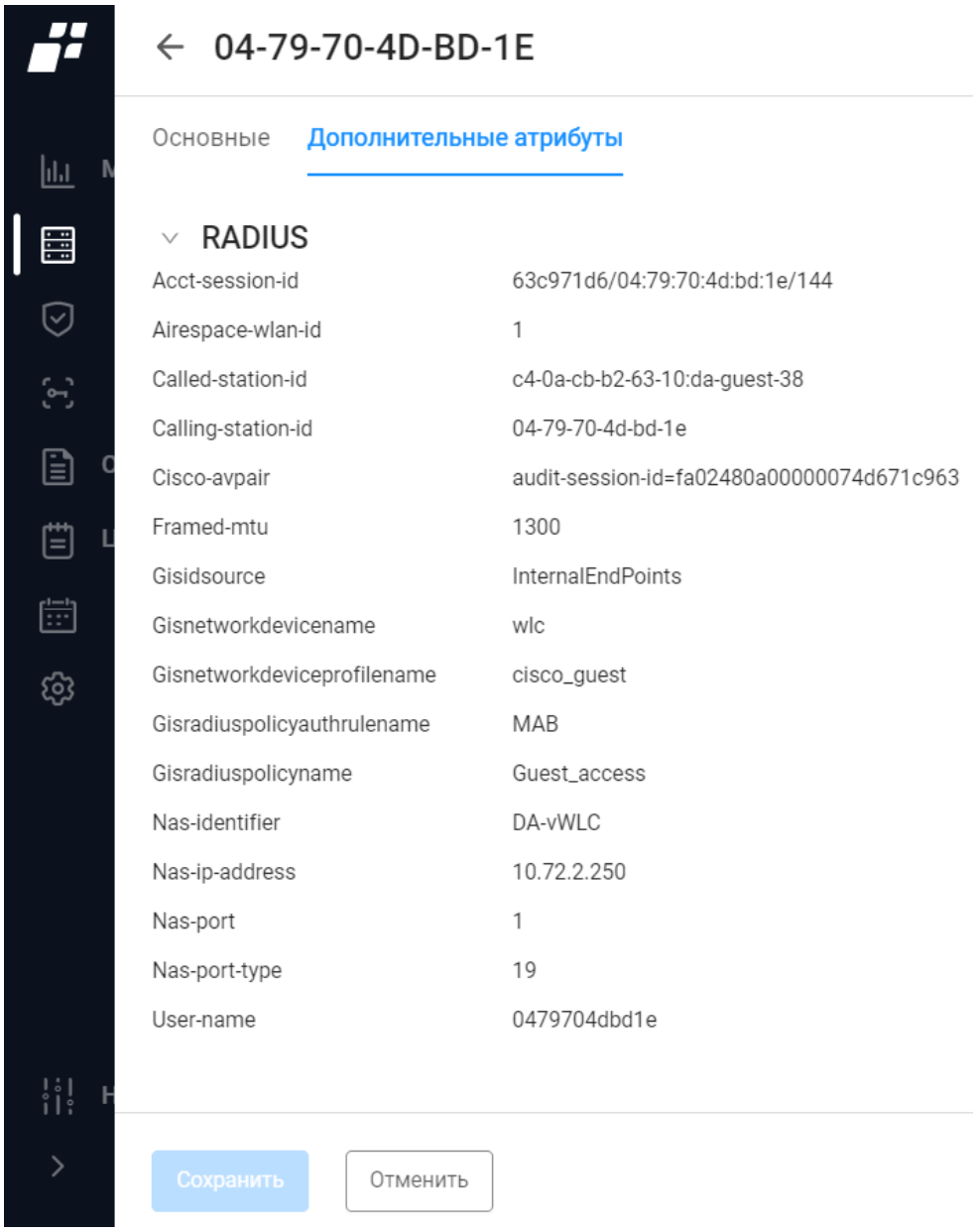


Рисунок 33 – Вкладка «Дополнительные атрибуты»

5.3.3 Проверка требований политики безопасности

Результат проверки подключенного устройства на соответствие заданным требованиям политики безопасности приведен в колонке «Безопасность» подраздела «Конечные точки». Значение является ссылкой, при нажатии на которую открывается соответствующее окно (рис. 34).

Проверка требований политики безопасности производится при наличии установленного агента ПК «Efros DO» для конечной точки и предварительно настроенной политики безопасности.

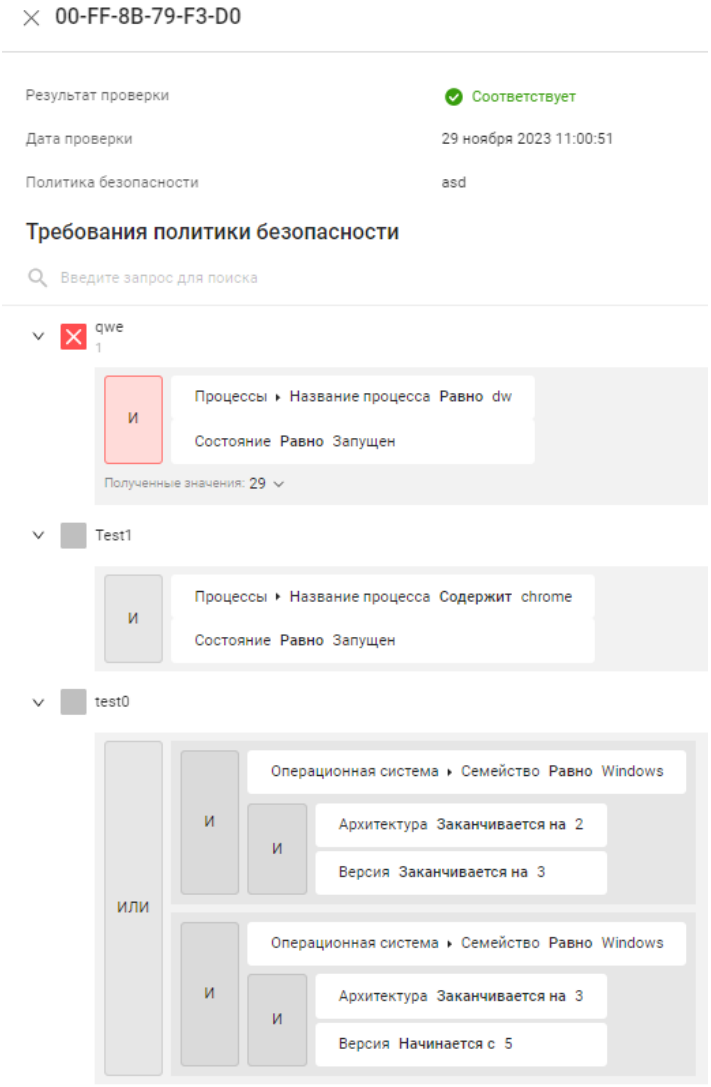


Рисунок 34 – Окно результата проверки требований политики безопасности

Для конечной точки в заголовке указан MAC-адрес и приведены следующие данные:

- результат проверки: «Соответствует», «Не соответствует», «Не определено»;
- дата и время проверки;
- наименование политики безопасности.

Область «Требования политики безопасности» содержит поле поиска по названию требования и список проверок с раскрывающимися строками блоков условий. Блоки условий состоят из наименования, описания требований политики безопасности и объединены логическими операторами «И», «ИЛИ».

В зависимости от результата проверки требований, для блока условий применены следующие цветовые обозначения:

- зеленый – проверка пройдена успешно;
- красный – проверка не пройдена;
- серый – проверка не производилась.

Количество полученных значений, сформированных в ходе проверки условий блока, приводится под блоком условия. Для просмотра значений необходимо нажать кнопку «Полученные значения».

При успешно пройденной проверке отображаются все значения проверки условий блока. Если проверка не пройдена, то отображаются только проверенные значения.

5.4 Карта сети

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

Подраздел «Карта сети» (рис. 35) 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.

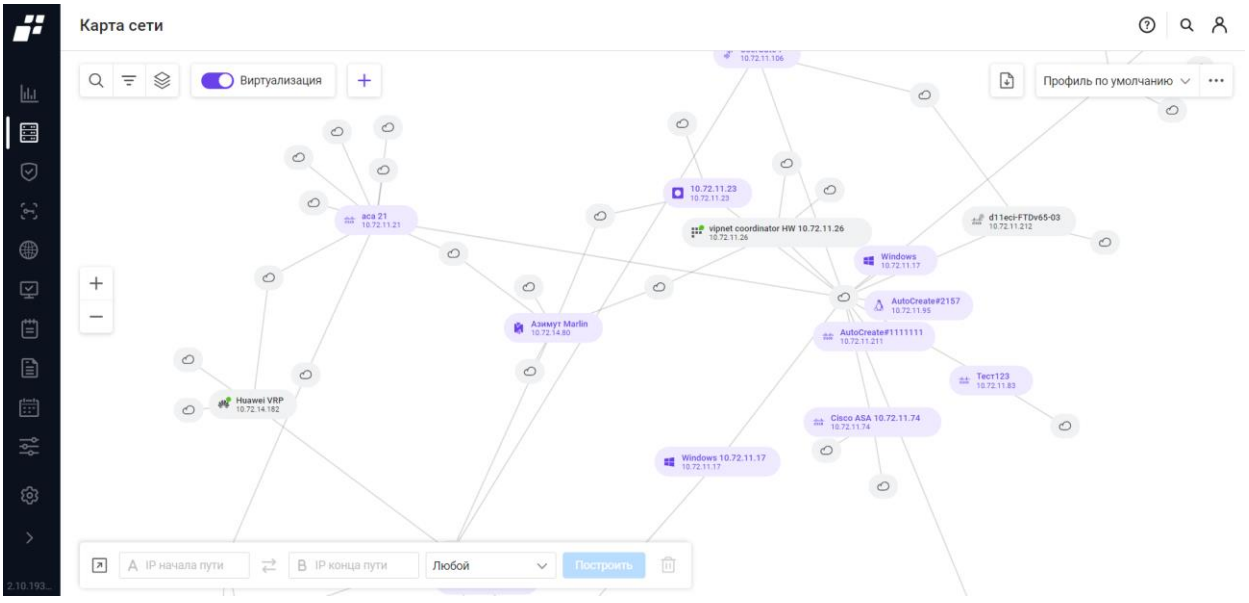


Рисунок 35 – Подраздел «Карта сети»

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

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

При наведении курсора на выбранный физический ОЗ (выделен серым цветом) появляется окно со следующей информацией (рис. 36):

— название и IP-адрес ОЗ;
— иконка производителя;
— статус ОЗ;
— уровень защищенности;
— количество и типы уязвимостей;
— модель, версия ОЗ;
— время последнего обновления;
— протоколы TACACS+/RADIUS;
— кнопки «Начало пути», «Подробнее», «Обновить» ( ).

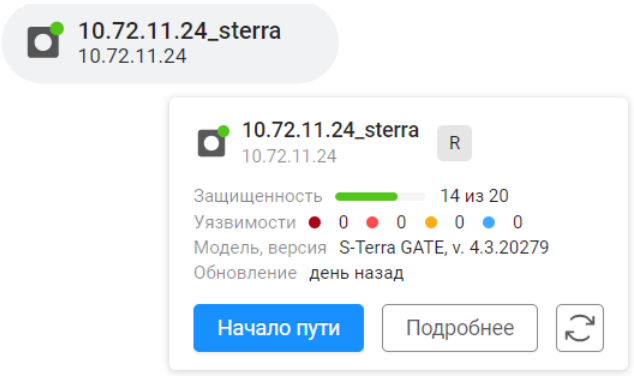
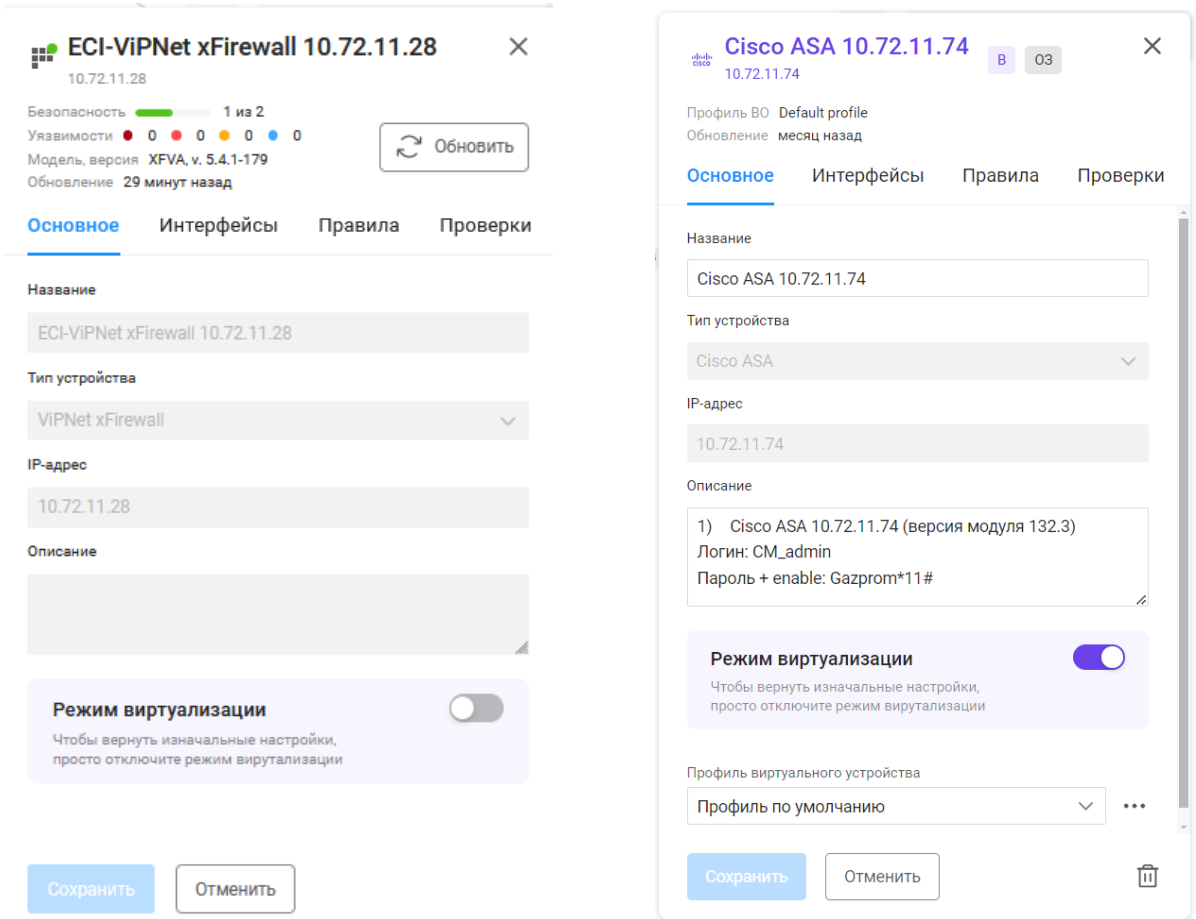


Рисунок 36 – Окно карточки физического ОЗ

При выделении ОЗ (физического или виртуального) и нажатии кнопки «Подробнее», открывается окно с информацией об ОЗ (рис. 37).

В таблице 12 приведен перечень и описание отображаемой информации для физического ОЗ, в таблице 13 – для виртуального ОЗ.



а) физический ОЗ б) виртуальный ОЗ

Рисунок 37 – Окно карточки ОЗ из карты сети

Таблица 12 – Состав и описание полей окна физического ОЗ

Поле	Описание
Поле с описанием ОЗ	Содержит информацию о физическом ОЗ аналогично карточке ОЗ и кнопку «Обновить» ( ) для обновления информации об ОЗ, которая представлена в окне
Вкладка «Основное»	
Поле «Название»*	Название ОЗ
Поле «Тип устройства»*	Тип устройства
Поле «IP-адрес»*	IP-адрес ОЗ
Поле «Описание»*	Краткое описание ОЗ
Режим виртуализации	Переключатель в режим виртуализации. При наличии у ОЗ виртуального объекта, подгружается вся информация из первого доступного профиля виртуального объекта
Поле «Метки»	Назначенные метки для ОЗ
Вкладка «Интерфейсы»**	Содержит список интерфейсов в табличной форме
Вкладка «Правила»**	Содержит списки правил МЭ и правил маршрутизации

Поле	Описание
Вкладка «Проверки»**	Содержит проверки межсетевых экранов типов «Зонный анализ» и «Оптимизация правил»
Элементы управления	
Сохранить	При нажатии кнопки окно ОЗ закрывается, изменения сохраняются
Отменить	При нажатии кнопки окно ОЗ закрывается без изменений
*Поле недоступно для редактирования. ** Подробное описание вкладки приведено в п. 5.4.1	

Таблица 13 – Состав и описание полей окна виртуального ОЗ

Поле	Описание
Поле с описанием ОЗ	Содержит следующую информацию: — название и IP-адрес ОЗ; — иконка производителя; — иконка виртуального объекта; — иконка наличия физического ОЗ; — профиль виртуального объекта; — время последнего обновления
Вкладка «Основное»	
Поле «Название»	Название ОЗ
Поле «Тип устройства»*	Тип устройства
Поле «IP-адрес»*	IP-адрес ОЗ
Поле «Описание»	Краткое описание ОЗ
Поле «Режим виртуализации»	Переключатель для выключения режима виртуализации и возвращения к изначальным настройкам ОЗ
Поле «Профиль виртуального устройства»	Раскрывающийся список профилей, каждый из которых содержит список параметров конкретного виртуального устройства. По нажатию кнопки «Меню» (•••) раскрывается контекстное меню, позволяющее изменить, обновить и удалить профиль Поле появляется только при редактировании виртуального объекта
Вкладка «Интерфейсы»**	Содержит список интерфейсов
Вкладка «Правила»**	Содержит списки правил МЭ и правил маршрутизации
Вкладка «Проверки»**	Содержит проверки межсетевых экранов типов «Зонный анализ» и «Оптимизация правил»
Элементы управления	
Сохранить	При нажатии кнопки окно ОЗ закрывается, изменения

Поле	Описание
	сохраняются
Отменить	При нажатии кнопки окно ОЗ закрывается без изменений
*Поле недоступно для редактирования. ** Подробное описание вкладки приведено в п. 5.4.1	

На странице карты сети располагаются:

- поле поиска ( );
- кнопка «Фильтр» ( );
- кнопка «Слои» ( ) – позволяет пользователю скрыть/отобразить такие атрибуты ОЗ и подсетей, как:
  - «Тип устройства»;
  - «Название»;
  - «IP-адрес»;
  - «VPN-туннели»;
  - «Адрес подсети»;
  - «Нетранзитные подсети».
- кнопка активации режима виртуализации. Позволяет показать скрытые виртуальные ОЗ;
- кнопка ( ) для создания виртуального объекта (отображается при активации режима виртуализации);
- кнопка экспорта « » для экспорта карты сети (всей или ее части по выбору пользователя) в необходимом формате (PNG или SVG по выбору пользователя ;
- поле для выбора профиля карты сети ( ). 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. 38).

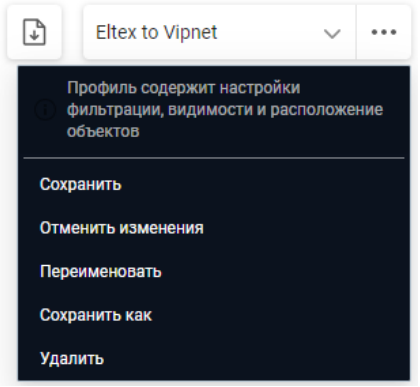


Рисунок 38 – Контекстное меню

— кнопки изменения масштаба карты сети;
— панель построения маршрута для проверки прохождения трафика между устройствами (подробнее см. п. 5.4.2).

5.4.1 Добавление и редактирование 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» (рис. 39). Состав и описание полей приведены в таблице 14.

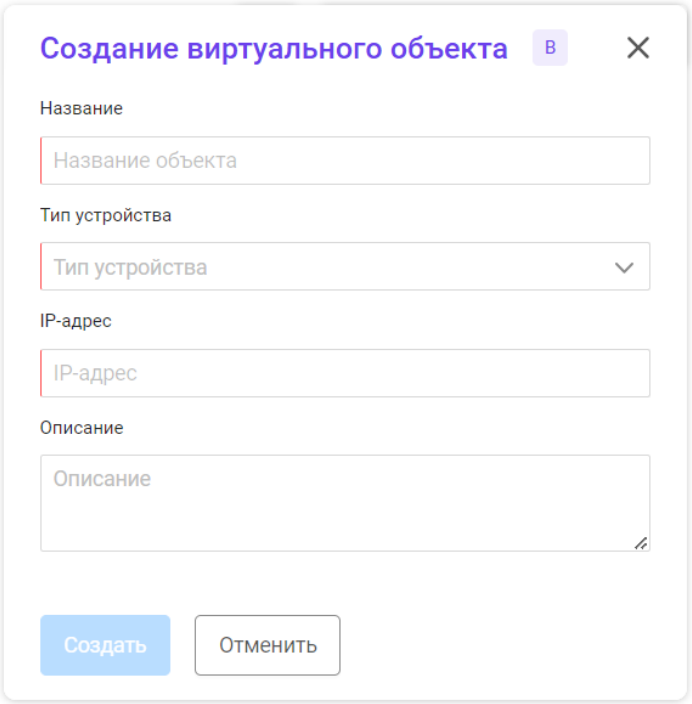


Рисунок 39 – Окно «Создание виртуального объекта»

Таблица 14 – Состав и описание полей окна «Создание виртуального объекта»

Поле	Описание
Поле «Название»	Текстовое поле для ввода названия виртуального ОЗ. Параметры ввода текста: от 1 до 50 любых символов
Поле «Тип устройства»	Раскрывающийся список типов устройств
Поле «IP-адрес»	Поле для ввода IP-адреса виртуального объекта. 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

Поле	Описание
Элементы управления	
Создать	При нажатии кнопки выполняется переход на страницу настройки виртуального объекта с сохранением внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу карты сети без сохранения внесенных данных

4) Заполнить поля необходимыми параметрами и нажать кнопку «Создать». Созданный виртуальный ОЗ отобразится на карте сети.

При создании нового виртуального ОЗ создается новый профиль объекта (профиль конфигураций). При создании виртуального ОЗ на основе физического ОЗ профиль виртуального объекта совпадает с профилем физического ОЗ.

5) Выбрать ОЗ на карте и нажать кнопу «Подробнее». Откроется окно просмотра данных ОЗ (см. рис. 37). Для редактирования доступны вкладки:
- «Основное» – вкладка активна по умолчанию;
- «Интерфейсы»;
- «Правила»;
- «Проверки».

6) Перейти на вкладку «Интерфейсы» (рис. 40).

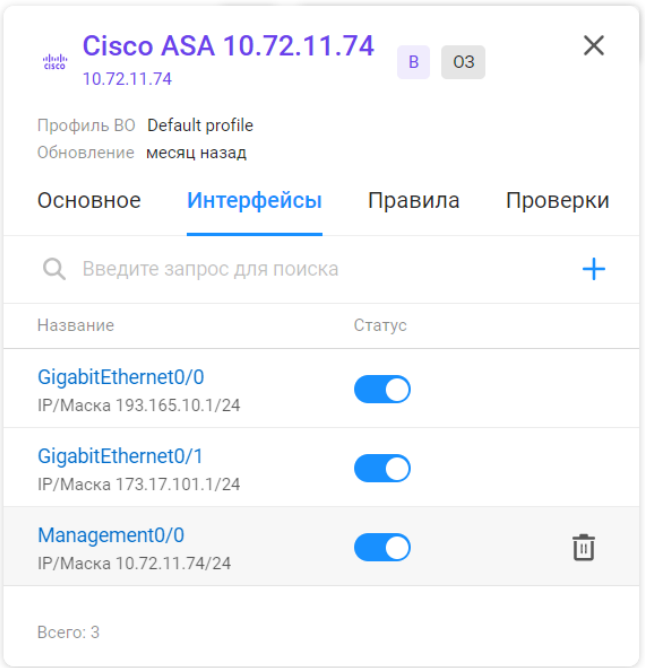


Рисунок 40 – Вкладка «Интерфейсы»

7) Добавить интерфейсы ОЗ. Для добавления одного интерфейса:
— нажать кнопку «Добавить» (+);
— в открывшемся окне «Создание интерфейса» указать название, IP-адрес подсети, выбрать маску подсети;
— нажать кнопку «Создать». Созданный интерфейс отобразится на вкладке.

Добавленные интерфейсы доступны для удаления по нажатию в их строке кнопки «Удалить» (🗑), а также для активации/деактивации установкой соответствующих переключателей в требуемое положение.

8) Перейти на вкладку «Правила» (рис. 41). Вкладка содержит переключатель выбора отображаемого списка правил по их типу «Межсетевые экраны» – правила МЭ, «Маршрутизация» – правила маршрутизации.

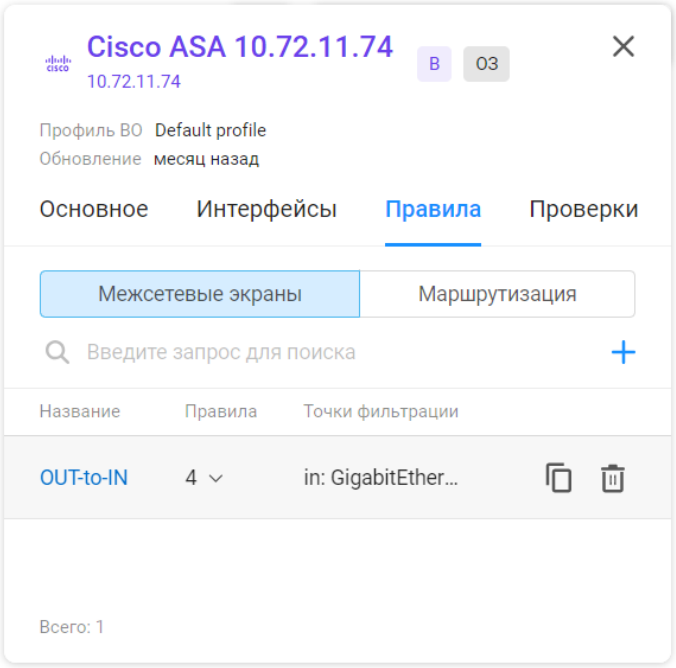


Рисунок 41 – Вкладка «Правила»

9) Добавить требуемые правила МЭ и маршрутизации. Для добавления одного правила МЭ:
— при выбранном типе правил «Межсетевые экраны» нажать кнопку «Добавить» (+). Откроется окно «Создание набора правил МЭ» (рис. 42);
— ввести во вкладке «Настройки» окна название правила и задать список точек фильтрации;
— нажать кнопку «Создать». Станет активна вкладка «Правила»;

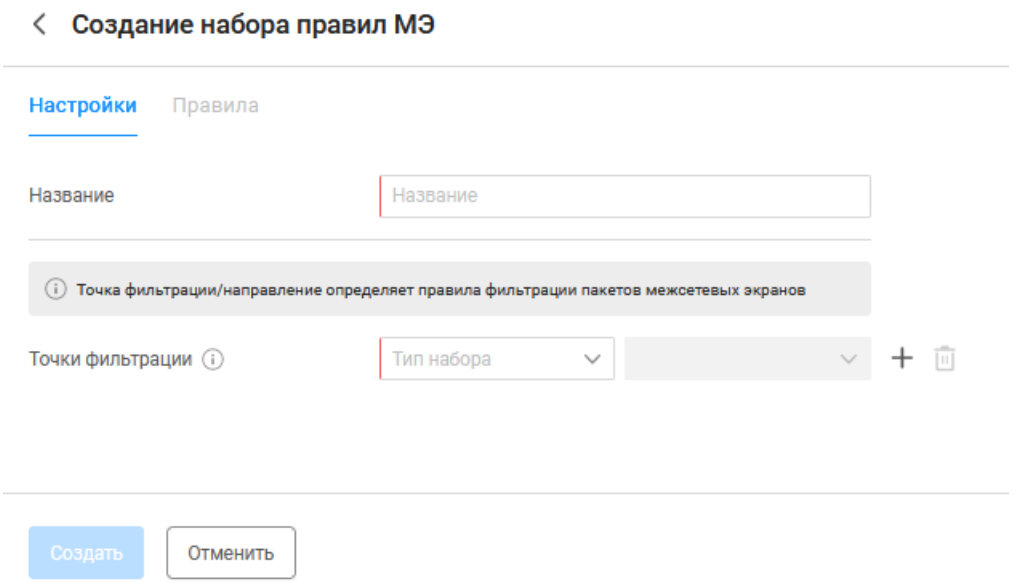


Рисунок 42 – Окно «Создание набора правил МЭ». Вкладка «Настройки»

— нажать кнопку «Создать правило» или «+ Правило». Откроется окно «Создание правила» (рис. 43);

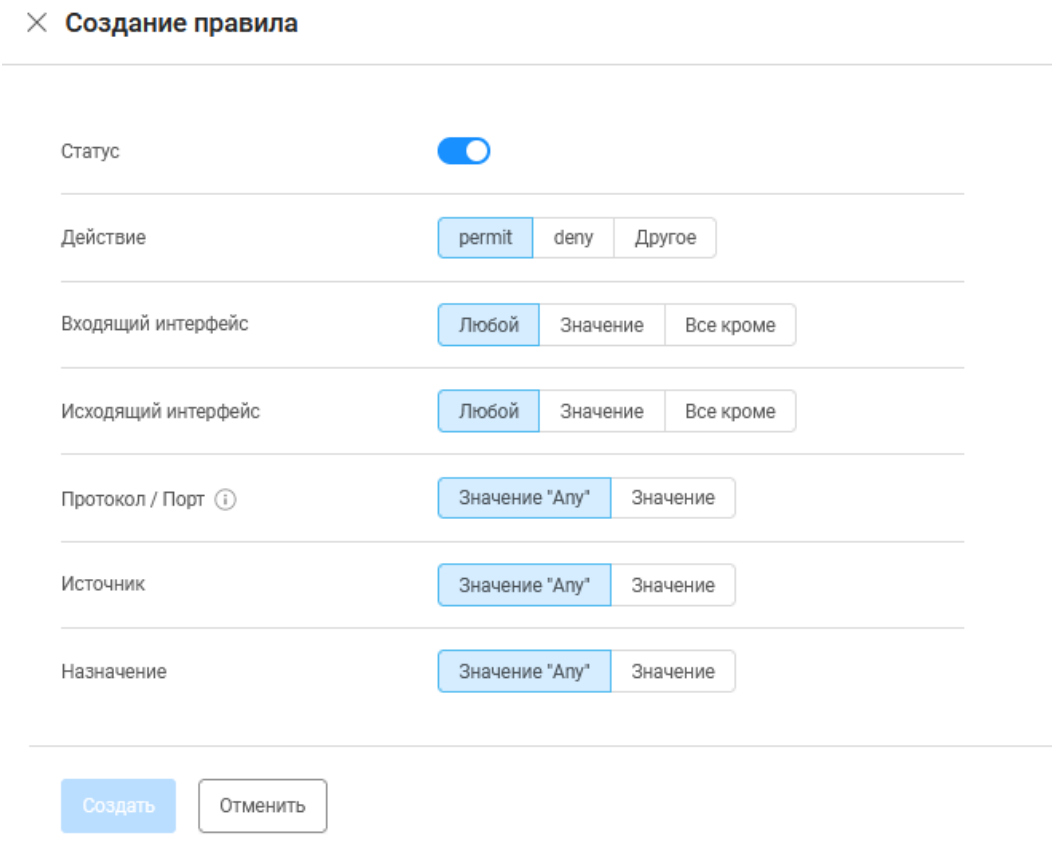


Рисунок 43 – Окно «Создание правила» для правила МЭ

— задать параметры правила, выбрав требуемое положение переключателей и

указав требуемые дополнительные параметры, активировать/деактивировать правило, включив/выключив соответственно переключатель «Статус», и нажать кнопку «Создать»;

— создать все требуемые правила, повторив предыдущие два шага. После добавления правила доступны во вкладке «Правила» (рис. 44) для активации/деактивации (выбор положения переключателя в колонке «Статус»), создания копии и удаления (кнопки в строках правил) и изменения порядка их следования (перетаскиванием пиктограммы «⠿» в требуемое положение);
— нажать во вкладке «Настройки» кнопку «Сохранить». Откроется окно просмотра данных ОЗ. Созданное правило отобразится на вкладке «Правила».

Правило доступно для редактирования (окно редактирования открывается при выборе наименования правила), удаления по кнопке «Удалить» ( ) в строке правила и создания копии правила (по кнопке «Создать копию» ( ) в строке правила).

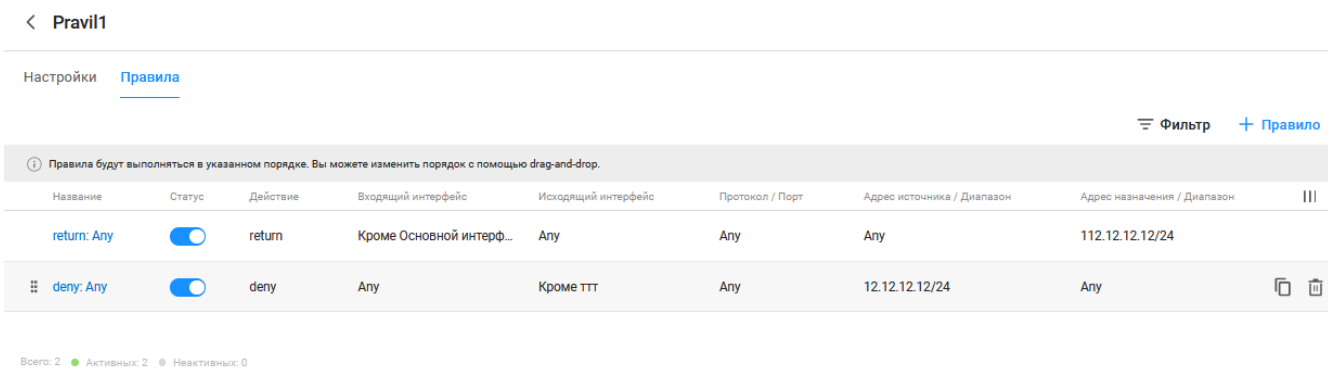


Рисунок 44 – Список правил

10)Для добавления одного правила маршрутизации:

— выбрать тип добавляемого правила «Маршрутизация»;
— нажать кнопку «Добавить» ( ). Откроется окно «Создание правила» (рис. 45);
— выбрать тип правила, указать IP-адрес/маску подсети, для стандартных правил выбрать интерфейс из списка интерфейсов ОЗ и ввести IP-адрес соседнего ОЗ;
— нажать кнопку «Создать». Откроется окно просмотра данных ОЗ. Созданное правило отобразится на вкладке «Правила»;

Правило доступно для редактирования (окно редактирования открывается при выборе наименования правила) и удаления по кнопке «Удалить» ( ) в строке правила.

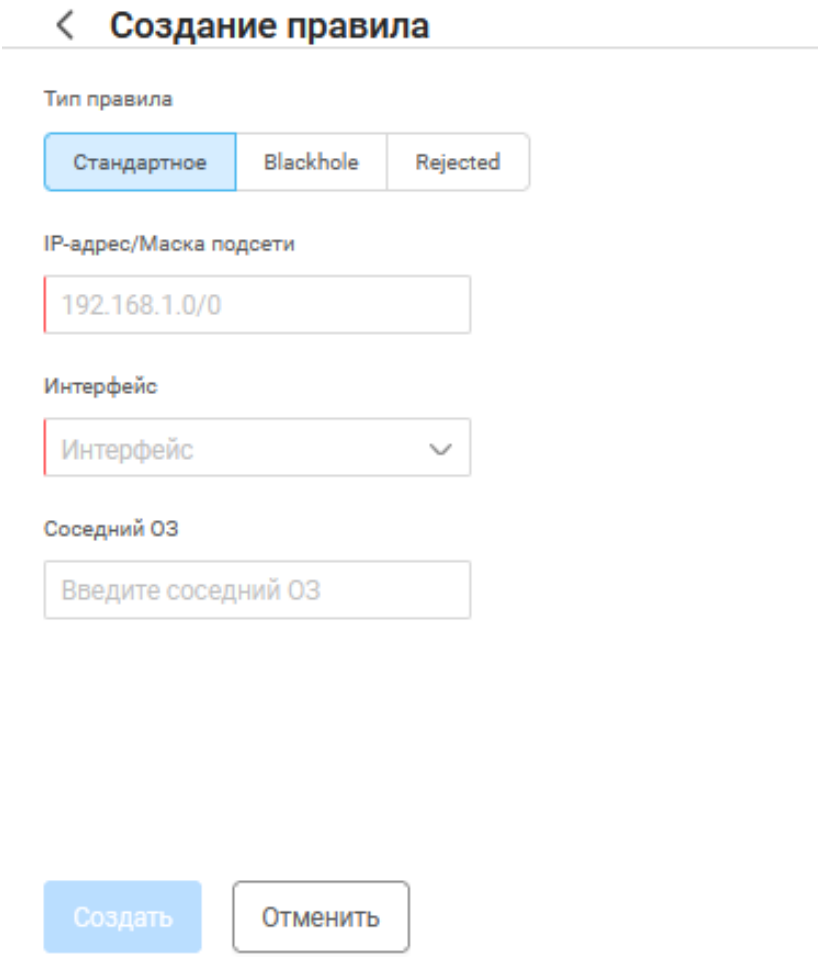


Рисунок 45 – Окно создания правила маршрутизации

11) Перейти на вкладку «Проверки». На вкладке отображаются ссылки МЭ: «Зонный анализ» и «Оптимизация правил» (рис. 46). При переходе по ссылке «Зонный анализ» открывается вкладка «Зонный анализ» подраздела «Проверки МЭ», в которой необходимо создать требуемую проверку (более подробно см. документ «Руководство пользователя. Часть 2. Контроль устройств»). Проверки «Оптимизация правил» срабатывают автоматически, как только назначаются на вкладке «Зонный анализ».

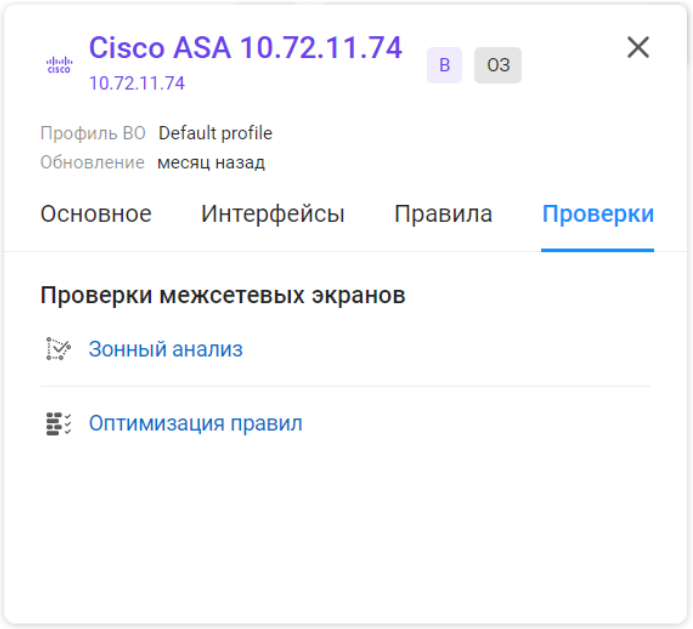


Рисунок 46 – Вкладка «Проверки»

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 кнопку « » в нижнем левом углу карты сети.
2) Откроется окно «Построение маршрута» (рис. 47). Необходимо заполнить поля требуемыми параметрами и нажать кнопку «Создать». Состав и описание полей окна приведены в таблице 15.
3) Нажать кнопку «Построить». После чего будет построен маршрут в окне «Построение маршрута» (рис. 48). Поля вкладки «Настройки» соответствуют полям при построении маршрута.

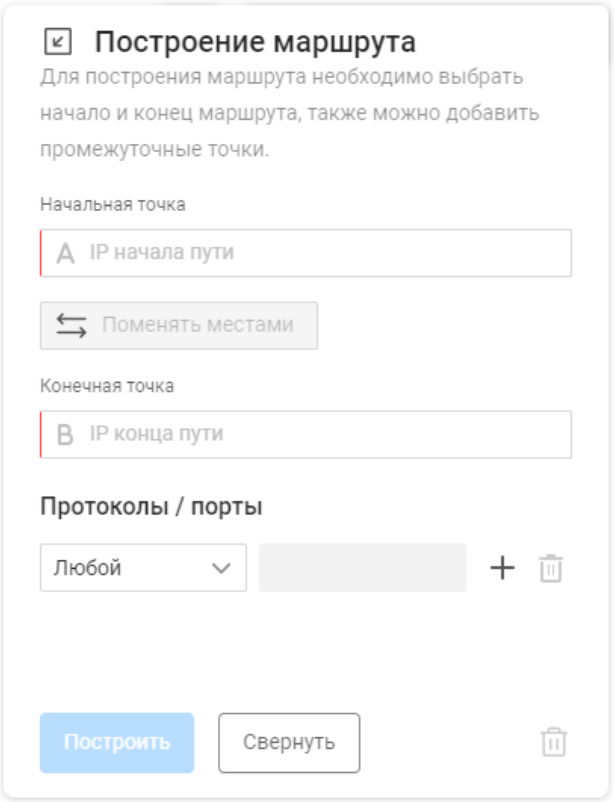


Рисунок 47 – Окно «Построение маршрута»

Таблица 15 – Состав и описание полей окна «Построение маршрута»

Поле	Описание
Поле «Начальная точка»	Поле для ввода IP-адреса ОЗ начальной точки A
Поле «Конечная точка»	Поле для ввода IP-адреса ОЗ конечной точки B
Поле «Протокол / порты»	Поле с раскрывающимся списком протоколов с возможностью поиска по номеру или по названию. Например: ICMP (1); TCP (6); UDP (17)
Элементы управления	
Построить	При нажатии на кнопку окно закрывается, введенные параметры применяются
Свернуть	При нажатии на кнопку вертикальное окно построения маршрута меняется на горизонтальное, при этом поля остаются заполненными
Поменять местами	Позволяет поменять местами начальную и конечную точки для построения маршрута. Кнопка становится активной после заполнения полей «Начальная точка» и «Конечная точка»
Кнопка «Удалить» (🗑)	При нажатии на иконку очищаются все поля, при этом форма остается открытой

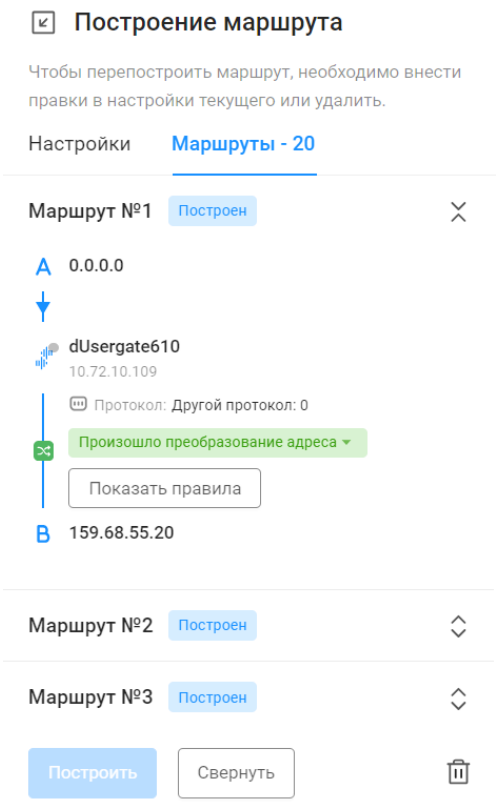


Рисунок 48 – Окно «Построение маршрута» с построенным маршрутом

Способ 2:

1) Заполнить параметры в панели построения маршрута непосредственно на карте сети (рис. 49). Состав и описание полей панели аналогичны составу и описанию полей окна «Построение маршрута» (см. таблицу 15).
2) Нажать кнопку «Построить».

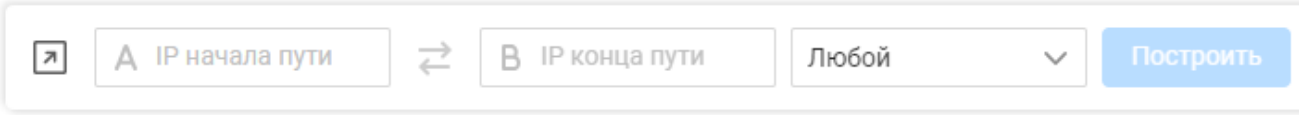


Рисунок 49 – Панель построения маршрута

Способ 3:

1) Навести курсор на необходимый ОЗ.
2) Нажать кнопку «Начало пути».
3) Навести курсор на второй ОЗ.
4) Нажать кнопку «Конец пути».
5) Нажать в открывшемся окне «Построение маршрута» кнопку «Построить».

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.

5.5 Векторы атак

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

Построение векторов атак в комплексе позволяет показать возможные варианты использования уязвимостей, обнаруженных на устройствах сети (рис. 50).

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.

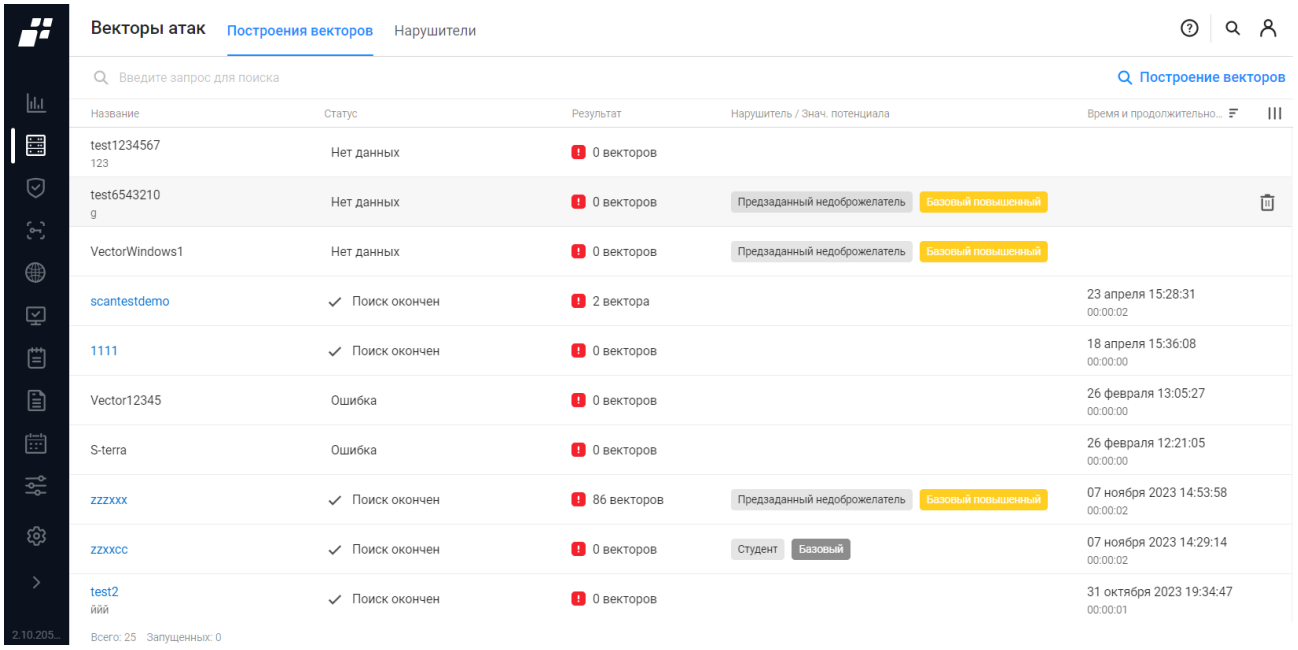


Рисунок 50 – Подраздел «Векторы атак»

Подраздел содержит следующие вкладки:

— «Построения векторов»;
— «Нарушители».

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.

5.5.1 Вкладка «Построения векторов»

На вкладке отображаются построенные вектора атак (см. рис. 50). Список векторов атак реализован в виде таблицы. Для каждой записи таблицы отображаются следующие данные:

— название вектора;
— статус (поиск окончен, ведется поиск, нет данных, ошибка);
— результат построения векторов атак в виде количества найденных векторов атак;
— нарушитель и значение потенциала атаки;
— время и продолжительность построения.

Над таблицей располагаются:

— поле поиска (Введите запрос для поиска);
— кнопка «Построение векторов» (Построение векторов);

— кнопка «Колонки» ( ).

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

— «Удалить» ( );

— «Настройки» ( ).

5.5.1.1 Построение вектора атак

Для создания нового вектора атак необходимо выполнить следующие действия:

1) Нажать кнопку в центре страницы «Построение векторов» (Построение векторов) или на кнопку «Построение векторов» (Построение векторов).
2) Откроется страница «Построение векторов атак» (рис. 51). Заполнить поля необходимыми параметрами и нажать кнопку «Построить». Состав и описание полей страницы приведено в таблице 16.

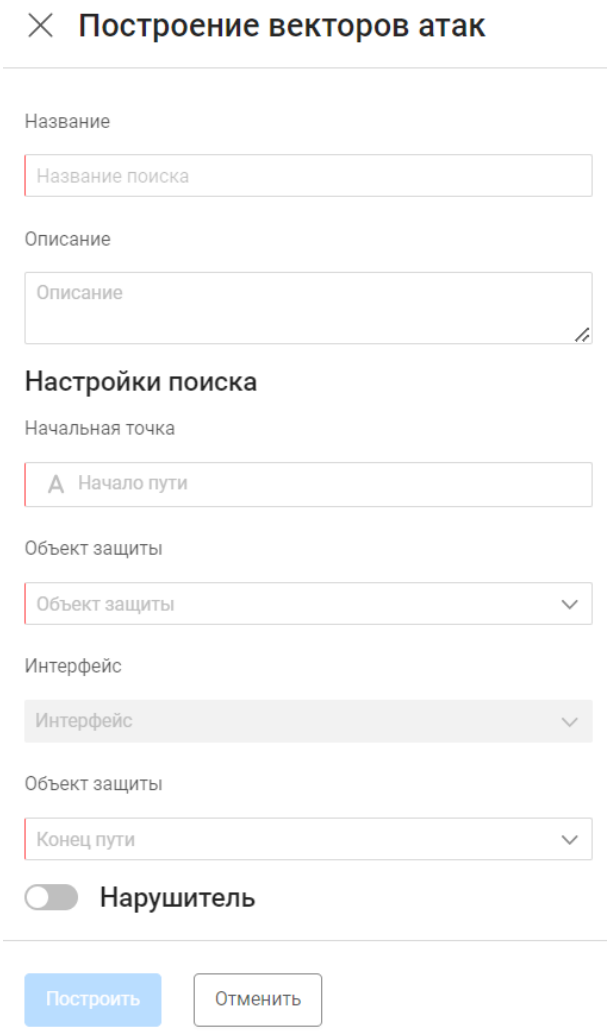


Рисунок 51 – Страница «Построение векторов атак»

Таблица 16 – Состав и описание полей страницы «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 точка)	Раскрывающийся список ОЗ
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) Будет запущен процесс построения векторов атак. Откроется страница раздела «Векторы атак», в списке векторов добавится строка, статус до окончания процесса построения в ней будет «Ведется поиск».
4) После успешного завершения процесса построения векторов атак статус в строке изменится на «Поиск окончен», неуспешного – «Нет данных» или «Ошибка», система отправит сообщение о завершении задачи на E-mail пользователя.

Для того, чтобы система автоматически сообщила о завершении построения векторов атак необходимо убедиться, что активирована задача по событию «Оповещение об окончании расчета векторов атак» (подробнее см. п. 10.4.1).

Вектор атак в статусе «Поиск окончен» доступен для просмотра и повторного построения (см. п. 3)).

5.5.1.2 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». Активной будет вкладка «Векторы» (рис. 52). 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.

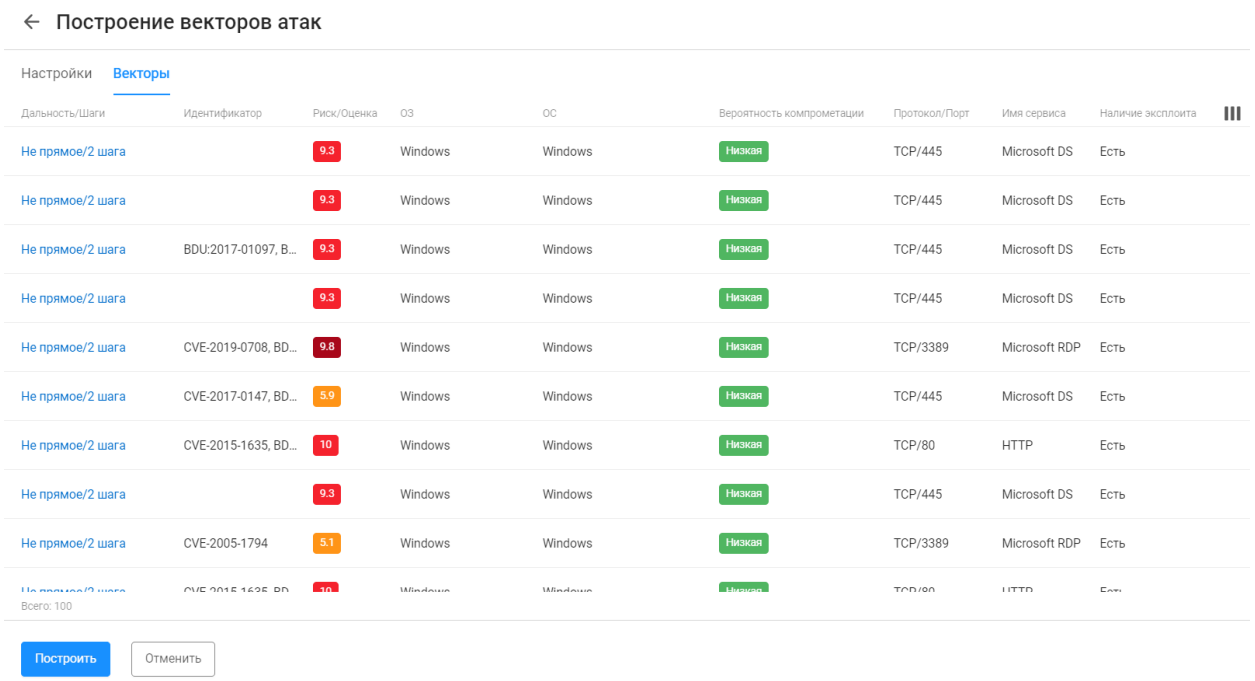


Рисунок 52 – Вкладка «Векторы»

3) Для просмотра отдельного вектора – нажать на ссылку-дальность/шаги. Откроется страница с визуальным отображением вектора атак на карте сети (рис. 53). На странице содержатся следующие данные:

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

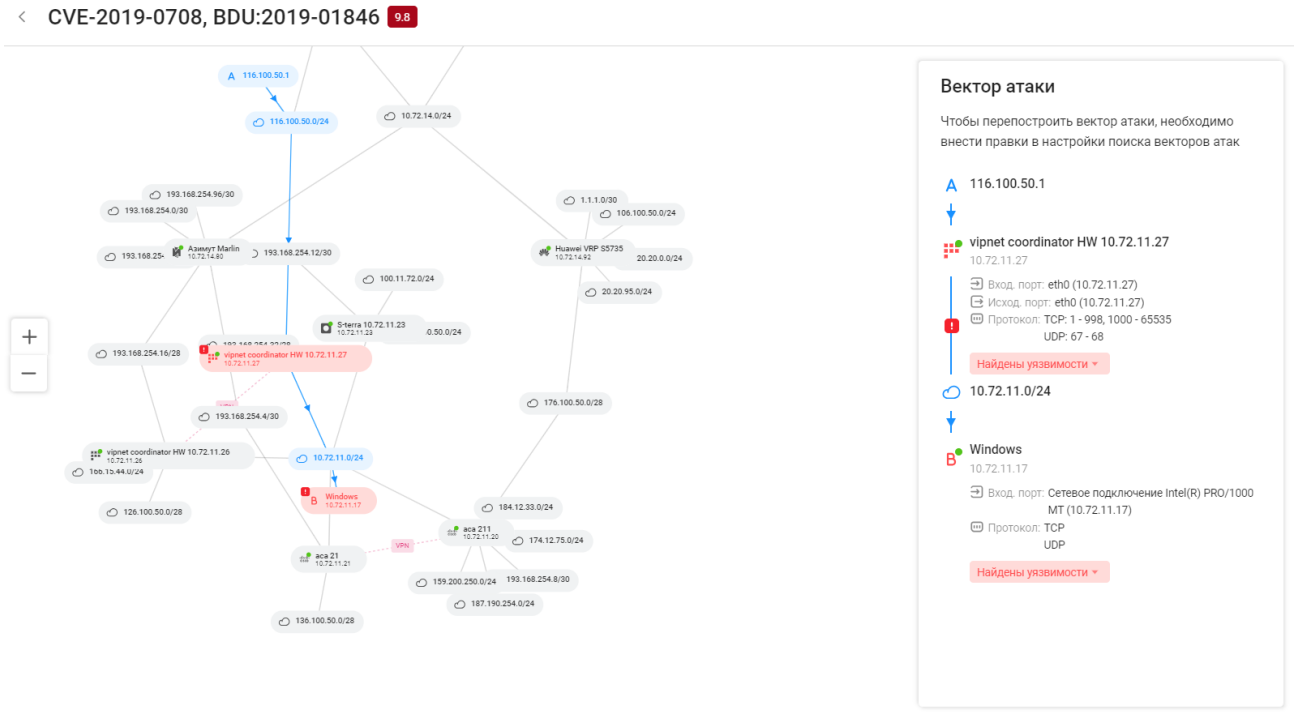


Рисунок 53 – Визуализация вектора атак на карте сети

4) Для возвращения на вкладку «Векторы» – нажать кнопку «<» в заголовке страницы.

Пользователь имеет возможность также скорректировать параметры построения векторов атак и запустить новый процесс построения, для чего:

1) Перейти на вкладку «Настройки» (состав полей вкладки аналогичен составу полей страницы «Построение векторов атак» (см. п. 5.5.1.1).
2) Внести требуемые изменения в настройки построения векторов атак и нажать кнопку «Построить».

5.5.2 Вкладка «Нарушители»

Нарушитель – это лицо или событие (явление), в результате действий (наступления, возникновения) которого 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 ее 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. 54). 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.

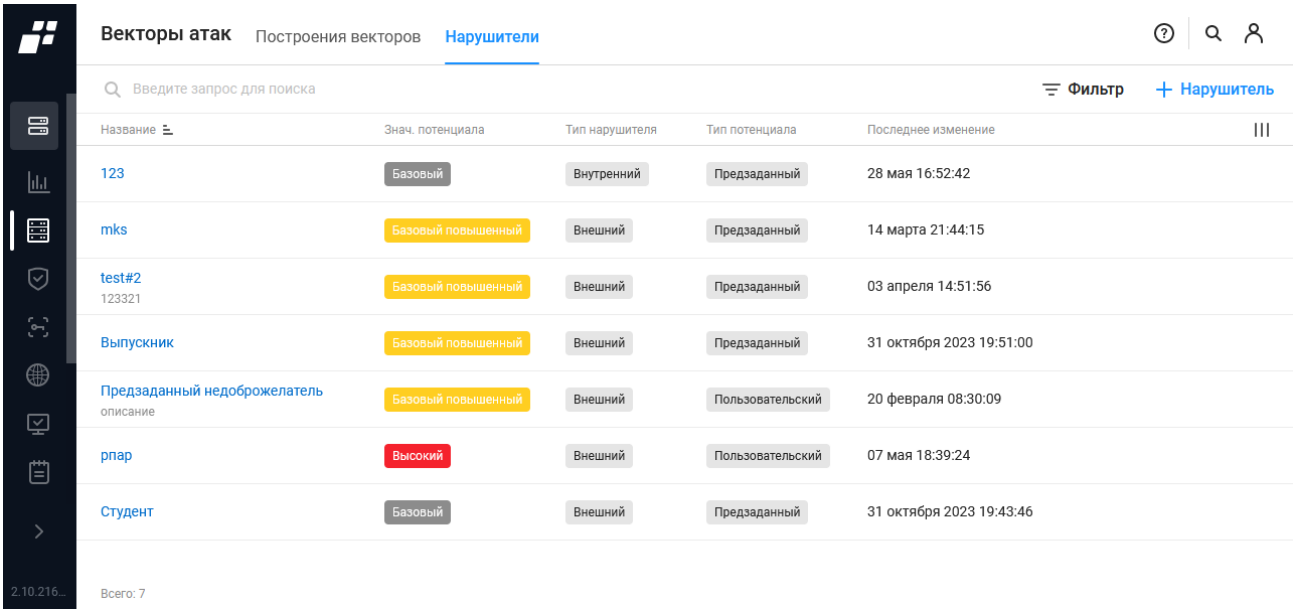


Рисунок 54 – Список нарушителей

Над списком нарушителей располагаются:

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

При выборе строки с нарушителем в строке появляется кнопка «Удалить» ( ).

5.5.2.1 Добавление нарушителя

Для добавления в список нового нарушителя пользователю необходимо:

1) Нажать на странице вкладки «Нарушители» (см. рис. 54) кнопку «Нарушитель» (Нарушитель). Откроется страница создания нового нарушителя (рис. 55). Состав и описание полей страницы приведены в таблице 17.
2) Заполнить поля необходимыми параметрами и нажать кнопку «Создать».

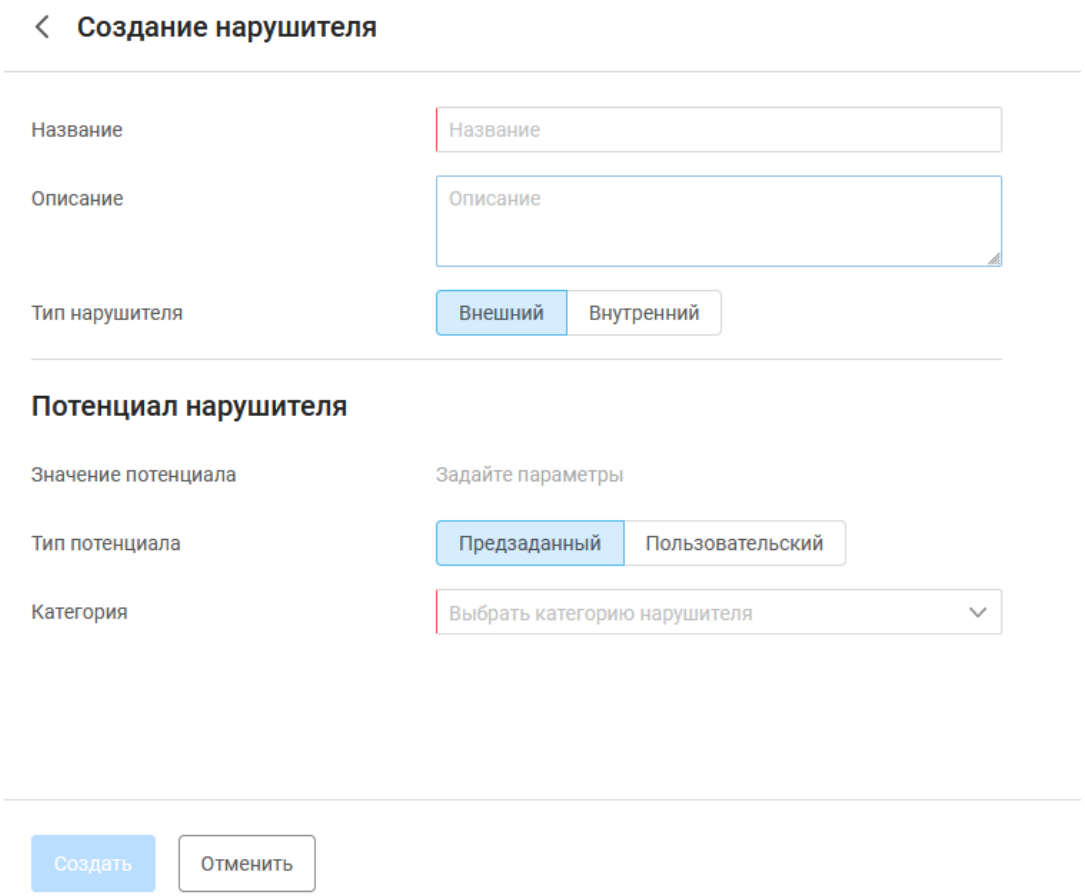


Рисунок 55 – Страница «Создание нарушителя»

Таблица 17 – Состав и описание полей страницы 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	Описание
Поле «Тип нарушителя»	Переключатель: — «Внешний»; — «Внутренний»
Группа полей «Потенциал нарушителя»	
Поле «Значение потенциала»*	Поле недоступно для редактирования. Существуют следующие значения: — «Базовый» – значение по умолчанию; — «Базовый повышенный»; — «Средний»; — «Высокий»
Поле «Тип потенциала»	Переключатель: — «Предзаданный»; — «Пользовательский». При выборе переключателя «Пользовательский» появляются дополнительные поля
Поле «Категория»	Раскрывающийся список с категориями нарушителя
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: — «Знание чувствительной информации»; — «Ограниченные знания»; — «Отсутствие знаний»
Поле «Возможности доступа к ИС»	Раскрывающийся список: — «<30 мин или не обнаруживаемый доступ»; — «<1 дня»; — «<1 месяца»; — «>1 месяца»
Поле «Оснащенность нарушителя»	Раскрывающийся список: — «Оборудование, сделанное на заказ»; — «Отсутствует»; — «Специализированное оборудование»;

Поле	Описание
	— «Стандартное оборудование»
Элементы управления	
Создать	При нажатии кнопки выполняется переход на страницу списка нарушителей с сохранением внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу списка нарушителей без сохранения внесенных данных
*Поле заполняется автоматически и зависит от параметров, указанных в группе полей «Потенциал нарушителя»	

5.6 Сканирование сети

Отображаемые данные и доступная функциональность в подразделе «Сканирование сети» 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 сети» 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. 56). Заполнить поля необходимыми параметрами и нажать кнопку «Выполнить». Состав и описание полей окна приведены в таблице 18.

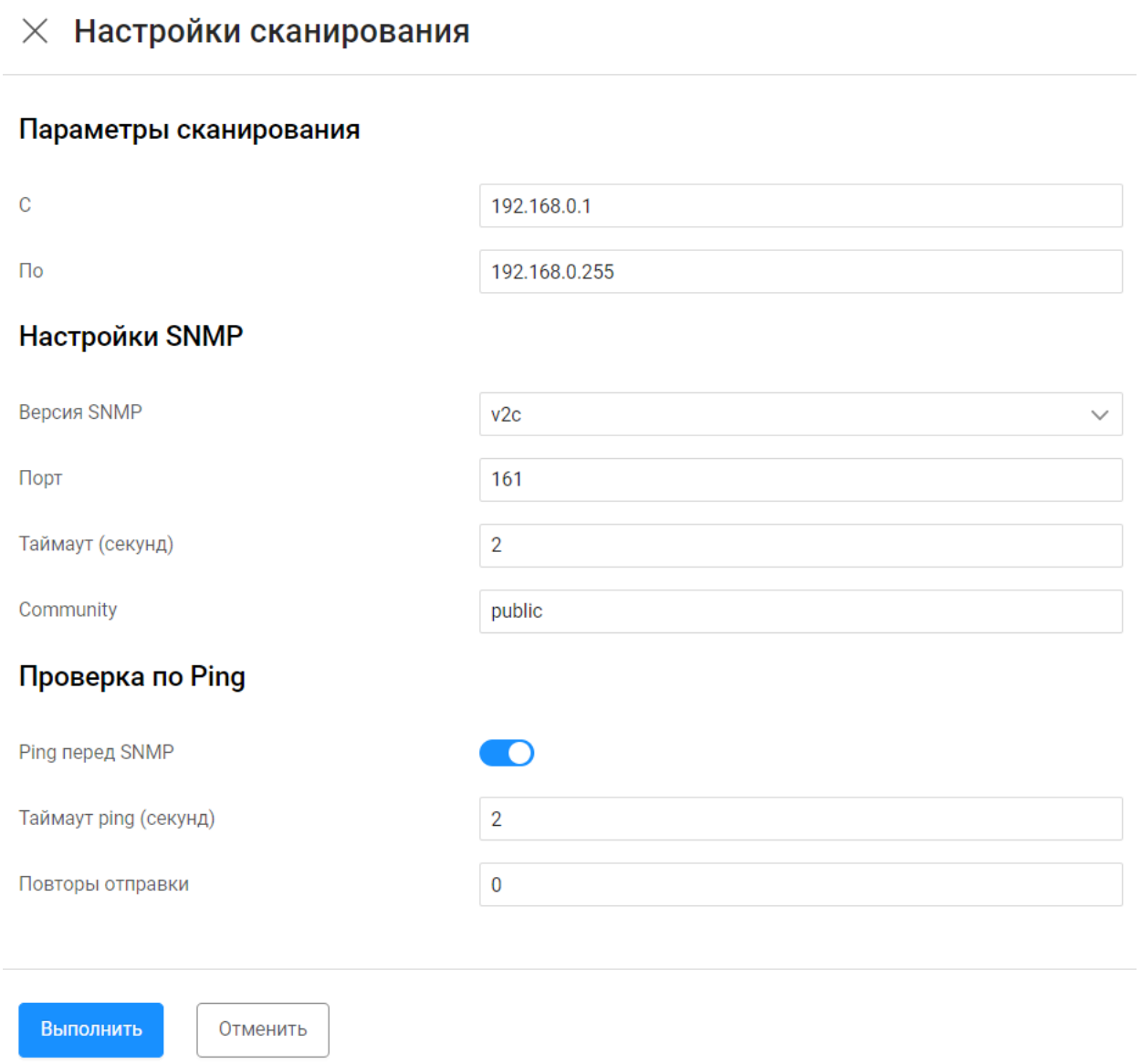


Рисунок 56 – Окно «Настройки сканирования»

Таблица 18 – 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

Поле	Описание
(секунд)»	перед сканированием следующего IP-адреса (в секундах)
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 пользователя»	Имя (логин) учетной записи пользователя, которая будет использоваться для авторизации на контролируемом устройстве по протоколу SNMPv.3. Поле обязательно к заполнению при использовании SNMPv.3
Поле «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 (в секндах)
Поле «Повторы отправки»	Количество повторных попыток отправки ping-запроса к каждому из адресов диапазона
Элементы управления	
Выполнить	При нажатии кнопки выполняется сканирование сети

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

3) Начнется процесс сканирования сети по указанным параметрам. Результат сканирования сети приведен на рис. 57. Состав и описание полей страницы приведены в таблице 19.

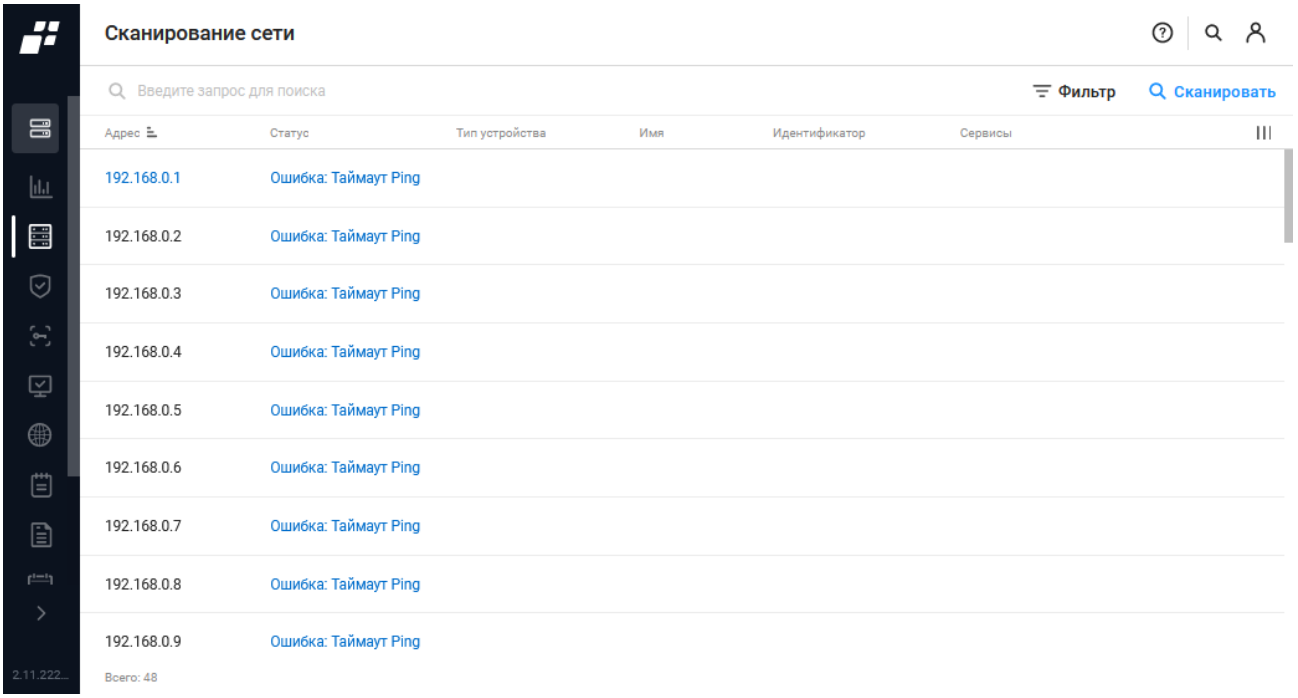


Рисунок 57 – Страница с результатом сканирования сети

Таблица 19 – 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 открывается окно с описанием устройства (рис. 58). Изменение параметров ОЗ описано в п. 5.1.1.6.

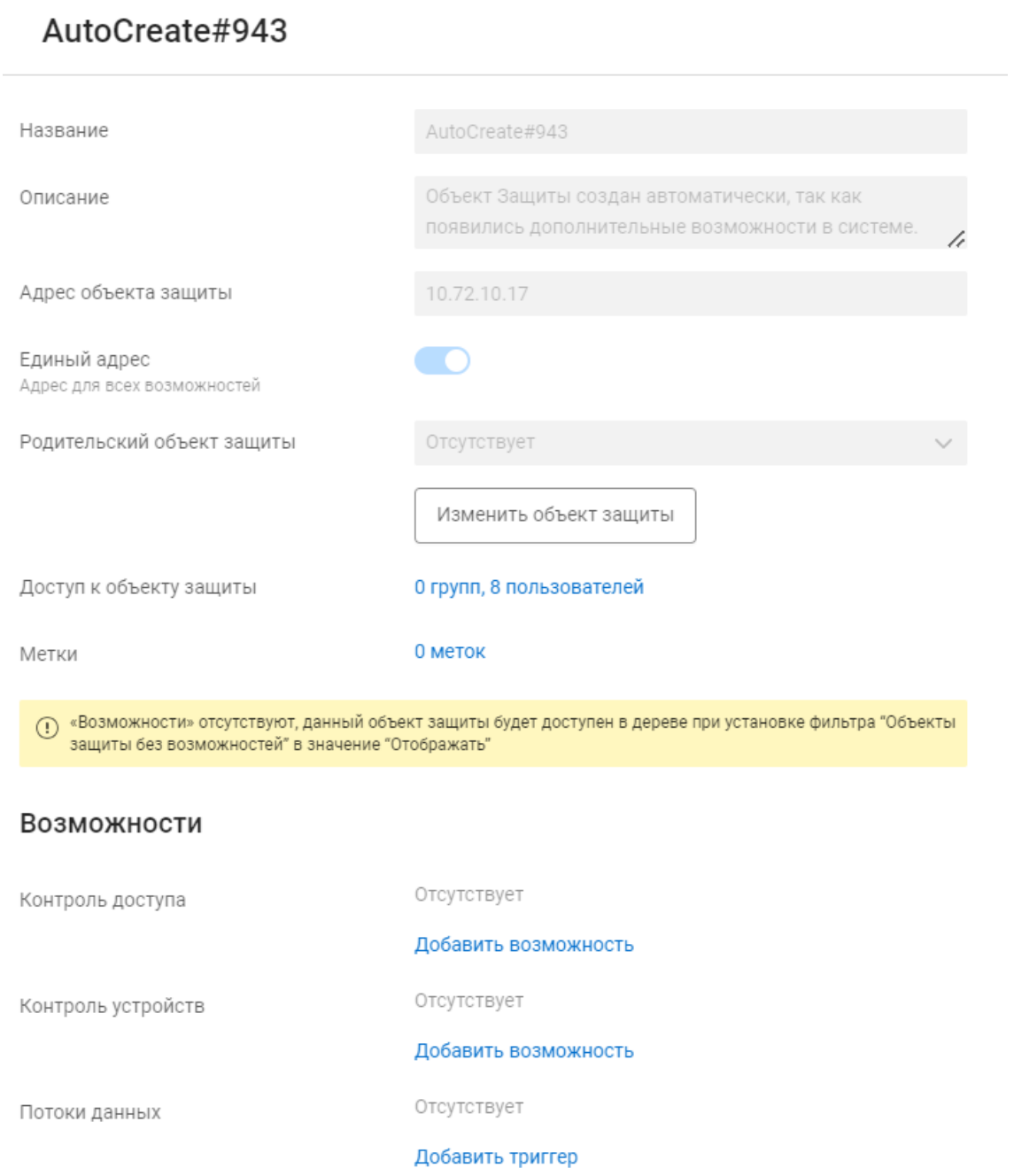


Рисунок 58 – Окно просмотра информации об ОЗ

6 Раздел «Защита DNS»

Раздел «Защита DNS» доступен пользователю для работы при наличии лицензии на функциональный модуль «Efros DNS».

Раздел «Защита DNS» предназначен для блокировки доступа к нежелательным сайтам, а также для обнаружения и предотвращения атак на DNS-трафик.

Модули (компоненты), применяемые для защиты DNS:

- сервер DNS;
- модуль проверки по черному и белому спискам:
  - проверка доменов;
  - проверка IP-адресов клиентов.
- IPS/IDS – проверка DNS-трафика на соответствие правилам IDS/IPS. Действия при срабатывании правил настраиваются индивидуально для каждого правила в подразделе «Правила IDS/IPS»;
- анализ DGA – проверка на аномальные или подозрительные домены, созданные с использованием алгоритма генерации доменных имен;
- изменение регистра DNS-запроса – алгоритм обработки DNS-запроса, который случайным образом изменяет регистр символов в доменных именах;
- модуль обработки DNS-запроса.

Последовательность действий для настройки параметров защиты DNS:

1) В подразделе «Защита DNS-трафика» выбрать необходимые модули проверок (см. подраздел 6.3).
2) В подразделе «Черный и белый списки» ввести пользовательские записи доменов и IP-адресов клиентов, которые считаются доверенными либо требующие блокировки (см. подраздел 6.1).
3) В подразделе «Правила IDS/IPS» настроить и активировать требуемые правила. Расположить правила в необходимой последовательности (см. подраздел 6.2).
4) В подразделе «Серверы пересылки» настроить параметры условной и безусловной пересылок (см. подраздел 6.4).

6.1 Черный и белый списки

Подраздел «Черный и белый списки» (рис. 59) позволяет управлять соответствующими списками доменов и IP-адресов для обеспечения безопасности DNS-трафика.

При соответствии данных DNS-запроса записи в белом списке – запрос считается доверенным и исключается из дальнейших проверок другими модулями защиты DNS, пользователю формируется и возвращается DNS-ответ.

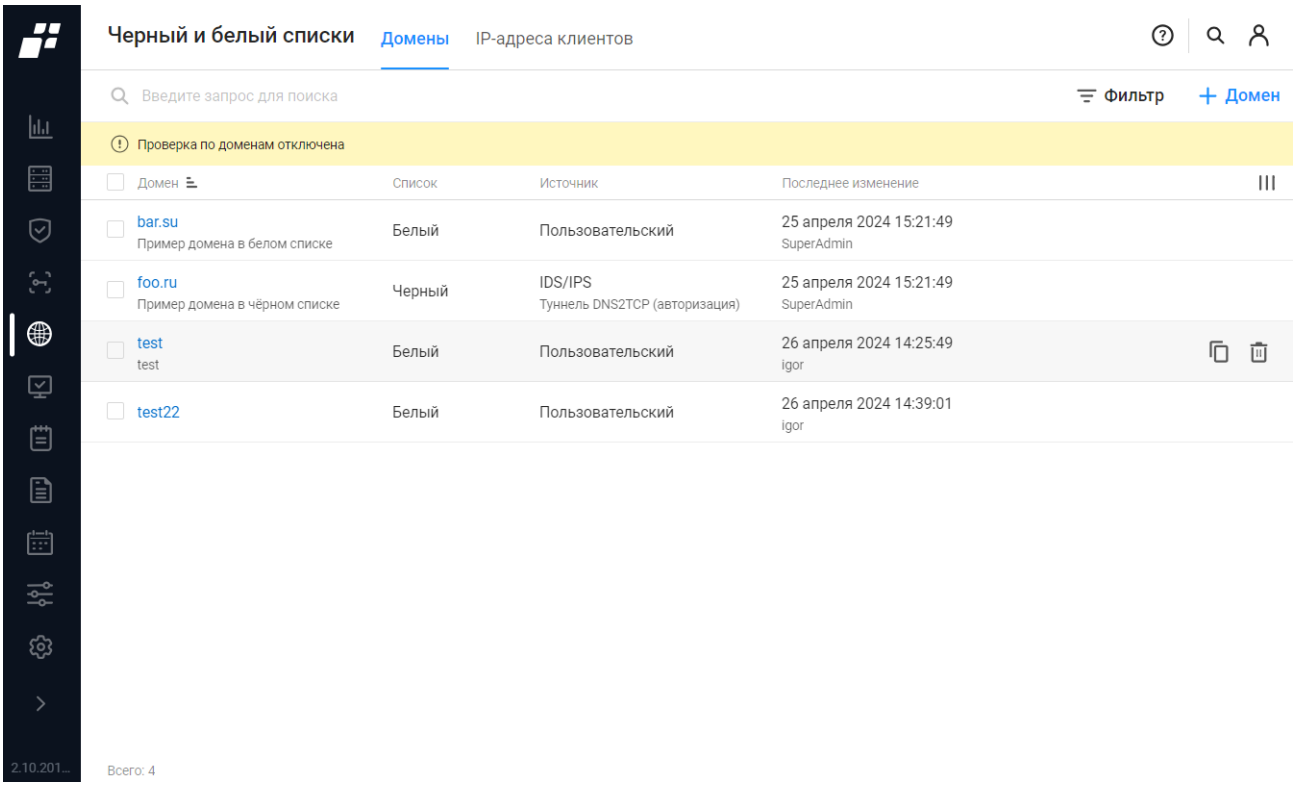


Рисунок 59 – Подраздел «Черный и белый списки»

При соответствии данных DNS-запроса записи в черном списке – запрос блокируется, дальнейшая проверка другими модулями не производится.

Страница «Черный и белый списки» состоит из вкладок:

— «Домены»;
— «IP-адреса клиентов».

6.1.1 Вкладка «Домены»

На вкладке «Домены» доступен просмотр записей доменов, добавленных в черный и белый списки, и доступна возможность добавления новой пользовательской записи.

Список доменов реализован в виде таблицы (см. рис. 59). Для каждой записи списка отображаются данные:

— поле для флага – для выбора записей для выполнения операции группового удаления записей;
— домен – является ссылкой, при переходе по которой открывается страница редактирования записи домена;
— тип списка (черный/белый);
— источник проверки DNS-трафика по списку разрешенных и запрещенных доменов:
  - «Пользовательский»;
  - модули, настраиваемые в подразделе «Защита DNS-трафика»:
    - «IDS/IPS»;
    - «DGA»;

- «Изменение регистра DNS-запроса».

— последнее изменение – дата внесения последних изменений и данные вносившего последние изменения (имя пользователя ПК «Efros DO» или «System»).

Над списком располагаются:

— поле поиска (Введите запрос для поиска);

— кнопка «Фильтр» (Фильтр);

— кнопка «Домен» (+ Домен);

— кнопка «Колонки» ( ).

При установке флага в строке с доменом над списком появляются кнопки:

— «Создать копию» ( );

— «Удалить» ( ).

Аналогичные кнопки появляются в правой части экрана в строке списка.

На рис. 59 над таблицей доменов отображается информационное сообщение «Проверка по доменам отключена». Для включения проверки необходимо в подразделе «Защита DNS-трафика» включить проверку по доменам (см. подраздел 6.3).

6.1.1.1 Добавление домена

Для добавления домена пользователю ПК «Efros DO» необходимо:

1) Нажать кнопку «Домен» (+ Домен).
2) Откроется страница «Добавление домена» (рис. 60). Необходимо заполнить поля требуемыми параметрами и нажать кнопку «Создать». Состав и описание полей страницы приведены в таблице 20.

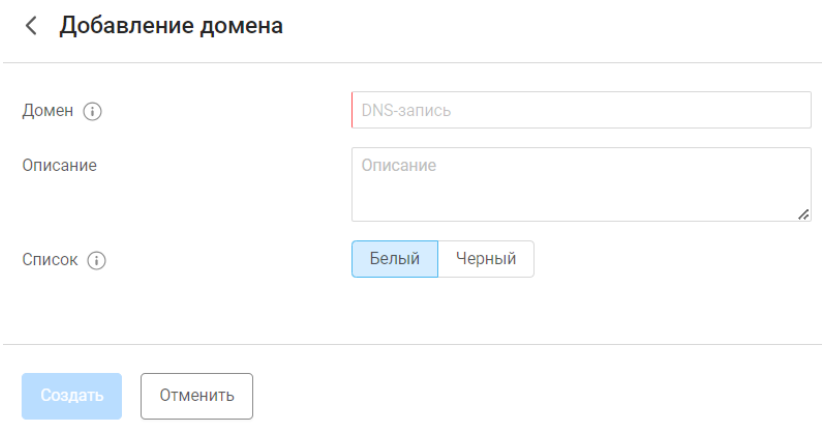


Рисунок 60 – Страница «Добавление домена»

Таблица 20 – Состав и описание полей страницы «Добавление домена»

Поле	Описание
Поле «Домен»	Текстовое поле для ввода DNS-записи. Допустимо указывать домен любого уровня. Параметры ввода текста: — всего символов: от 2 до 254; — уровней: от 1 до 127; — символов на уровне: от 1 до 63; — формат: Unicode. Уровень – блок текста, разделенный точкой. Например, в домене «edo.ru» два уровня. При проверке по черным и белым спискам учитываются не только явно заданные домены, но и все поддомены, выбор происходит по наиболее точному совпадению уровня домена. Пример ввода доменов: — «edo.ru» – запись в черном списке; — «ru» – запись в белом списке. Результат применения черного и белого списков: — «test.edo.ru» – считается записью черного списка; — «example.ru» – считается записью белого списка
Поле «Описание»	Текстовое поле для ввода описания домена. Параметры ввода текста: от 1 до 250 любых символов
Переключатель «Список»	Переключатель: — «Белый» – домен, доступ к которому будет разрешен; — «Черный» – домен, доступ к которому будет запрещен При попадании домена в белый или черный списки, запрос к такому домену исключается из дальнейших проверок
Элементы управления	
Создать	При нажатии кнопки выполняется переход на страницу списка доменов с сохранением внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу списка без сохранения внесенных данных

6.1.2 Вкладка «IP-адреса клиентов»

На вкладке «IP-адреса клиентов» доступен просмотр записей IP-адресов, добавленных в черный и белый списки, и доступна возможность добавления новой пользовательской записи.

Список IP-адресов реализован в виде таблицы (рис. 61).

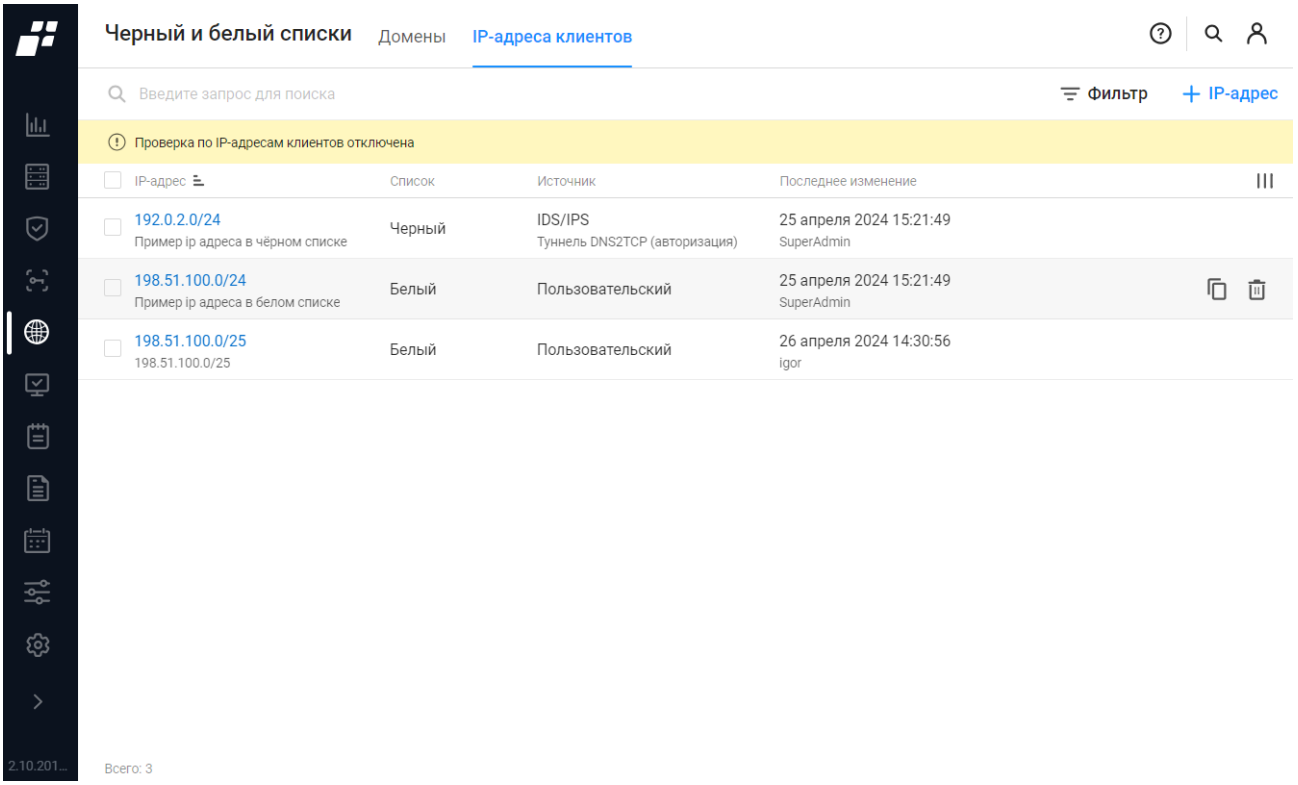


Рисунок 61 – Вкладка «IP-адреса клиентов»

Для каждой записи списка отображаются:

- поле для флага – для выбора записей для выполнения операции группового удаления записей;
- IP-адрес – является ссылкой, при переходе по которой открывается страница редактирования записи;
- тип списка (черный/белый);
- источник проверки DNS-трафика по списку разрешенных и запрещенных IP-адресов:
  - «Пользовательский»;
  - модули, настраиваемые в подразделе «Защита DNS-трафика»:
    - «IDS/IPS»;
    - «DGA»;
    - «Изменение регистра DNS-запроса».
- последнее изменение – дата внесения последних изменений и данные вносившего последние изменения (имя пользователя ПК «Efros DO» или «System»).

Над списком располагаются:

— поле поиска (Введите запрос для поиска);

— кнопка «Фильтр» (Фильтр);

— кнопка «IP-адрес» (+ IP-адрес);

— кнопка «Колонки» ( ).

При установке флага в строке с IP-адресом над списком появляются кнопки:

— «Создать копию» ( );

— «Удалить» ( ).

Аналогичные кнопки появляются в правой части экрана в строке списка.

На рис. 61 над таблицей IP-адресов клиентов отображается информационное сообщение «Проверка по IP-адресам клиентов отключена». Для включения проверки необходимо в подразделе «Защита DNS-трафика» включить проверку по IP-адресам клиентов (см. подраздел 6.3).

6.1.2.1 Добавление IP-адреса

Для добавления IP-адреса клиента пользователю ПК «Efros DO» необходимо:

1) Нажать кнопку «IP-адрес» (+ IP-адрес).
2) Откроется страница «Добавление IP-адреса» (рис. 62). Необходимо заполнить поля требуемыми параметрами и нажать кнопку «Создать». Состав и описание полей страницы приведены в таблице 21.

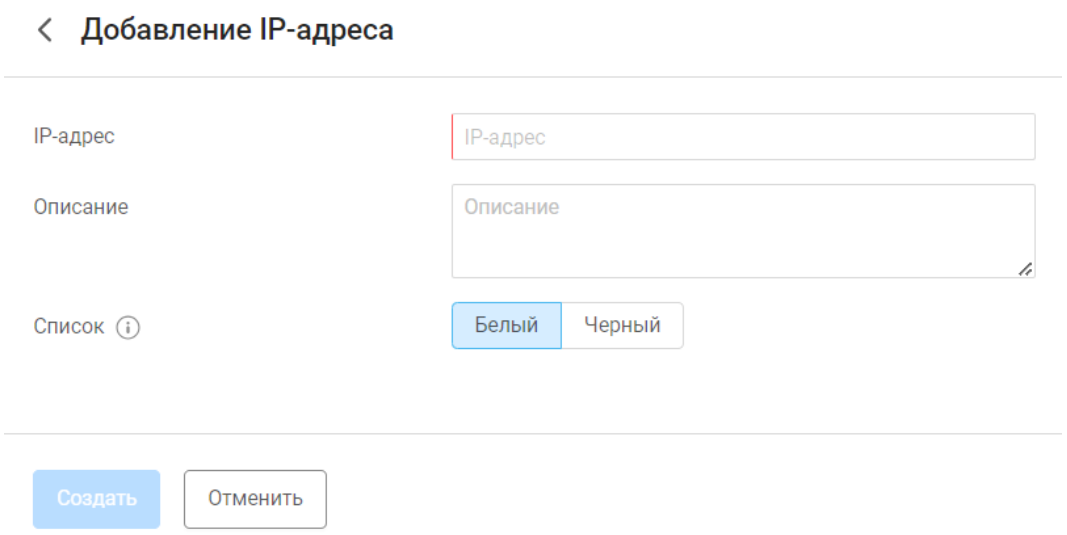


Рисунок 62 – Страница «Добавление IP-адреса»

Таблица 21 – Состав и описание полей страницы «Добавление IP-адреса»

Поле	Описание
Поле «IP-адрес»	Текстовое поле для ввода IP-адреса клиента. Параметры ввода текста: формат от 0.0.0.0 до 255.255.255.255/32 кроме 0.0.0.0 и 255.255.255.255
Поле «Описание»	Текстовое поле для ввода описания IP-адреса клиента. Параметры ввода текста: от 1 до 250 любых символов
Переключатель «Список»	Переключатель: — «Белый» – домен, доступ к которому будет разрешен; — «Черный» – домен, доступ к которому будет запрещен При попадании домена в белый или черный списки, запрос к такому домену исключается из дальнейших проверок
Элементы управления	
Создать	При нажатии кнопки выполняется переход на страницу списка IP-адресов с сохранением внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу списка без сохранения внесенных данных

6.2 Правила IDS/IPS

Подраздел «Правила IDS/IPS» позволяет управлять правилами систем обнаружения вторжений и систем предотвращения вторжений.

На странице список правил реализован в виде таблицы (рис. 63). Список правил IDS/IPS:

— «Base32/Base64 (вариант № 1)» – возможное кодирование в Base32/Base64;
— «Base32/Base64 (вариант № 2)» – возможное кодирование в Base32/Base64;
— «Base32/Base64 (вариант № 3)» – возможное кодирование в Base32/Base64;
— «Base32/Base64 (вариант № 4)» – возможное кодирование в Base32/Base64;
— «Превышен лимит TXT-запросов» – превышен лимит количества TXT-запросов;
— «Превышение размера TXT» – превышен размер пакета с типом TXT;
— «Вредоносный TXT-ответ» – вредоносный паттерн в TXT-ответе;
— «Превышение размера CNAME» – превышен размер пакета с типом CNAME;
— «Превышение размера MX» – превышен размер пакета с типом MX;
— «Тип запроса NULL» – запрос с типом NULL;
— «Туннель DNS2TCP (авторизация)» – наличие паттернов туннеля DNS2TCP;
— «Туннель DNS2TCP (установка соединения)» – наличие паттернов туннеля DNS2TCP;

— «Туннель DNS2TCP (передача данных)» – наличие паттернов туннеля DNS2TCP;
— «Туннель Ozyman (установка туннеля)» – наличие паттернов туннеля Ozyman;
— «Туннель Ozyman (закрытие туннеля)» – наличие паттернов туннеля Ozyman;
— «Туннель NSTX (установка соединения)» – наличие паттернов туннеля NSTX;
— «Туннель Heyoka (вариант №1)» – наличие паттернов туннеля Heyoka;
— «Туннель Heyoka (вариант №2)» – наличие паттернов туннеля Heyoka;
— «Туннель Cobalt Strike Beacon» – наличие паттернов туннеля Cobalt Strike Beacon;
— «Атака методом DNS Rebinding» – атака методом DNS Rebinding.

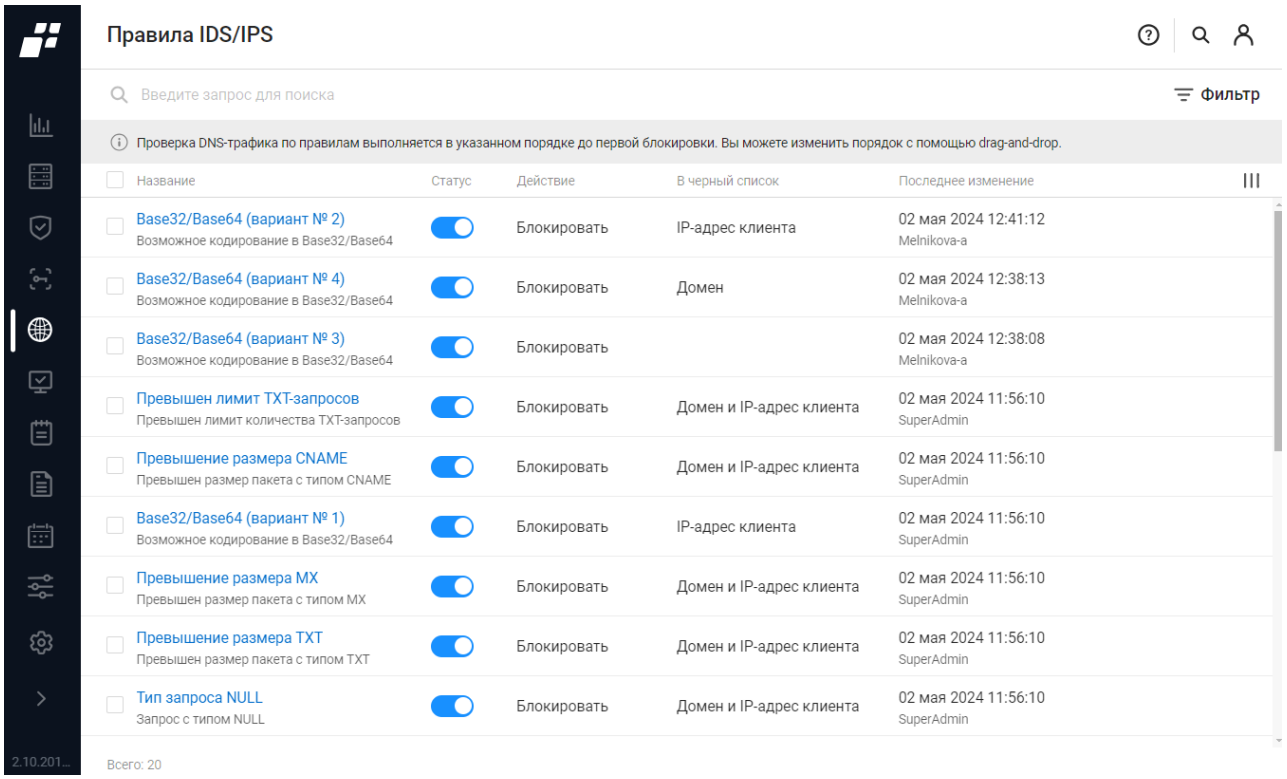


Рисунок 63 – Подраздел «Правила IDS/IPS»

Проверка DNS-трафика по правилам IDS/IPS осуществляется в указанном порядке до первого события срабатывания правила, где действие соответствует значению «Блокировать».

В случае, если в сработавшем правиле IDS/IPS выбрано действие «Логировать», то продолжается дальнейшая обработка правил.

Изменить порядок правил IDS/IPS можно с помощью перемещения. При наведении курсора на строку с названием правила слева от поля для флага отображается символ «⠿». Перетаскиванием символа выбирается требуемое положение в списке.

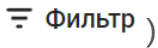
Для каждой записи списка отображаются следующие данные:

— поле для флага – для выбора записей для выполнения операций групповой настройки записей (выбор статуса, действия и необходимости добавления в черный список домена и/или IP-адреса);

— название и описание правил;
— статус (включен/отключен);
— действия (блокировать/логировать);
— добавить в черный список домен и (или) IP-адрес клиента;
— последнее изменение – дата внесения последних изменений и имя пользователя ПК «Efros DO».

Над списком располагаются:

— поле поиска (

 );
— кнопка «Фильтр» (

 );
— кнопка «Колонки» ().

При установке флага в строке с необходимым правилом над списком появляются следующие кнопки:

— кнопка изменения статуса:
  - «Включен»;
  - «Отключен».

— кнопка изменения действия:
  - «Блокировать»;
  - «Логировать».

— кнопка изменения добавления в черный список:
  - «Домен»;
  - «IP-адрес клиента»;
  - «Домен и IP-адрес клиента»;
  - «Не добавлять».

6.2.1 Редактирование правила IDS/IPS

Для редактирования правила IDS/IPS необходимо:

1) На странице подраздела «Правила IDS/IPS» выбрать наименование необходимого правила (см. рис. 63).
2) Откроется страница редактирования выбранного правила IDS/IPS (рис. 64). Необходимо внести в параметры требуемые изменения и нажать кнопку «Сохранить». Состав и описание полей страницы приведены в таблице 22.

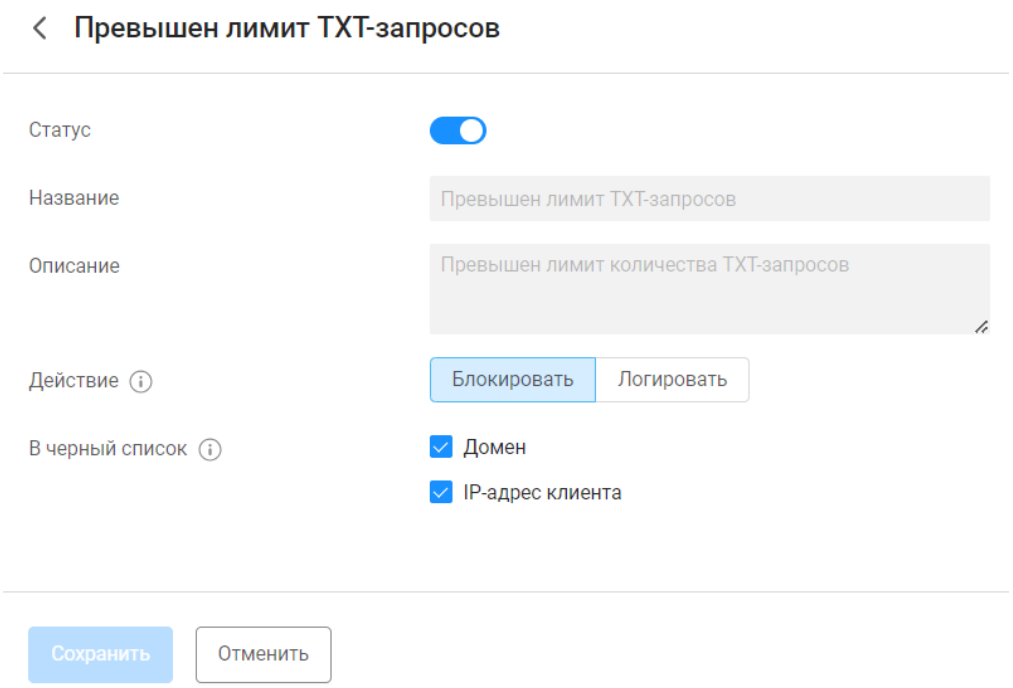


Рисунок 64 – Страница редактирования правила IDS/IPS

Таблица 22 – Состав и описание полей страницы редактирования правила IDS/IPS

Поле	Описание
Поле «Статус»	Переключатель: — «Включен»; — «Отключен»
Поле «Название»	Поле названия правила IDS/IPS. Недоступно для редактирования
Поле «Описание»	Поле описания правила IDS/IPS. Недоступно для редактирования
Поле «Действие»	Переключатель действия при срабатывании правила: — «Блокировать» – заблокировать DNS-трафик и прекратить дальнейшую его обработку; — «Логировать» – продолжить обработку DNS-трафика, в том числе по нижеследующим правилам. В обоих случаях запись о срабатывании сохраняется в журнале событий
Поле «В черный список»	Поле для выбора добавления в черный список: — «Домен» – добавить запрашиваемый домен в черный список; — «IP-адрес клиента» – добавить IP-адрес источника в черный список.

Поле	Описание
	При отсутствии записи в обоих списках – осуществляется дальнейшая проверка DNS-запроса. «Домен» или «IP-адрес клиента» добавляется в черный список в подразделе «Защита DNS» → «Черный и белый списки»
Элементы управления	
Сохранить	При нажатии кнопки выполняется переход на страницу списка правил с сохранением внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу списка без сохранения внесенных данных

6.3 Защита DNS-трафика

Подраздел «Защита DNS-трафика» (рис. 65) позволяет управлять настройками модулей защиты DNS, используемых при обработке DNS-трафика. Состав и описание полей страницы приведены в таблице 23.

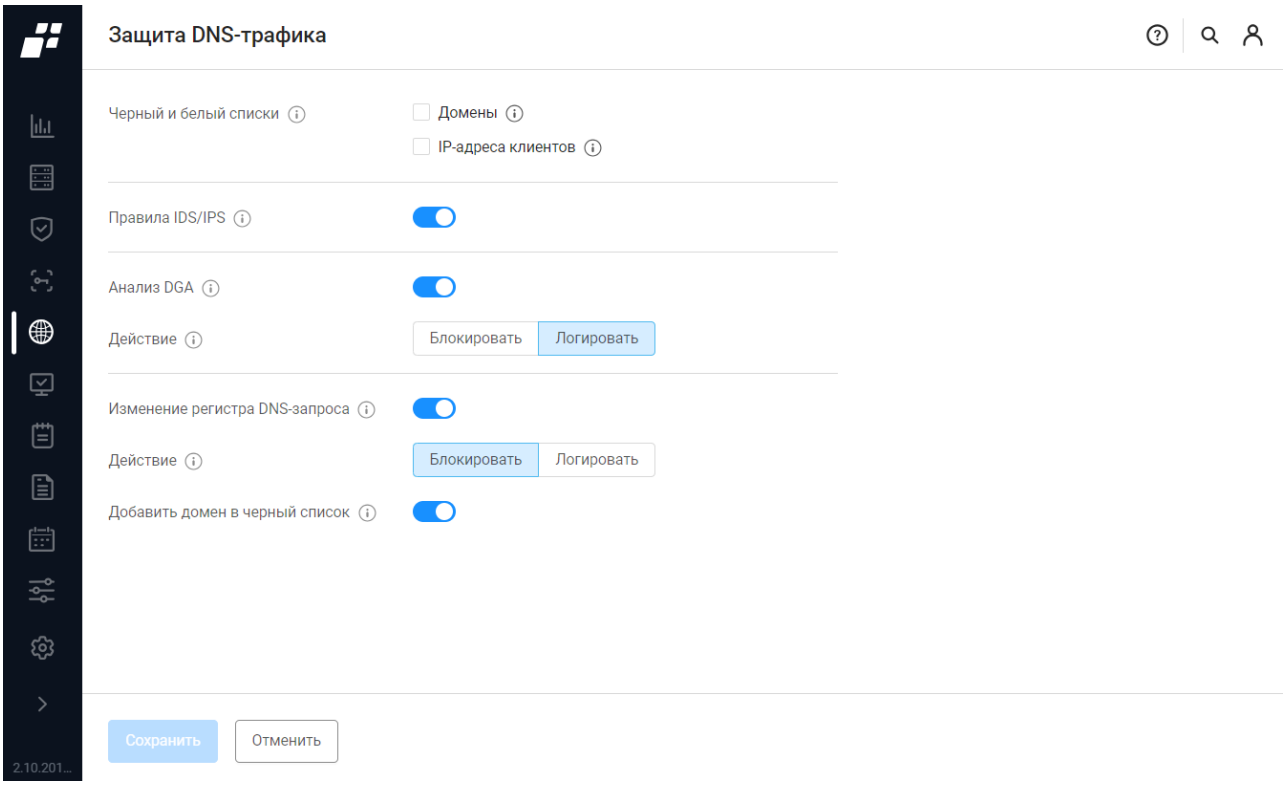


Рисунок 65 – Подраздел «Защита DNS-трафика»

Таблица 23 – Состав и описание полей подраздела «Защита DNS-трафика»

Поле	Описание
Поле «Черный и	Поле для выбора проверки по черным и белым спискам:

Поле	Описание
белый списки»	— «Домены» – проверка по списку доменов, доступ к которым явно разрешен или запрещен; — «IP-адрес клиентов» – проверка по списку IP-адресов клиентов, доступ к которым явно разрешен или запрещен. При отсутствии записи в обоих списках – осуществляется дальнейшая проверка DNS-запроса
Поле «Правила IDS/IPS»	Переключатель: — «Включен» ( ) – включение проверки DNS-трафика на соответствие правилам IDS/IPS; — «Отключен» ( ). Действия при срабатывании правил настраиваются индивидуально для каждого правила в подразделе «Защита DNS» → «Правила IDS/IPS» (см. п. 6.2)
Поле «Анализ DGA»	Переключатель: — «Включен» ( ) – включение проверки на аномальные или подозрительные домены, созданные с использованием алгоритма генерации доменных имен; — «Отключен» ( ). При включении появляется дополнительное поле «Действие»
Поле «Действие»	Переключатель действия при обнаружении подозрительного домена: — «Блокировать» – запретить обработку DNS-запроса; — «Логировать» – продолжить обработку DNS-запроса. В обоих случаях запись о срабатывании сохраняется в журнале событий. При выборе положения «Блокировать» доступен дополнительно переключатель «Добавить домен в черный список» (описание см. ниже)
Поле «Добавить домен в черный список»	Переключатель: — «Включен» ( ) – включение добавления подозрительного домена в черный список для быстрой блокировки последующих запросов; — «Отключен» ( ).

Поле	Описание
Поле «Изменение регистра DNS-запроса»	Переключатель: — «Включен» ( ) – включение алгоритма обработки DNS-запроса, который случайным образом изменяет регистр символов в доменных именах; — «Отключен» ( ).
Поле «Действие»	Переключатель действия при обнаружении подозрительного домена: — «Блокировать» – запретить обработку DNS-запроса; — «Логировать» – продолжить обработку DNS-запроса. В обоих случаях запись о срабатывании сохраняется в журнале событий При выборе положения «Блокировать» доступен дополнительно переключатель «Добавить домен в черный список» (описание см. выше)
Элементы управления	
Сохранить	При нажатии кнопки выполняется сохранение внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу без сохранения внесенных данных

6.4 Серверы пересылки

Подраздел «Серверы пересылки» (рис. 66) позволяет управлять настройками DNS-сервера в части переадресации DNS-запросов. Серверы пересылки можно использовать для перенаправления DNS-запросов на сторонние DNS-серверы для разрешения запрашиваемых доменных имен.

Виды пересылок:

— «Условная пересылка» – позволяет настроить DNS-сервер для перенаправления DNS-запросов к другим DNS-серверам на основе заданных условий. В качестве условия задается домен (любого уровня), для которого необходимо выполнить разрешение доменного имени;

— «Безусловная пересылка» – позволяет настроить DNS-сервер для перенаправления всех DNS-запросов на указанные сторонние DNS-серверы без каких-либо дополнительных условий.

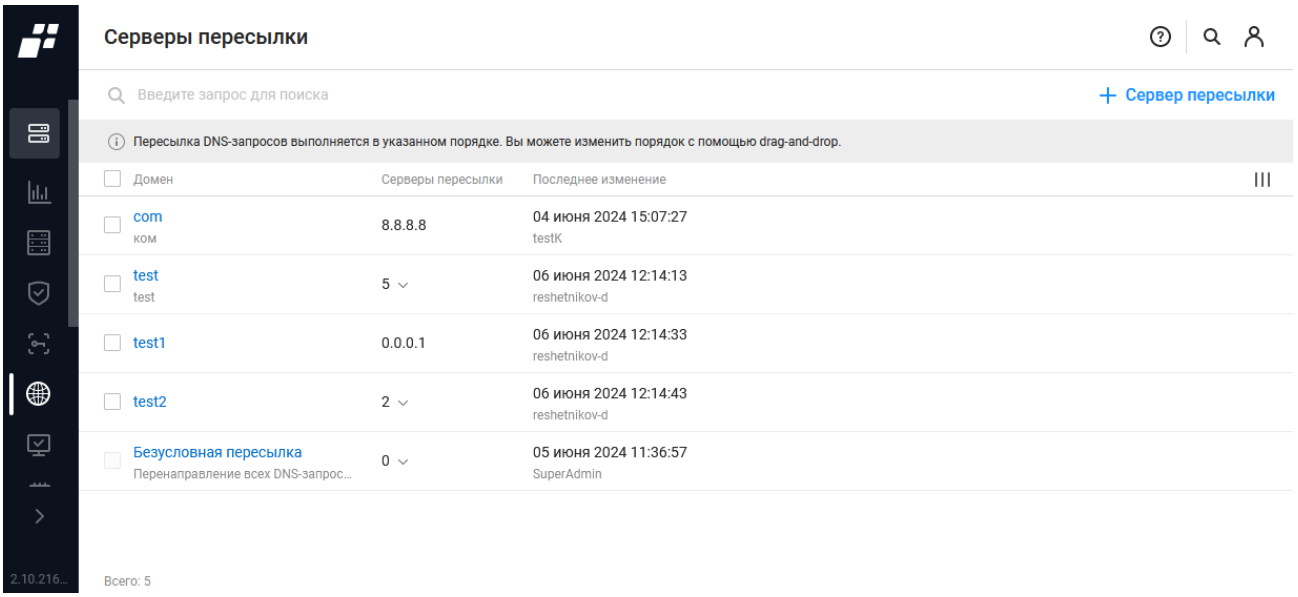


Рисунок 66 – Подраздел «Серверы пересылки»

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

- поле для флага – для выбора записей для выполнения операции группового удаления записей;
- домен – является ссылкой, при переходе по которой открывается страница редактирования параметров сервера пересылки;
- сервер пересылки – IP-адрес сервера пересылок или их количество, если их несколько;
- последнее изменение – дата внесения последних изменений и имя пользователя ПК «Efros DO», вносившего последние изменения.

Над списком располагаются:

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

При установке флага в строке с сервером пересылки над списком появляются кнопки:

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

Аналогичные кнопки появляются в правой части экрана в строке списка.

Запись «Безусловная пересылка» является предустановленной и недоступна для копирования и удаления.

6.4.1 Редактирование сервера безусловной пересылки

Запись сервера «Безусловная пересылка» располагается в конце списка. Для ее редактирования пользователю ПК «Efros DO» необходимо:

1) Нажать на предустановленную запись «Безусловная пересылка».
2) Откроется страница записи «Безусловная пересылка» (рис. 67). Заполнить поля требуемыми параметрами и нажать кнопку «Сохранить». Состав и описание полей страницы приведены в таблице 24.

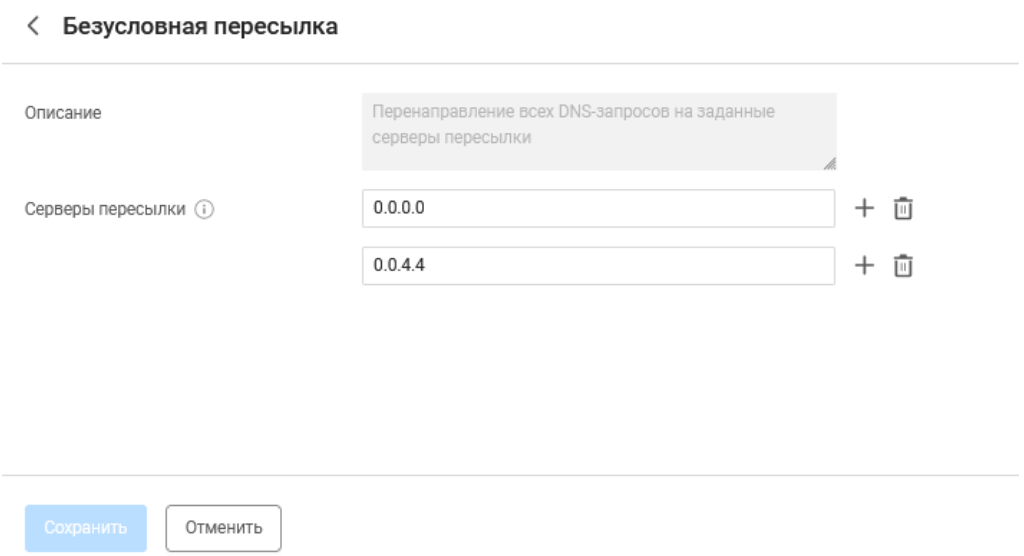


Рисунок 67 – Страница записи «Безусловная пересылка»

Таблица 24 – Состав и описание полей страницы записи «Безусловная пересылка»

Поле	Описание
Поле «Описание»	Текстовое поле описания домена. Недоступно для редактирования
Поле «Серверы пересылок»	Поле для ввода IP-адреса и номера порта сервера DNS, на который будет перенаправлен DNS-запрос, в формате <IP-адрес>:<порт>. Если порт не задан, по умолчанию будет использован 53 порт. При необходимости добавления нескольких IP-адресов нужно нажать на «+», при необходимости удалить – нажать на « »
Элементы управления	
Сохранить	При нажатии кнопки выполняется переход на страницу списка серверов пересылки с сохранением внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу списка без сохранения внесенных данных

6.4.2 Добавление сервера пересылки

Для добавления сервера пересылки пользователю ПК «Efros DO» необходимо:

1) Нажать кнопку «Сервер пересылки» (+ Сервер пересылки).
2) Откроется страница «Добавление сервера пересылки» (рис. 68). Заполнить поля требуемыми параметрами и нажать кнопку «Создать». Состав и описание полей страницы приведены в таблице 25.

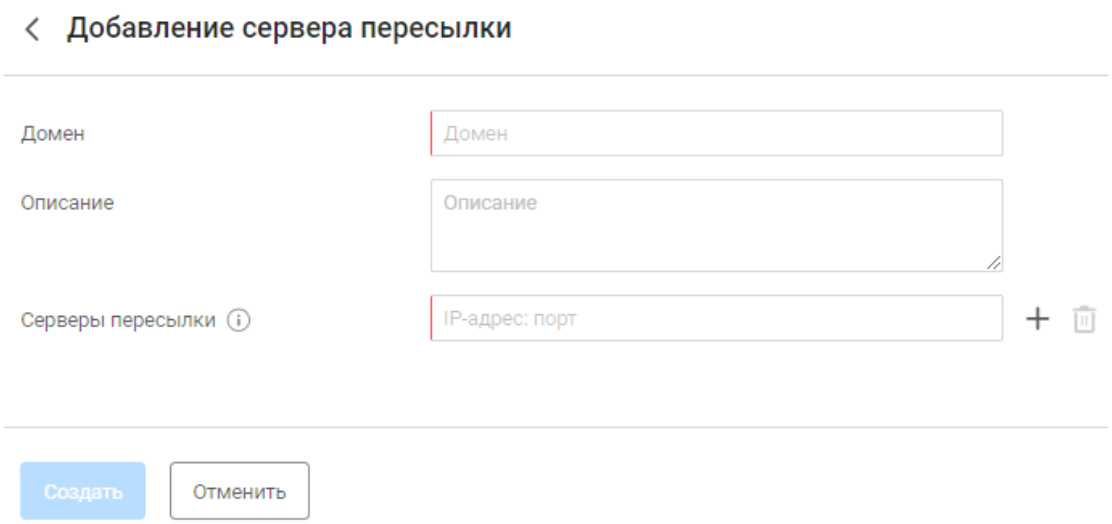


Рисунок 68 – Страница «Добавление сервера пересылки»

Таблица 25 – Состав и описание полей страницы «Добавление сервера пересылки»

Поле	Описание
Поле «Домен»	Текстовое поле для указания домена, DNS-запросы к которому будут перенаправлены на заданные серверы пересылки. Допустимо вводить домен любого уровня. Параметры ввода текста: — всего символов: от 2 до 254; — уровней: от 1 до 127; — символов на уровне: от 1 до 63; — формат: Unicode
Поле «Описание»	Текстовое поле для ввода описания. Параметры ввода текста: от 1 до 250 любых символов
Поле «Серверы пересылок»	Поле для ввода IP-адреса и номера порта сервера DNS, на который будет перенаправлен DNS-запрос, в формате <IP-адрес>:<порт>. Если порт не задан, по умолчанию будет использован 53 порт.

Поле	Описание
	При необходимости добавления нескольких IP-адресов нужно нажать на «+», при необходимости удалить – нажать на « »
Элементы управления	
Создать	При нажатии кнопки выполняется переход на страницу списка серверов пересылки с сохранением внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу списка без сохранения внесенных данных

7 Раздел «Центр задач»

Раздел «Центр задач» (рис. 69) позволяет пользователю выполнять следующие действия:

- создавать заявки на выполнение определенных действий в комплексе;
- автоматически контролировать статусы выполнения заявок;
- контролировать процесс выполнения заявок;
- назначать сроки исполнения заявки;
- выбирать маршруты движения заявок;
- получать необходимую информацию по ходу движения заявки на каждой стадии маршрута;
- назначать исполнителя заявки;
- назначать согласующих и утверждающих лиц в заявке.

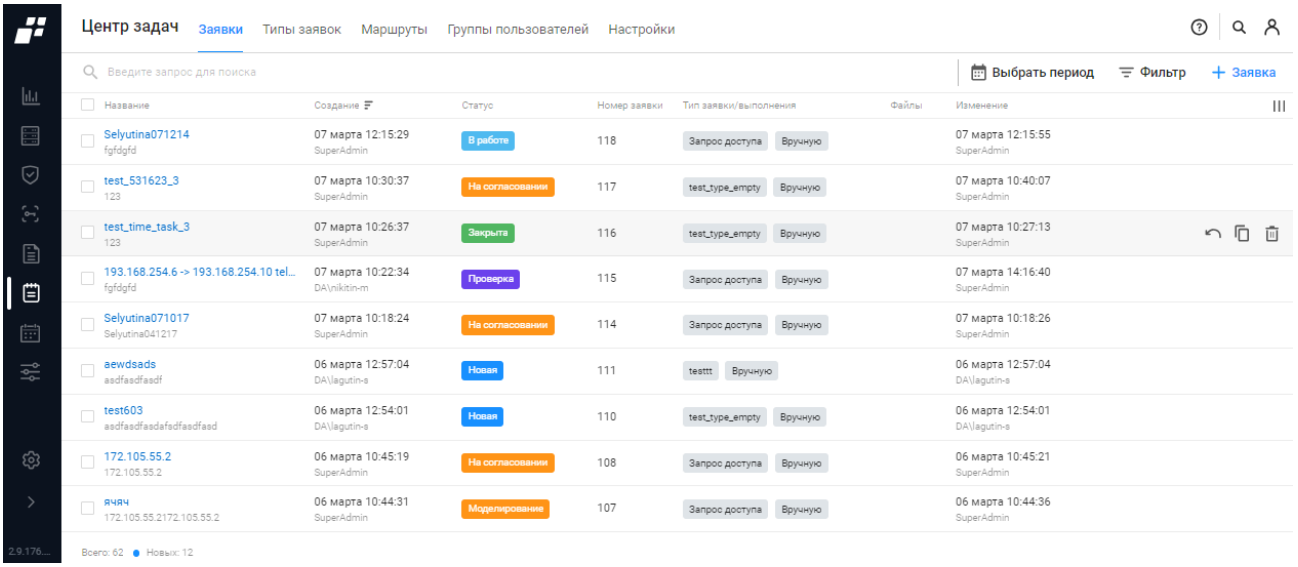


Рисунок 69 – Раздел «Центр задач»

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[6] и заявки пользователя-участника[7] в маршруте.

Список заявок реализован в виде таблицы (см. рис. 69). Для каждой записи списка отображаются:

- поле для флага – для выбора записи для выполнения с ней операции «Создать копию» или «Удалить»;
- название заявки. Является ссылкой, при переходе по которой открывается страница управления заявкой;
- дата создания заявки и логин пользователя, создавшего заявку;
- статус заявки. Статус заявки подсвечен определенным цветом:
  - «Новая» (Новая);
  - «В работе» (В работе);
  - «Проверка» (Проверка);
  - «Закрыта» (Закрыта);
  - «На согласовании» (На согласовании);
  - «На утверждении» (На утверждении);
  - «Моделирование» (Моделирование);
  - «На корректировке» (На корректировке);
  - «Не согласована» (Не согласована);
  - «Не утверждена» (Не утверждена);
  - «Срок истек» (Срок истек);
  - «Ошибка моделирования» (Ошибка моделирования).
- номер заявки (присваивается автоматически при создании заявки);
- тип заявки и способ выполнения заявки;
- файлы, прикрепленные к заявке, в виде раскрывающегося списка с возможностью скачивания;
- дата последнего изменения заявки и логин пользователя, внесшего изменение.

[6] Пользователь, создавший заявку
[7] Пользователь, принимающий участие в исполнении заявки (например, согласовывает заявку)

Над списком заявок располагаются:

— поле поиска (Введите запрос для поиска);
— кнопка «Выбрать период» (Выбрать период);
— кнопка «Фильтр» (Фильтр);
— кнопка «Заявка» (+ Заявка);
— кнопка «Колонки» ( ).

При выборе строки с необходимой заявкой в ее строке появляются кнопки:

— «Удалить» ( ) для заявки со статусом «Новая» или «Закрыта» доступна только при наличии возможности удаления;
— «Создать копию» ( );
— «Отмена изменений» ( ) для заявки со статусом «Закрыта» доступна только при наличии возможности отмены изменений.

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 создания заявки с типом «Запрос доступа» необходимо убедиться, что в карточке нужного устройства активирован тип контроля «CHANGE MANAGER».

Существуют следующие заявки:

— стандартная пользовательская заявка. В поле «Тип заявки» указывается пользовательский тип, который создается на вкладке «Тип заявки». Более подробно о работе с такой заявкой написано в п. 7.1.2;
— заявка с типом заявки «Запрос доступа». Более подробно о работе с такой заявкой написано в п. 7.1.3.

Для добавления в список новой заявки пользователю необходимо:

1) Нажать на вкладке «Заявки» (см. рис. 69) кнопку «Заявка» (+ Заявка).
2) Откроется страница создания новой заявки (рис. 70). Заполнить поля страницы требуемыми параметрами и нажать кнопку «Создать». Состав и описание полей страницы приведены в таблице 26.

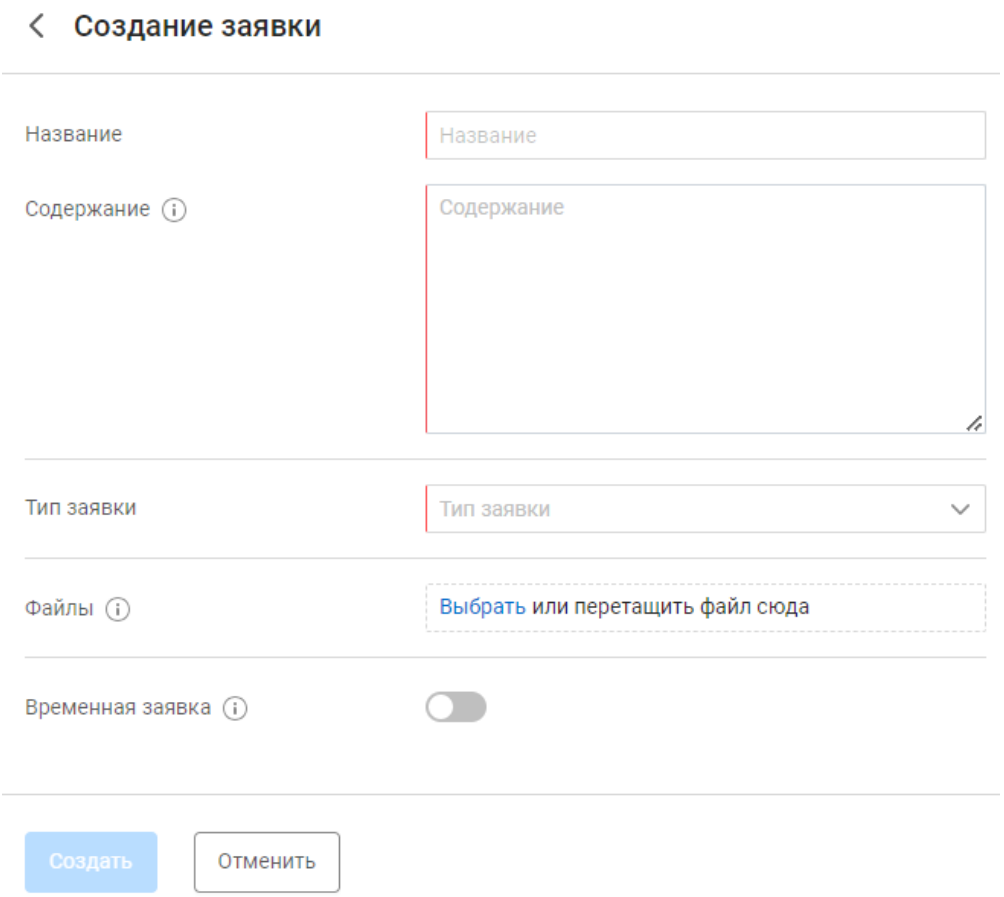


Рисунок 70 – Окно «Создание заявки»

Таблица 26 – 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 содержания заявки. На основании содержания заявки будет проводиться ее последующее выполнение. Параметры ввода текста: от 1 до 4000 любых символов
Поле «Тип заявки»	Раскрывающийся список для выбора типа заявки. При выборе типа заявки «Запрос доступа»[8] появляются дополнительные поля (см. ниже)
Поле «Файлы»	Поле для загрузки файла. Допустимые расширения файлов: .docx, .csv, .xls, .xlsx, .pdf. Максимальный размер всех вложений: 10 МБ
Поле «Временная	Переключатель:

[8] Тип заявки «Запрос доступа» доступен только при наличии лицензии на функциональный модуль «Efros CM»

Поле	Описание
заявка»	— «Включен» ( ) – создаваемая заявка будет иметь ограничение по времени действия с автоматическим созданием заявки на отмену; — «Отключен» ( ) – заявка не будет иметь ограничение по времени действия. При включенном переключателе добавляются поля «Окончание срока заявки» и «Дата/Период окончания» (см. ниже)
Поле «Окончание срока заявки»	Переключатель: — «Дата» – назначить дату и время окончания срока заявки в поле «Дата окончания»; — «Период» – назначить период до окончания срока заявки в поле «Период окончания» в минутах, часах, днях, неделях, месяцах или годах.
Блок полей «Запрос доступа»	
Поле «Начальная точка»	Поле для ввода IP-адреса начальной точки пути маршрута
Поле «Конечная точка»	Поле для ввода IP-адреса конечной точки пути маршрута
Поле «Протоколы/порты»	Раскрывающийся список для выбора протокола и числовое поле для ввода номера порта. Порты указываются через «,» и допустимо указывать диапазон портов. Пример: 22,23,45-47. Допустимые значения портов: от 1 до 65535
Элементы управления	
Создать	При нажатии на кнопку отображается окно созданной заявки
Отменить	При нажатии на кнопку окно создания заявки закрывается без сохранения данных

7.1.2 Управление стандартной пользовательской заявкой

После создания стандартной пользовательской заявки пользователю необходимо отправить заявку в работу:

1) После создания заявки откроется страница управления заявкой (рис. 71). Либо для перехода на страницу необходимо на вкладке «Заявки» нажать на название созданной заявки.

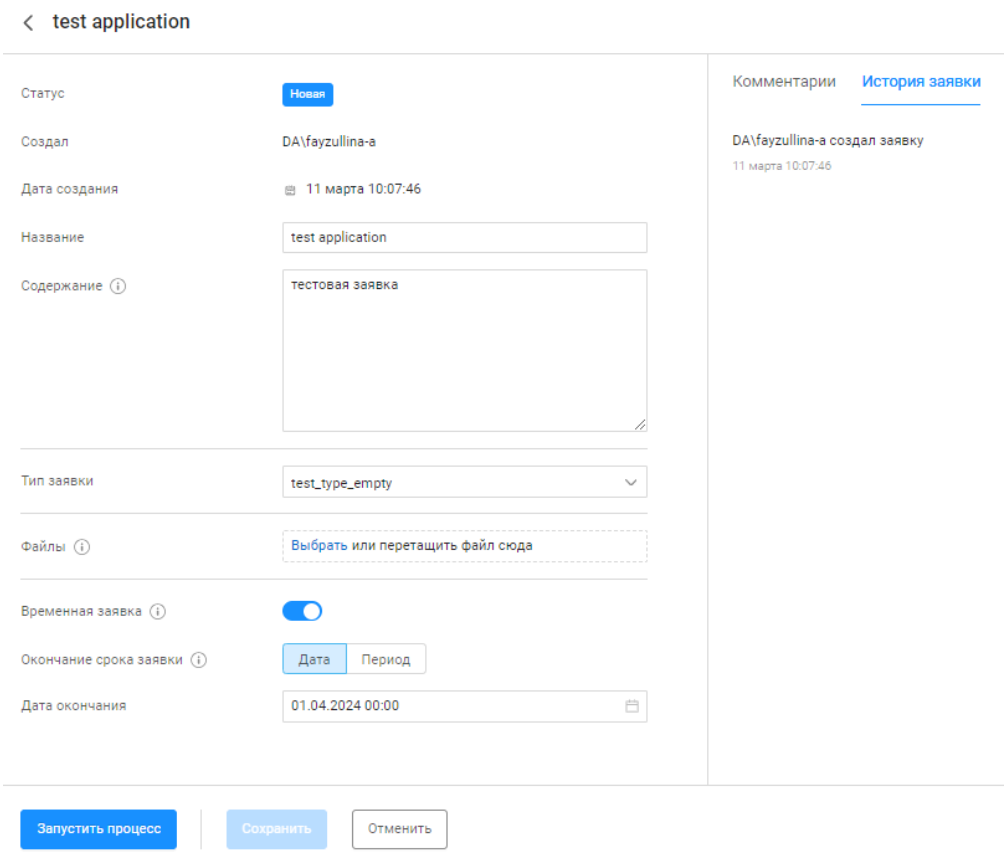
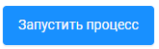
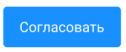


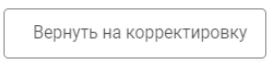
Рисунок 71 – Страница управления заявкой со статусом «Новая»

2) На странице заявки со статусом «Новая» пользователь может выполнить следующие действия:
— отредактировать название и содержание заявки;
— поменять тип заявки;
— загрузить файл с расширением .docx, .csv, .xls .xlsx или .pdf, содержащий уточняющую информацию. Поле доступно на любой стадии заявки;
— добавить комментарий. Вкладка доступна на любой стадии заявки;
— просмотреть историю заявки от начала ее создания до закрытия;
— отправить заявку в работу, нажав кнопку «Запустить процесс» (

).

3) На странице заявки с запущенным процессом выполнения – заявки в статусе «На согласовании» (рис. 72) пользователь может выполнить следующие действия:
— согласовать заявку, нажав кнопку «Согласовать» (

);
— отклонить заявку, нажав кнопку «Отклонить» (

). При нажатии кнопки заявка закрывается со статусом «Не утверждена» или «Не согласована»;
— отправить заявку на корректировку, нажав кнопку «Вернуть на корректировку» (

) и заполнив поле «Комментарий» в окне «Возврат заявки на корректировку» (рис. 73). На этапе согласования заявка отправляется на

корректировку пользователю, создавшему ее. На этапе утверждения заявка отправляется на корректировку исполнителю.

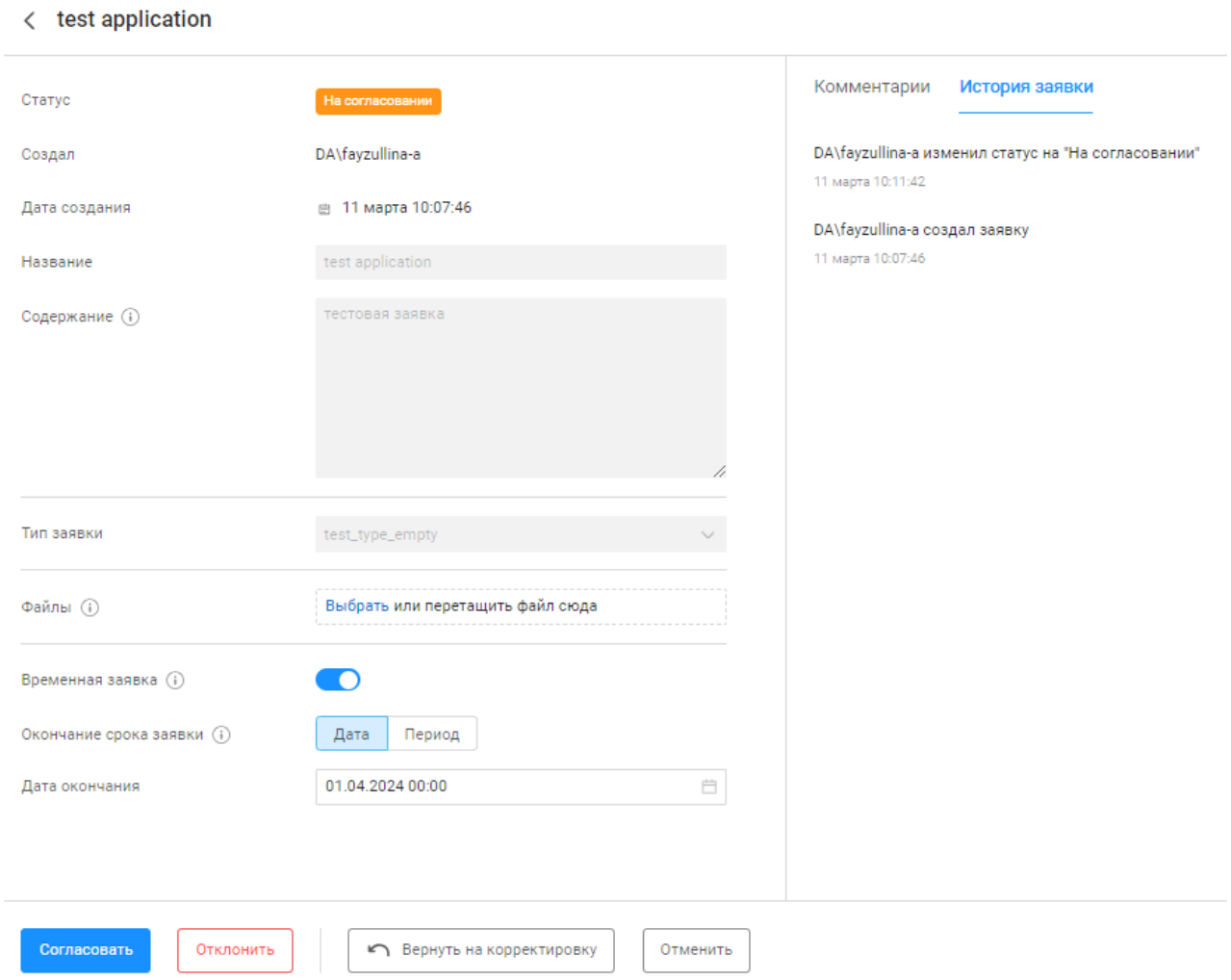


Рисунок 72 – Страница управления заявкой в статусе «На согласовании»

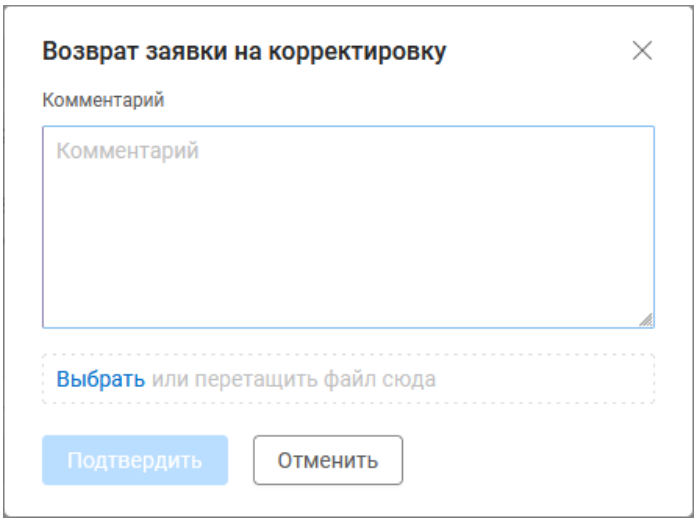
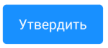
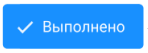


Рисунок 73 – Окно «Возврат заявки на корректировку»

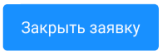
4) После согласования заявки на странице управления заявкой пользователь может выполнить следующие действия:

— утвердить заявку, нажав кнопку «Утвердить» (

);

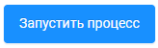
— отметить заявку как выполненную, нажав кнопку «Выполнено» (

) и заполнив поле «Комментарий» в окне «Выполнение заявки»;

— закрыть заявку, нажав кнопку «Закрыть заявку» (

) и заполнив поле «Комментарий» в окне «Закрытие заявки».

7.1.3 Управление типом заявки «Запрос доступа»

После создания заявки пользователю необходимо нажать кнопку «Запустить процесс» (

). Автоматически начнется процесс моделирования, который состоит из следующих этапов:

— построение всех возможных маршрутов;
— поиск устройств по всем возможным маршрутам;
— поиск правил МЭ по каждому найденному устройству, которые могут мешать построению маршрута;
— выдача информации по каждому найденному правилу МЭ.

Процессы моделирования, создания комплексом и применения правил для устранения блокировки трафика по выбранному маршруту осуществляются на виртуальных устройствах сети. Для выполнения смоделированных процессов на физических устройствах необходимо на вкладке «Выполнение» выбрать режим выполнения: «Авторежим» или «Ручной режим». Более подробное описание см. в п. 7.1.3.4.

После завершения процесса моделирования откроется страница с результатами построения маршрута (рис. 74).

На странице доступны следующие вкладки:

— «Настройки»;
— «Маршруты доступа»;
— «Соответствие»;
— «Выполнение»;
— «Проверка».

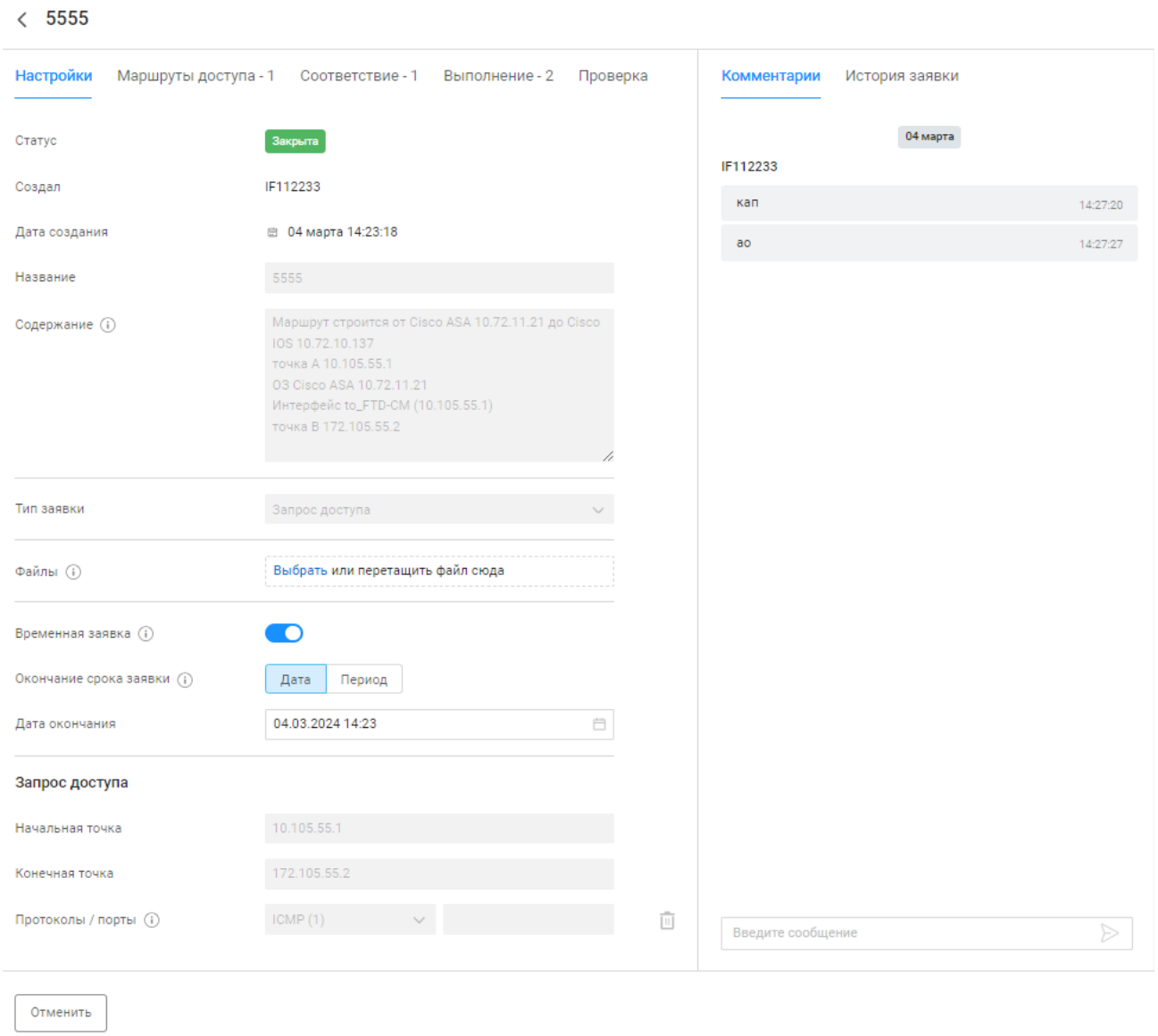


Рисунок 74 – Страница управления заявкой с результатами моделирования

7.1.3.1 Вкладка «Настройки»

На вкладке «Настройки» отображаются основные параметры заявки, такие как «Статус», логин пользователя, создавшего заявку, дата создания заявки, название, содержание, тип заявки «Запрос доступа», файлы, параметры запроса доступа. Все поля недоступны для редактирования.

Также на странице есть вкладки «Комментарии» и «История заявки» (см. рис. 74).

7.1.3.2 Вкладка «Маршруты доступа»

На вкладке «Маршруты доступа» отображаются все смоделированные маршруты движения трафика от начальной точки до конечной (рис. 75). Маршруты моделируются с использованием виртуальных устройств.

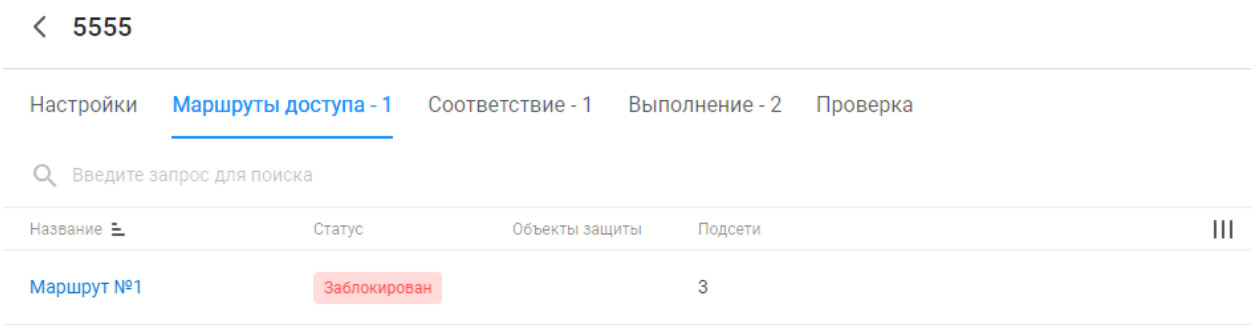


Рисунок 75 – Вкладка «Маршруты доступа»

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

- название маршрута. Является ссылкой, при переходе открывается страница с информацией о построенном маршруте;
- статус маршрута:
  - «заблокирован»;
  - «частично заблокирован»;
  - «построен»;
  - «прерван».
- объекты защиты, через которые построен маршрут;
- количество подсетей, при установке в поле курсора открывается подсказка с данными всех подсетей.

Над списком маршрутов располагаются:

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

Для просмотра детальной информации по смоделированному маршруту необходимо нажать на название маршрута. Откроется страница с активной вкладкой «Карта маршрута», содержащей графическое представление выбранного маршрута (рис. 76).

На вкладке «Карта маршрута» отображаются следующие данные:

- графическое отображение маршрута, который проходит трафик сети. Смоделированный маршрут выделен голубым цветом;
- табличное отображение маршрута;
- ОЗ. При наведении курсора на ОЗ появится всплывающее окно с краткой информацией об ОЗ.

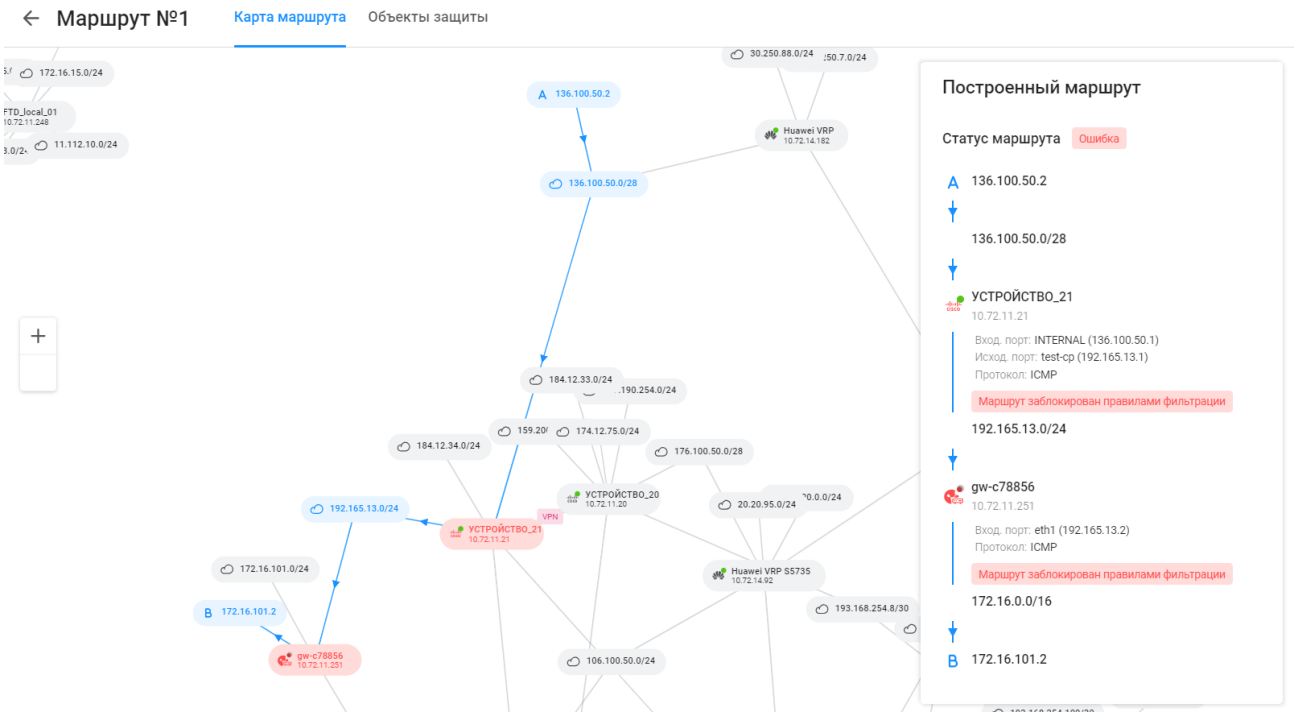


Рисунок 76 – Графическое представление построенного маршрута

Для просмотра детальной информации об ОЗ, через которые проходит маршрут, необходимо перейти на вкладку «Объекты защиты» (рис. 77).

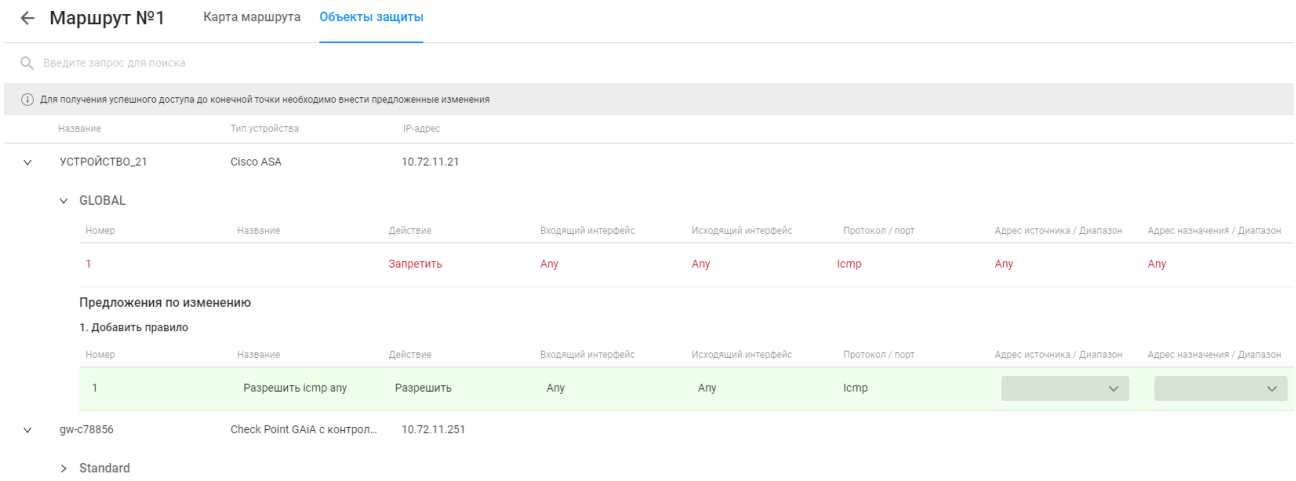


Рисунок 77 – Вкладка «Объекты защиты»

На вкладке «Объекты защиты» отображаются следующие данные:

- название блокирующего маршрут ОЗ;
- тип устройства;
- IP-адрес устройства;
- набор правил, блокирующих прохождение маршрута;
- правила, сгенерированные комплексом, для устранения блокировки движения трафика по маршруту.

Сгенерированные в процессе моделирования правила МЭ добавляются на

виртуальном устройстве перед соответствующим блокирующим правилом. Правила МЭ на устройстве выполняются по списку сверху вниз до первого сработавшего правила.

Над списком ОЗ располагается поле поиска (Введите запрос для поиска). При выборе строки с необходимым ОЗ в правом углу строки появляется кнопка «Сравнить» ( ) для сравнения отчетов: сравниваются отчет, который блокирует трафик на устройстве, и отчет, который сгенерирован системой для снятия блокировки.

7.1.3.3 Вкладка «Соответствие»

На вкладке «Соответствие» (рис 78) представлена следующая информация:

- ОЗ, блокирующие трафик на маршруте;
- отчеты по каждому блокирующему трафик на маршруте ОЗ. Данные отчеты содержат информацию с учетом добавленных изменений в ходе моделирования по соответствующему виртуальному устройству в рамках всех маршрутов доступа одновременно (в которых участвует рассматриваемое устройство).

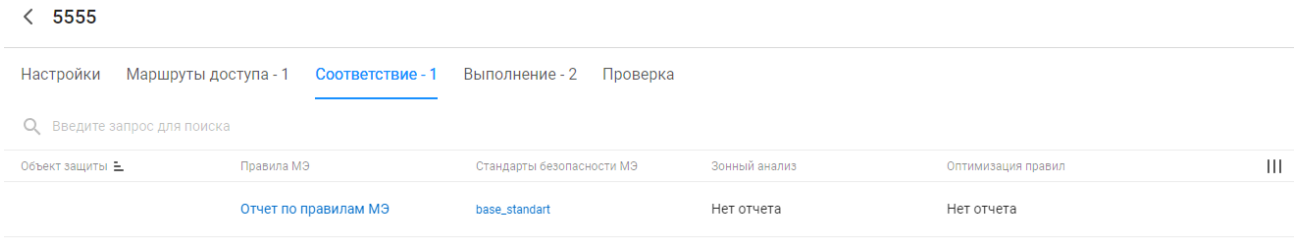


Рисунок 78 – Вкладка «Соответствие»

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

- название ОЗ;
- правило МЭ. Является ссылкой. При нажатии открывается отчет с информацией о правиле МЭ;
- название стандарта безопасности МЭ, если их несколько, то количество стандартов безопасности МЭ (при установке в поле курсора открывается список всех стандартов) или текст «Нет отчета» при отсутствии стандартов. Название стандарта является ссылкой. При нажатии открывается отчет с информацией о соответствующем стандарте безопасности МЭ по ОЗ;
- название стандарта зонного анализа МЭ, если их несколько, то количество стандартов зонного анализа МЭ (при установке в поле курсора открывается список всех стандартов) или текст «Нет отчета» при отсутствии стандартов. Название стандарта является ссылкой. При нажатии открывается отчет с информацией о соответствующем стандарте зонного анализа МЭ по ОЗ;
- оптимизация правил (или текст «Нет отчета» при отсутствии отчета по оптимизации правил для ОЗ). Является ссылкой. При нажатии открывается отчет

с информацией по оптимизации правил.

Над списком соответствий располагаются:

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

7.1.3.4 Вкладка «Выполнение»

На вкладке «Выполнение» (рис 79) предоставлена следующая информация:

— ОЗ, блокирующие прохождение трафика на маршруте;
— отчеты по каждому блокирующему ОЗ.

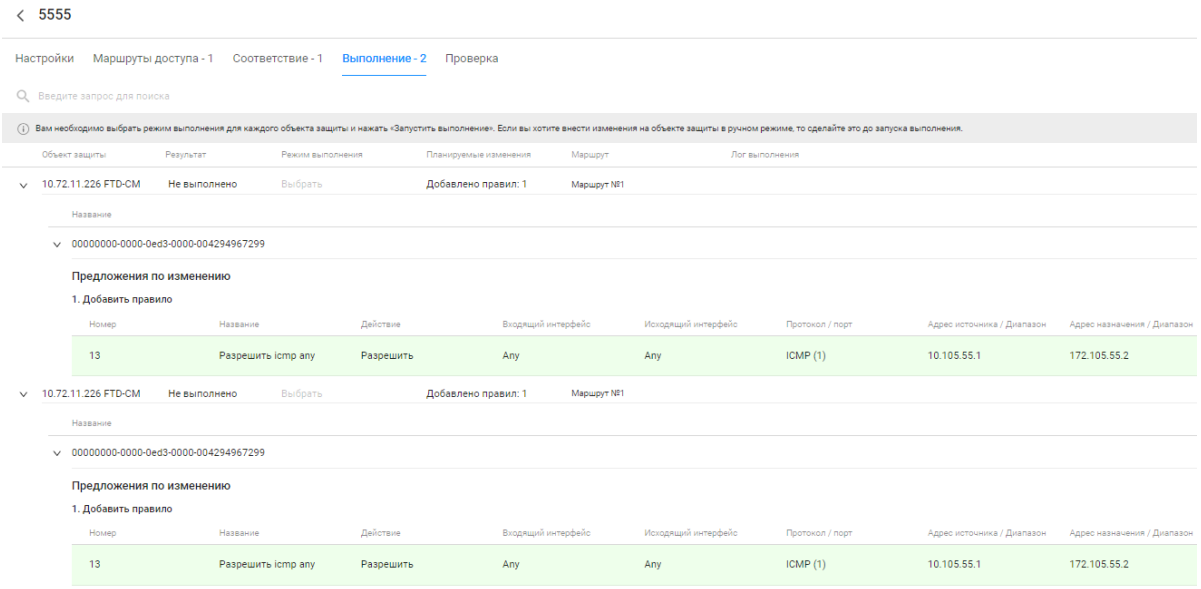


Рисунок 79 – Вкладка «Выполнение»

Список выполнений реализован в виде таблицы. Для каждой записи отображаются следующие данных:

— список ОЗ;
— наборы правил, в которых содержится хотя бы одно блокирующее правило по каждому блокирующему трафик ОЗ;
— разрешающие правила.

Блок «Предложения по изменению» предназначен для отображения списка сгенерированных моделированием правил МЭ, которые пользователь может добавить на физическое устройство вручную или автоматически путем выбора «Авторежим» в столбце «Режим выполнения» и последующего нажатия кнопки «Запустить выполнение» (Запустить выполнение). Также для ОЗ можно посмотреть изменения в отчете «Правила МЭ», нажав на кнопку «Сравнить» ( ). Над списком заявок располагается поле поиска (Введите запрос для поиска).

7.1.3.5 Вкладка «Проверка»

Вклада «Проверка» отображается после того, как завершится процесс моделирования запроса доступа, а заявка будет отмечена как выполненная.

На вкладке «Проверка» (рис. 80) отображаются следующие списки:

- запрашиваемый доступ;
  - начальная точка;
  - конечная точка;
  - протоколы / порт.
- изменение конфигурации – список блокирующих физических устройств с соответствующими отчетами «Правила МЭ»;
- соответствие – список блокирующих физических устройств с соответствующими отчетами «Стандарты безопасности МЭ», «Зонный анализ» и «Оптимизация правил»;
- результат моделирования – для просмотра построенных маршрутов доступа.

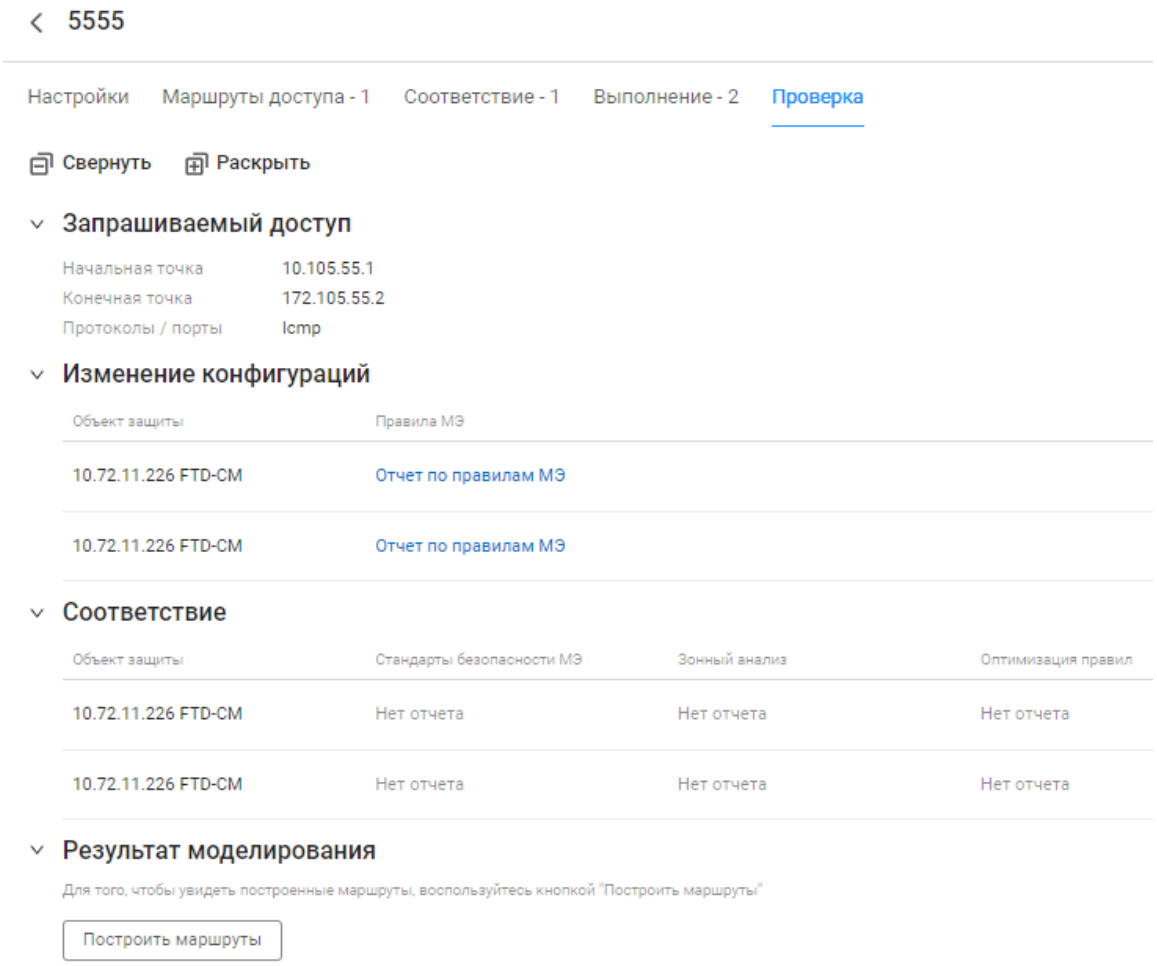


Рисунок 80 – Вкладка «Проверки»

7.2 Вкладка «Типы заявок»

На вкладке «Типы заявок» отображаются существующие типы заявок:

- пользовательские типы заявок;
- системные типы заявок:
  - «Запрос доступа»;
  - «Отмена изменений».

Тип заявки «Запрос доступа» доступен пользователю только при наличии лицензии на функциональный модуль «Efros CM».

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

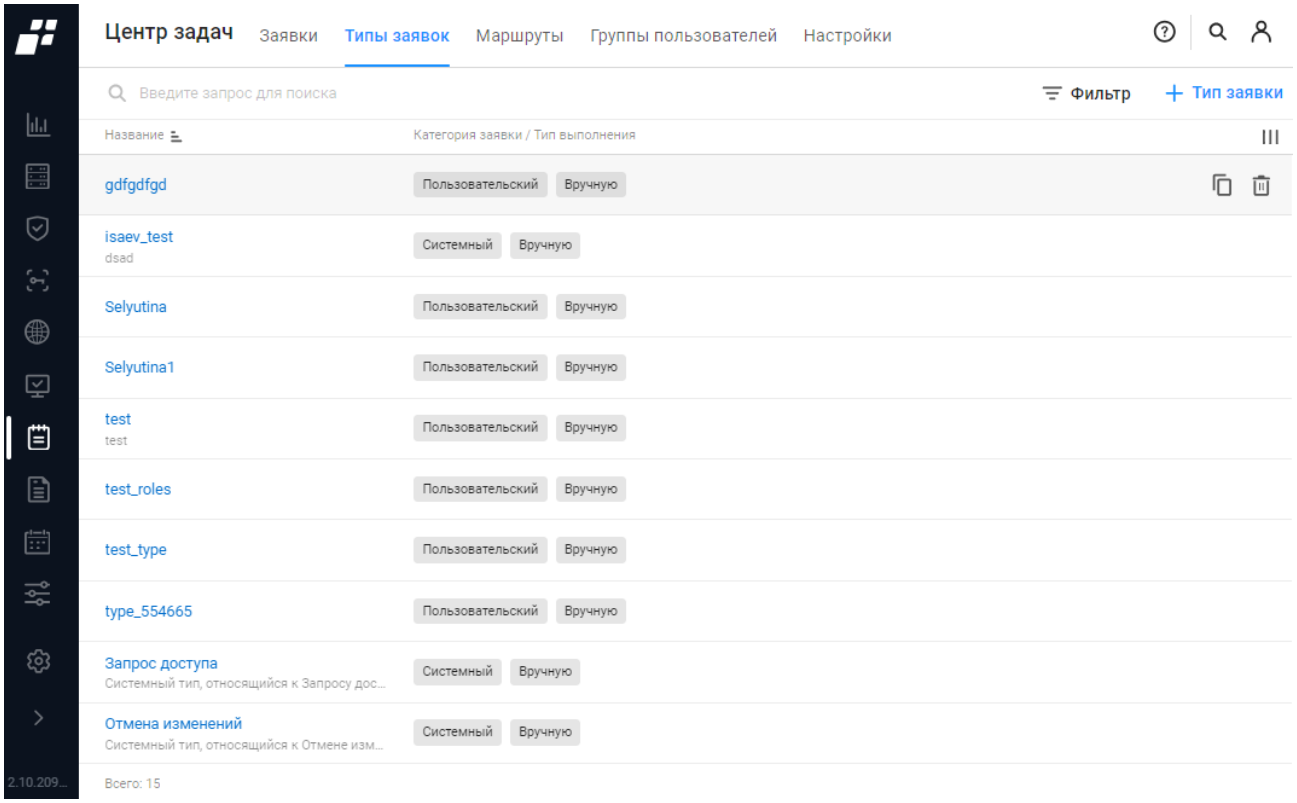


Рисунок 81 – Вкладка «Типы заявок»

Для каждой записи списка отображаются следующие данные:

- название типа заявки. Является ссылкой, при переходе по которой открывается окно редактирования типа заявки;
- категория заявки и способ выполнения заявки.

Над списком располагаются:

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

— кнопка «Тип заявки» (+ Тип заявки);

— кнопка «Колонки» ( ).

При выборе строки с типом заявки в правом углу строки появляются кнопки:

— «Удалить» ( ). Для удаления доступны только пользовательские типы заявок;

— «Создать копию» ( ).

7.2.1 Создание нового типа заявки

Для создания нового типа заявки пользователю необходимо:

1) Нажать на странице вкладки «Типы заявок» (см. рис. 81) кнопку «Тип заявки» (+ Тип заявки).
2) Откроется страница создания нового типа заявки (рис. 82). Заполнить поля необходимыми параметрами и нажать кнопку «Создать». Состав и описание полей страницы приведены в таблице 27.

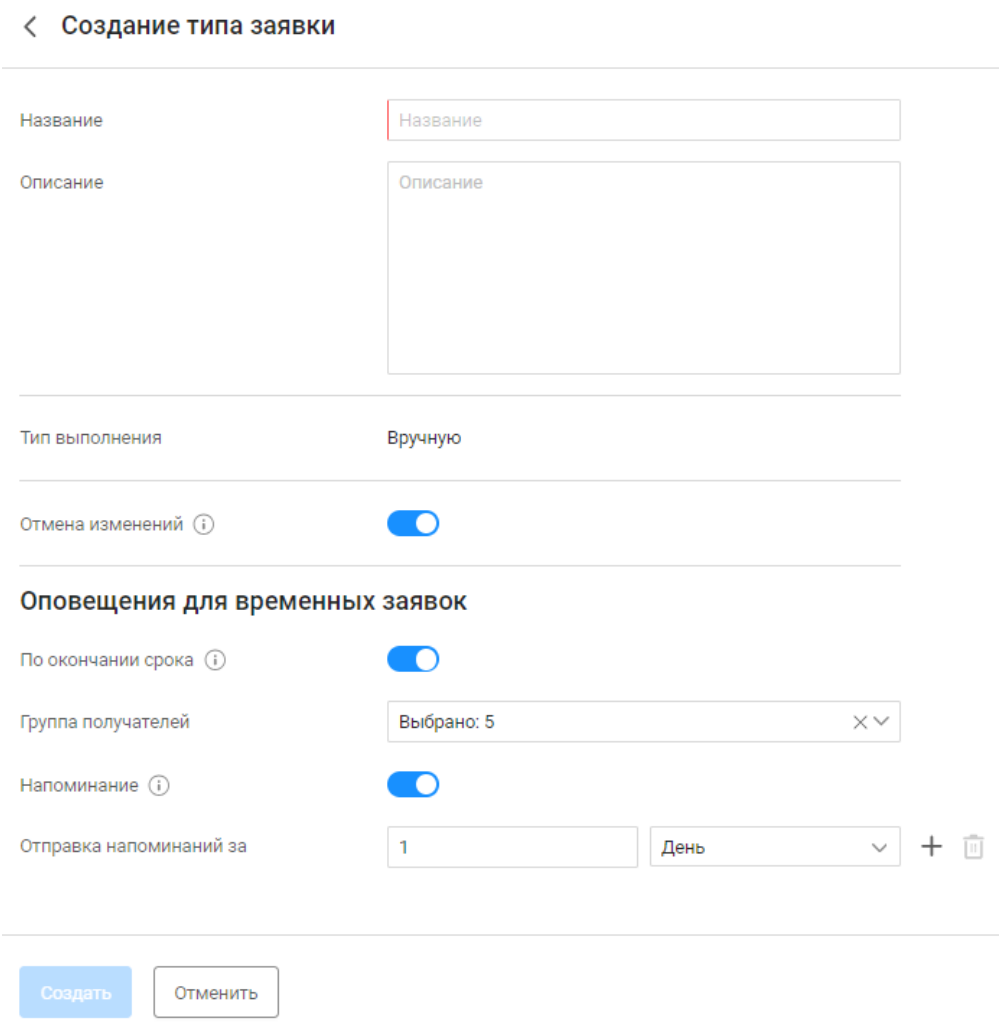


Рисунок 82 – Окно «Создание типа заявки»

Таблица 27 – 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 «Тип выполнения»	Поле заполняется автоматически: «Вручную». Параметр неизменяемый
Поле «Отмена изменений»	Переключатель: — «Активен» ( ) – автоматическое создание заявки на отмену изменений после окончания срока основной заявки; — «Неактивен» ( ) – заявка на отмену изменений не создается
Блок полей «Оповещения для временных заявок»	
Поле «По окончании срока»	Переключатель: — «Активен» ( ) – оповещение пользователей об окончании срока заявки с возможностью выбора групп получателей; — «Неактивен» ( ) – отсутствие оповещений. При активации переключателя появляются дополнительные поля «Группа получателей» и «Напоминание»
Поле «Группа получателей»	Поле с раскрывающимся списком для выбора групп получателей: — «Автор»; — «Исполнители»; — «Проверяющие»; — «Согласующие»; — «Утверждающие»
Поле «Напоминание»	Переключатель: — «Активен» ( ) – оповещения до окончания срока заявки; — «Неактивен» ( ) – отсутствие оповещений. При активации переключателя появляется дополнительное поле «Отправка напоминаний за» для ввода периода времени
Поле «Отправка напоминаний за»	Поле для ввода одного или нескольких периодов времени отправки получателям напоминаний в минутах, часах, днях, неделях, месяцах и годах по выбору пользователя
Элементы управления	

Поле	Описание
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

7.2.2 Редактирование типа заявки «Запрос доступа»

Для редактирования типа заявки «Запрос доступа» пользователю необходимо:

1) Нажать на странице (см. рис. 81) на запись системного типа заявки «Запрос доступа». Откроется страница редактирования типа заявки, аналогичная странице создания типа заявки (см. п. 7.2.1). Отличием является наличие переключателя «Динамический маршрут».

Динамический маршрут предназначен для отправки связанных заявок в рамках движения по маршруту пользователям, которые являются ответственными по ОЗ. Так по одной заявке может производиться параллельная работа по ОЗ соответствующими пользователями на каждой из стадий маршрута: «Согласование», «Утверждение», «Выполнение», «Проверка».

2) Внести требуемые изменения в параметры типа заявки «Запрос доступа», включить при необходимости переключатель «Динамический маршрут».
3) Нажать кнопку «Сохранить».

7.3 Вкладка «Маршруты»

Вкладка «Маршруты» содержит маршруты следования заявок (рис. 83).

Для каждой записи списка отображаются следующие данные:

- название маршрута. Является ссылкой, при переходе по которой открывается окно редактирования маршрута;
- дата создания маршрута и логин пользователя, создавшего маршрут;
- тип заявки, примененный к маршруту.

Тип заявки «Запрос доступа» может быт применен только для одного маршрута.

Над списком располагаются:

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

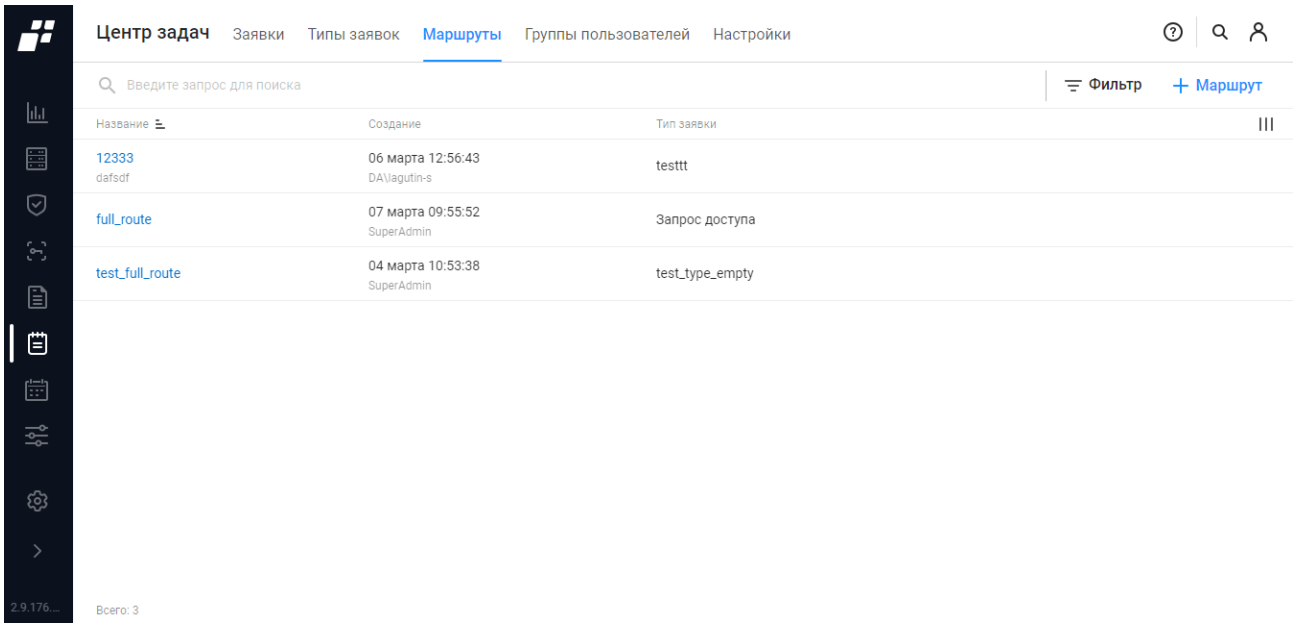


Рисунок 83 – Вкладка «Маршруты»

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

— «Удалить» ( );

— «Создать копию» ( ).

7.3.1 Создание нового маршрута

Перед созданием маршрута необходимо проверить, что созданы 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. 84).

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 «Тип заявки», «Название» и «Описание».

Добавление стадий маршрута заявки доступно после выбора «Типа заявки». Добавление стадии производится по нажатию кнопки «⊕» рядом с объектом маршрута (рис. 85).

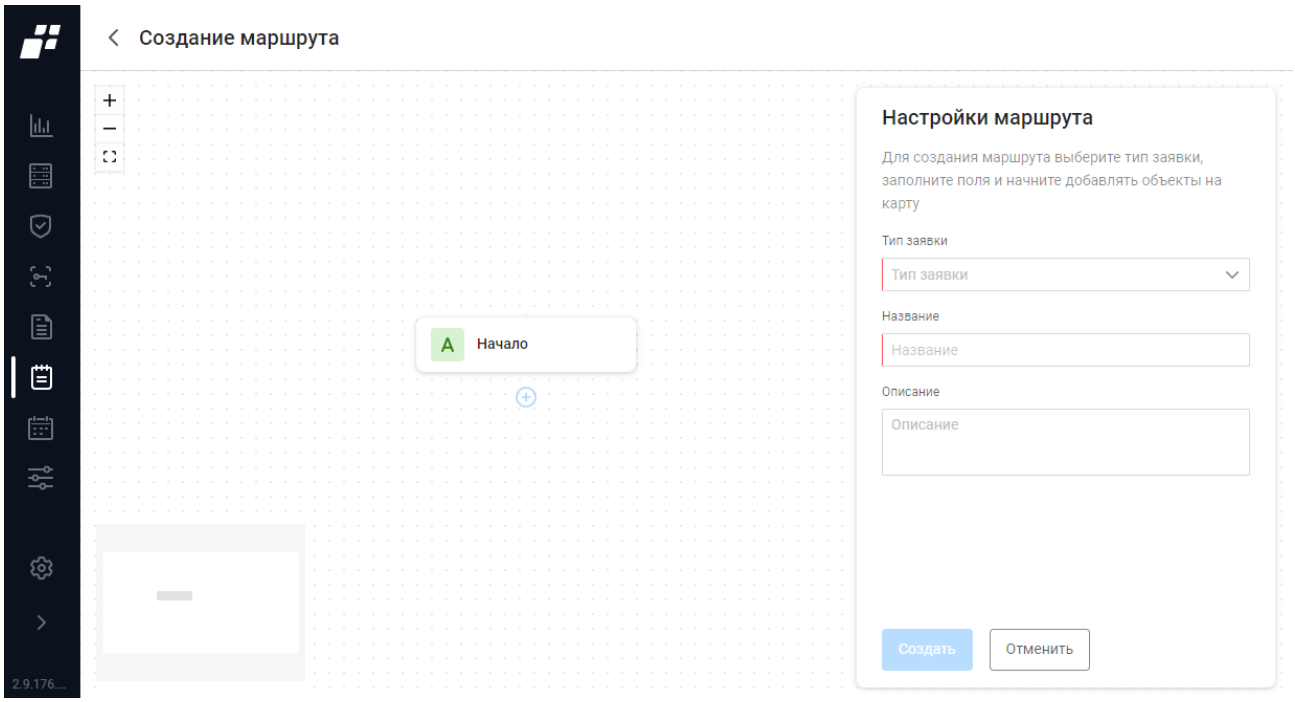


Рисунок 84 – Страница создания маршрута

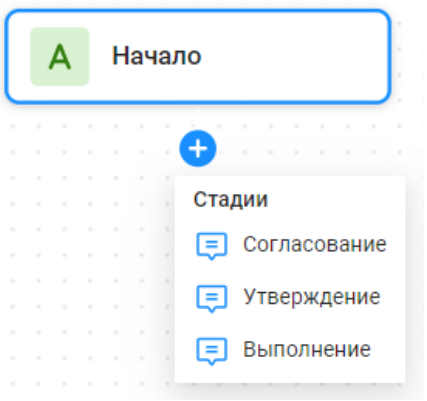


Рисунок 85 – Добавление стадии маршрута

Существуют следующие основные стадии заявки:

- «Начало»;
- «Согласование»;
- «Утверждение»;
- «Выполнение»;
- «Проверка»;
- «Корректировка»;
- «Закрытие».

Для типа заявки «Запрос доступа» после стадии заявки «Начало» создается стадия «Моделирование», которая предназначена для оповещения пользователя о возврате построенного маршрута на начальное состояние в случае изменения типа заявки.

В случае возникновения ошибки при использовании маршрута с типом заявки «Запрос доступа», необходимо убедиться в наличии у маршрута стадии «Моделирование». При отсутствии стадии «Моделирование», требуется удалить маршрут и создать его заново.

Дополнительные шаги при прохождении заявки по маршруту:

- «Условие» – шаг, позволяющий выбрать одну из стадий: «Завершение», «Корректировка», «Согласование», «Утверждение» или «Выполнение»;
- «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.

Для корректного выполнения шага «Уведомление» необходимо включить и настроить возможность отправки сообщений для используемых почтовых серверов SMTP и Microsoft Exchange (подробнее см. п. 11.6)

При добавлении стадий «Согласовано», «Утверждение», «Выполнение» и «Проверка» необходимо выбрать группу пользователей, которые будут участвовать в процессе выполнения заявки и добавить требуемое условие:

- «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.

Для типа заявки «Запрос доступа» после стадии «Моделирование» обязательно должны присутствовать стадии «Завершение» и «Корректировка».

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 несколькими 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 не доступны для редактирования.

7.4 Вкладка «Группы пользователей»

Вкладка «Группы пользователей» содержит группы пользователей, которые участвуют в маршруте выполнения заявки (рис. 86).

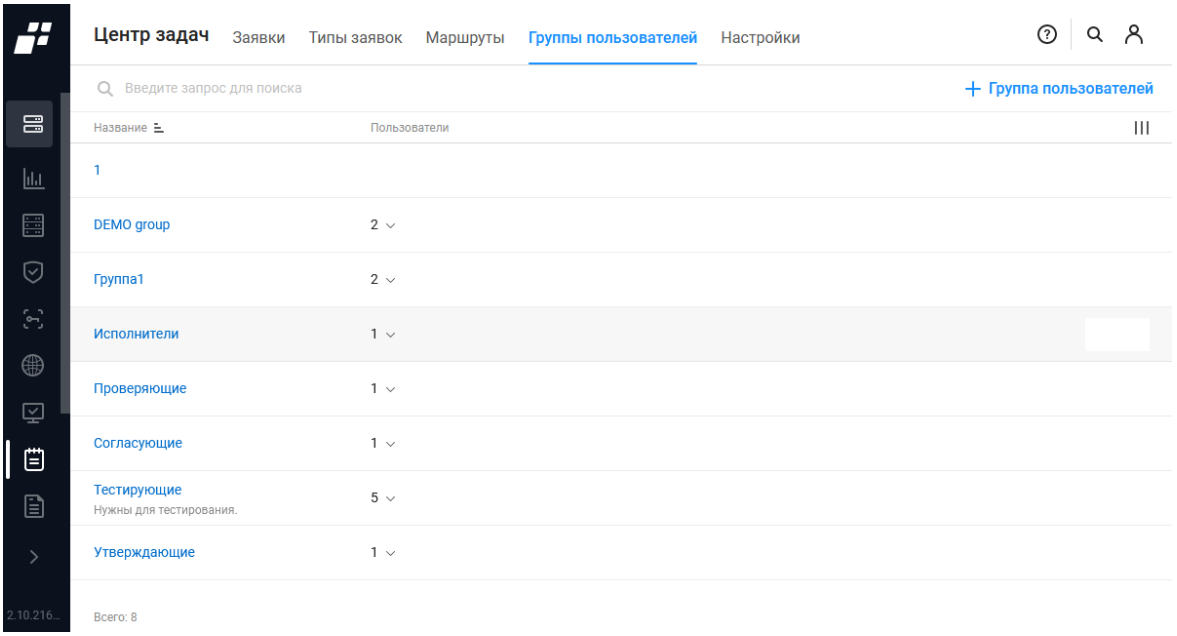


Рисунок 86 – Вкладка «Группы пользователей»

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;
- количество пользователей, входящих в группу. При установке в поле курсора раскрывается подсказка со списком пользователей.

Над списком располагаются:

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

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

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

7.4.1 Создание новой группы пользователей

Для создания новой группы пользователей пользователю необходимо:

1) Нажать на странице вкладки «Группы пользователей» (см. рис. 86) кнопку «Группа пользователей» (+ Группа пользователей).
2) Откроется страница создания новой группы пользователей (рис. 87). Состав и описание полей страницы приведены в таблице 28.
3) Заполнить поля необходимыми параметрами и нажать кнопку «Создать»

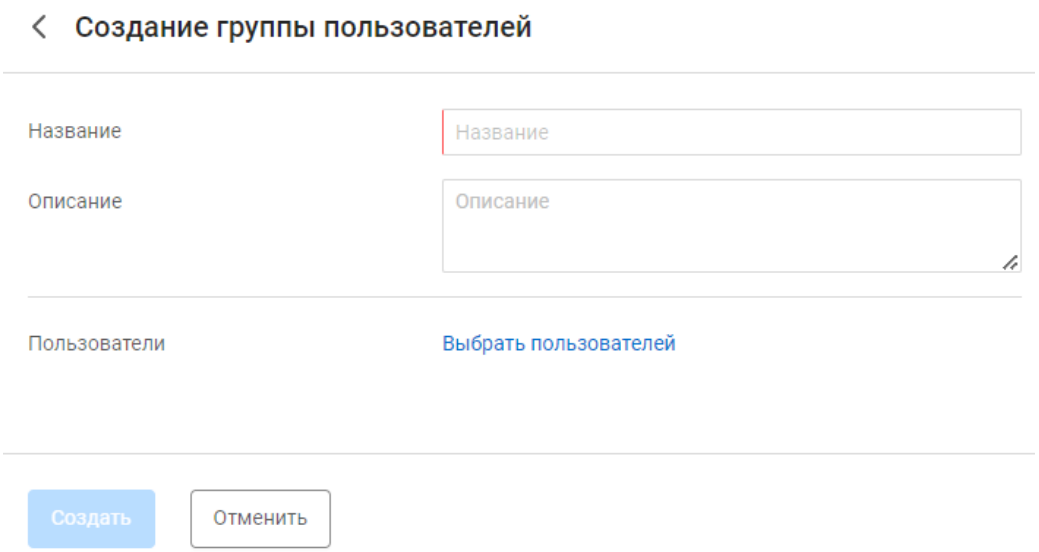


Рисунок 87 – Окно «Создание группы пользователей»

Таблица 28 – 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 «Выбрать пользователей» открывается окно выбора пользователей для добавления их в создаваемую группу. В окне необходимо установить флаг в строках требуемых пользователей и нажать кнопку «Выбрать»
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

7.5 Вкладка «Настройки»

Вкладка «Настройки» (рис. 88) позволяет пользователю задать временные промежутки прохождения каждой стадии заявки и максимальный размер прикрепляемого файла. Состав и описание полей страницы приведены в таблице Таблица 29.

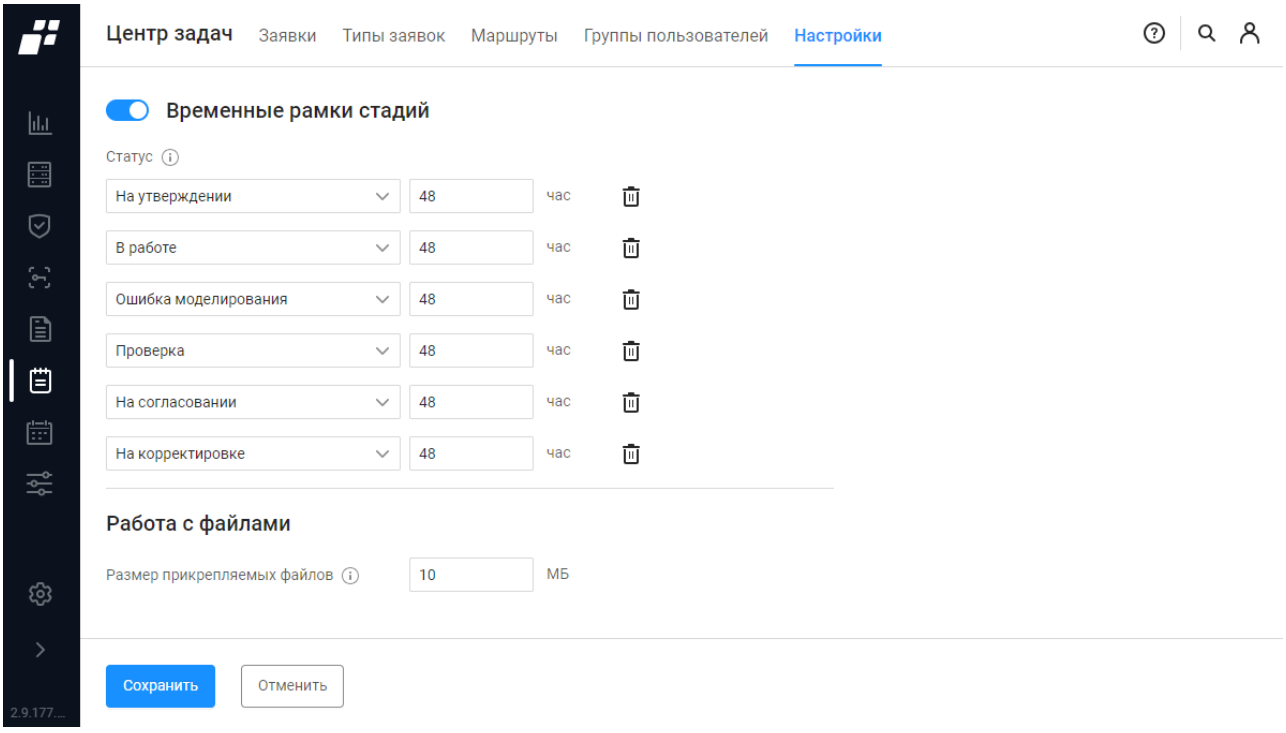


Рисунок 88 – Вкладка «Настройки»

Таблица 29 – Состав и описание полей вкладки «Настройки»

Поле	Описание
Поле «Временные рамки стадий»	Переключатель: — «Включен» ( ) – заявки в указанных в поле «Статус» (см. ниже) статусах будет иметь ограничение по времени действия с автоматическим созданием заявки на отмену; — «Отключен» ( ) – заявка не будет иметь ограничение по времени действия. При включенном переключателе добавляется поле «Статус»» (см. ниже)
Поле «Статус»	Таблица статусов заявки. Для добавления дополнительного поля необходимо нажать кнопку « + ». Для удаления лишнего поля – нажать кнопку « »
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
Элементы управления	
Сохранить	При нажатии кнопку происходит сохранение внесенных данных
Отменить	При нажатии на кнопку внесенные данные не сохраняются

8 Раздел «Отчеты»

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

В разделе «Отчеты» 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. Описание типов отчетов, применяемых для создания шаблонов, приведены в таблице 30.

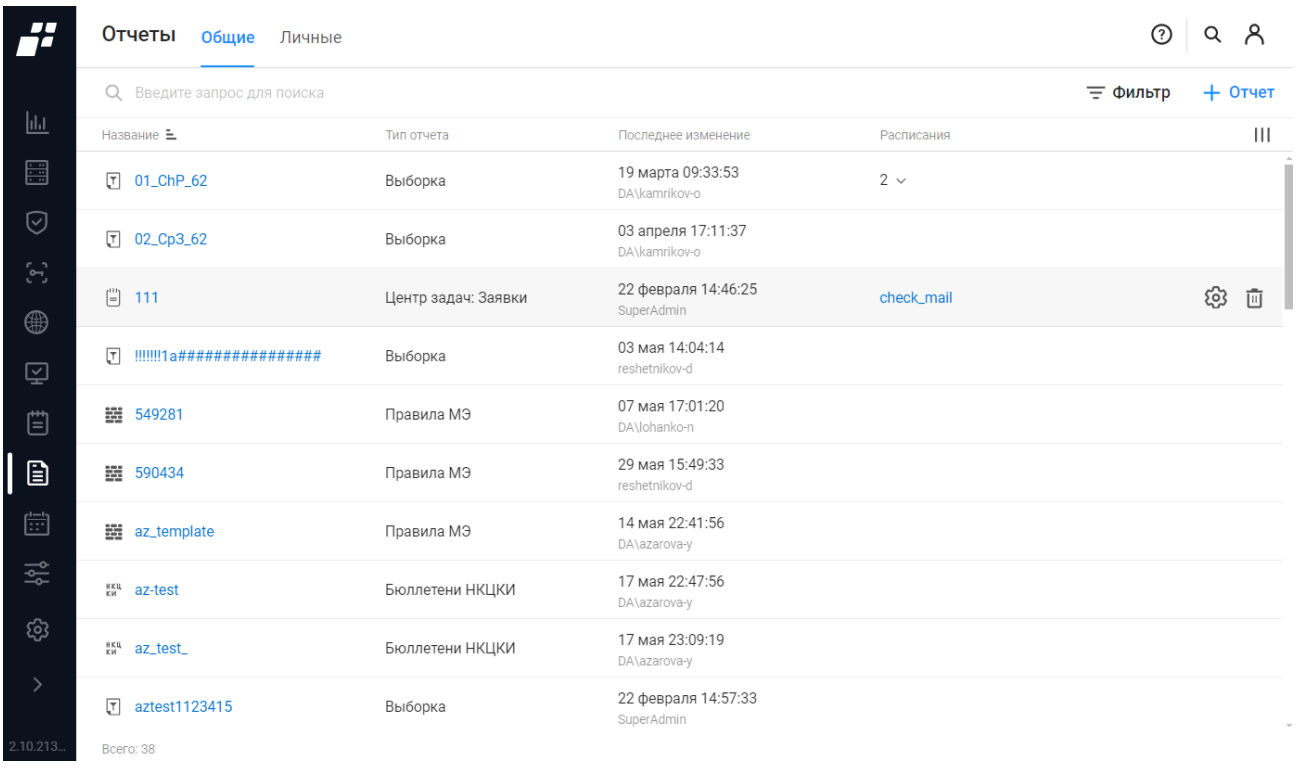


Рисунок 89 – Раздел «Отчеты»

Таблица 30 – Состав и описание полей страницы создания шаблона отчета

Тип отчета	Описание	Требуемая лицензия
Выборка	Представляет собой сводную информацию, содержащуюся в последних загруженных отчетах одного типа ОЗ, имеющих возможность «Контроль устройств»	«Efros NA» или «Efros ICC»
Действия	Представляет собой сводную информацию по	«Efros NA»,

Тип отчета	Описание	Требуемая лицензия
пользователей	действиям пользователей на ОЗ (по событиям протокола TACACS+: Аутентификация, Авторизация и Аудит)	«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»	«Efros VC»
Бюллетени НКЦКИ	Представляет собой сводный перечень отчетов по бюллетеням Национального координационного центра по компьютерным инцидентам (НКЦКИ) на ОЗ и бюллетеням из базы данных уязвимостей (БДУ)	«Efros VC»
Оптимизация правил МЭ	Представляет собой сводную информацию из существующих отчетов по оптимизации правил МЭ	«Efros FA»
Правила МЭ	Представляет собой сводные данные по всем правилам МЭ на ОЗ, отобранных пользователем по определенным критериям	«Efros FA»
Центр задач: Заявки	Представляет собой отчет, в котором отображается информация по заявкам из раздела «Центр задач»	«Efros CM»
Доступ в сеть: Трафик	Представляет собой сводную информацию по событиям доступа в сеть ОЗ и конечных точек, отобранных пользователем по определенным критериям	«Efros NAC»

Список шаблонов 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;
- тип отчета;
- дата последнего изменения шаблона и логин пользователя, внесшего изменения;
- расписание или, если их несколько, то количество расписаний, настроенных для шаблона. Является ссылкой, при переходе по которой открывается страница редактирования расписания.

Расписания для загрузки отчетов создаются во вкладке «По расписанию» раздела «Планировщик». Описание и правила редактирования расписания приведены в п. 10.4.2.

Над списком шаблонов располагаются:

— поле поиска (Введите запрос для поиска);

— кнопка «Фильтр» (Фильтр);

— кнопка «Добавить отчет» (+ Отчет);

— кнопка «Колонки» ( ).

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

— «Удалить» ( );

— «Настройки» ( ).

Содержание вкладки «Личные» аналогично содержанию вкладки «Общие», кроме того, что отсутствует колонка «Расписания».

8.1 Создание шаблона отчета

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

1) Нажать кнопку «Отчет» (+ Отчет) (см. рис. 89).
2) Из раскрывающегося списка выбрать необходимый тип шаблона.
3) Откроется страница создания шаблона отчета. Заполнить поля необходимыми параметрами и нажать кнопку «Выполнить». Состав и описание полей страницы в зависимости от типа создаваемого шаблона приведены в таблице 31.
4) Просмотреть отчет и при необходимости сохранить его, для чего нажать кнопку «Экспорт» (Экспорт), выбрать в раскрывшемся меню формат файла (PDF, DOCX или XLSX) и выбрать путь для сохранения файла.
5) При необходимости, изменить параметры отчета, для чего нажать кнопку «Параметры» (Параметры), в открывшемся окне настройки параметров отчета внести требуемые изменения и нажать кнопку «Применить». Отчет отобразится в соответствии с новыми параметрами.
6) Сохранить шаблон отчета, для чего нажать кнопку «Шаблон» (+ Шаблон), в открывшемся окне «Создание шаблона»:

— выбрать тип шаблона «Личный» или «Общий»;

— ввести название шаблона,

— оставить текущие параметры формирования отчета без изменений или внести требуемые изменения;

— нажать кнопку «Сохранить».

Таблица 31 – Состав и описание полей страницы создания шаблона отчета

Поле	Описание
Поля страницы «Создание отчета (Выборка)»	
Поле «Тип устройства»	Раскрывающийся список всех типов устройств, доступных в комплексе
Поле «Базовый отчет»	Раскрывающийся список базовых отчетов для выбранного ранее типа устройства. Поле становится активно после выбора типа устройства
Поле «Объекты защиты»	Является ссылкой на форму выбора ОЗ, доступных в комплексе
Поле «Тип фильтрации»	Поле отображается только после выбора структурированного базового отчета. Предназначено для выбора типа фильтрации данных
Блок полей «Фильтр содержимого». Состав полей зависит от типа выбранного базового отчета (текстовый или структурированный) Описание регулярных выражений стандарта PCRE, допустимых к применению в ПК «Efros DO» при задании условий поиска для создания шаблонов отчетов, приведено в Приложении А документа «Руководство пользователя. Часть 2. Контроль устройств».	
Для текстовых отчетов	В зависимости от выбранного ранее типа фильтрации содержит поля: 1. Для типа фильтрации «Простой поиск»: — «Условия поиска» – для ввода ключевого значения. Поиск будет выполняться по полному совпадению строки конфигурации введенному условию поиска.; — «Условия исключения» – для ввода значения исключения. При формировании отчета будут исключены строки, содержащие введенное значение. В полях поддерживается ввод символов «?» (один любой символ) и «*» (любые символы). Справа поля содержат кнопки «Добавить» (+) и «Удалить» () для добавления новых условий и удаления лишних. 2. Для типа фильтрации «Регулярные выражения (Поиск)»: — «Выражение поиска» – для ввода шаблона поиска данных; — «Только первое совпадение» – для поиска данных до обнаружения первого совпадения; — «Добавлять переводы строк между совпадениями» –

Поле	Описание
	для отображения каждого из найденных совпадений (при поиске всех совпадений) на новой строке отчета. 3. Для типа фильтрации «Регулярные выражения (Замена)»: — «Выражение поиска» – для ввода шаблона поиска данных; — «Выражение замены» – для ввода шаблона данных, которыми будут заменены искомые выражения; — «Только совпадения» – в форме просмотра отфильтрованного отчета в одну строку будут отображены только найденные и замененные выражения; — «Заменять только первое совпадение» – в форме просмотра отфильтрованного отчета будет изменено только первое из найденных выражений
Для структурированных отчетов	Содержит структурированный список параметров исходного отчета. В формируемый отчет попадут параметры, выбранные установкой флагов. Для выбранных параметров должны быть заданы правила отбора в полях, раскрывающихся при нажатии соответствующей параметру кнопки «+»: — для логических параметров – значение «Да» или «Нет» (выполняется или не выполняется); — для текстовых параметров – условия отбора. Может быть задано несколько условий типов «Равно», «Не равно», «Содержит» и «Не содержит» со значениями для отбора через логические условия «и»/«или». Справа поля параметров содержат кнопки «Добавить» (+) и «Удалить» (🗑) для добавления новых условий и удаления лишних
Поля страницы «Создание отчета (Действия пользователей)»	
Поле «Пользователи»	Раскрывающийся список сетевых пользователей АСО
Поле «Объекты защиты»	Является ссылкой на форму 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

Поле	Описание
Поля страницы «Создание отчета (Уязвимости ОЗ)»	
Поле «Источник»	Переключатель для выбора источника, отчет по уязвимостям ОЗ которого должен быть сформирован: — «Текущий сервер» – текущий активный сервер (выбор пользователем активного сервера при наличии иерархии серверов приведен в п. 3.1.2); — «Подчиненные серверы» – серверы, подчиненные текущему
Поле «Тип устройства»	Раскрывающийся список всех типов устройств, доступных в комплексе
Поле «Объекты защиты»	Является ссылкой на форму выбора ОЗ, имеющих возможность «Контроль устройств»
Поле «Критичность уязвимостей»	Раскрывающийся список видов критичности уязвимостей: — «Все значения» – по умолчанию; — «Высокой важности»; — «Критичные»; — «Низкой важности»; — «Средней важности». Более подробно см. документ «Руководство пользователя. Часть 2. Контроль устройств»
Поля страницы «Создание отчета (Бюллетени НКЦКИ)»	
Поле «Тип устройства»	Раскрывающийся список всех типов устройств, доступных в комплексе
Поле «Объекты защиты»	Является ссылкой на форму выбора 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: — «Все значения» – по умолчанию; — «Высокой важности»; — «Критичные»; — «Не определен»; — «Средней важности»
Поля страницы «Создание отчета (Оптимизация правил МЭ)»	
Поле «Тип	Раскрывающийся список с типами устройств, которые

Поле	Описание
устройства»	поддерживают отчет «Правила МЭ»
Поле «Объекты защиты»	Является ссылкой на форму выбора ОЗ. Количество ОЗ зависит от выбранного типа устройств
Поле «Типы оптимизации»	Раскрывающийся список со следующими значениями: — «Все значения» – по умолчанию; — «Избыточные»; — «Неиспользуемые»; — «Нулевые Hit Count»; — «Теневые»
Поля страницы «Создание отчета (Правила МЭ)»	
Поле «Тип устройства»	Раскрывающийся список с типами устройств, которые поддерживают отчет «Правила МЭ»
Поле «Объекты защиты»	Является ссылкой на форму выбора ОЗ. Количество ОЗ зависит от выбранного типа устройств
Группа полей «Фильтр содержимого»	
Поле «Действие»	Переключатель: — «Все» – в отчет попадают правила независимо от значения действия правила; — «Разрешить» – в отчет попадают правила, в которых в качестве действия указано Permit; — «Запретить» – в отчет попадают правила, в которых в качестве действия указано Deny
Поле «Протоколы/порты»	Переключатель: — «Не учитывать» – в отчет попадают правила независимо от значения протоколов/портов правила; — «Значение "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 «Источник»	Переключатель: — «Не учитывать» – в отчет попадают правила независимо от значения адреса источника; — «Значение "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.

Поле	Описание
	При выборе переключателя «Значение» появляется дополнительное поле для ввода адресов источников, указанных во включаемом в отчет правиле
Поле «Назначение»	Переключатель: — «Не учитывать» – в отчет попадают правила независимо от значения адреса назначения; — «Значение "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» – в отчет попадают правила в любом статусе; — «Активные» – в отчет попадают активные правила; — «Отключенные» – в отчет попадают отключенные правила
Поле «Дополнительные поля»	Фильтрация уровня приложений для правил МЭ. Переключатель: — «Не учитывать» – при формировании отчета дополнительные данные не учитываются — «Значение» – в отчет попадают правила, содержащие хотя бы одно из указанных в отобразившихся под полем дополнительных полях значение. При выборе переключателя «Значение» появляется дополнительное поле для выбора полей и их значений, по которым в колонках Additional и Comment будет выполнен поиск правил для включения в отчет
Поля страницы «Создание отчета (Центр задач: Заявки)»	
Поле «Атрибут»	Раскрывающийся список возможных атрибутов заявки
Поле «Оператор»	Раскрывающийся список. Значения зависят от выбранного атрибута. Поле становится доступно только после заполнения поля «Атрибут»
Поле «Значение»	Раскрывающийся список. Значения зависят от выбранного атрибута. Поле становится доступно только после заполнения поля «Атрибут»
Поля страницы «Создание отчета (Доступ в сеть: Трафик)»	

Поле	Описание
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 трафику (если вводится количество дней, то допустимые значения от 1 до 1825 – максимальное значение дней хранения событий доступа в сеть)
Поле «Направление трафика»	Раскрывающийся список с типами направлений трафика: — «Входящий» (выбран по умолчанию); — «Исходящий»; — «Оба направления» – превышение трафика рассчитывается по сумме значений входящего и исходящего трафика
Поле «Пороговое значение превышения»	Поле для ввода порогового разрешенного значения трафика в МБ (от 1 до 1000000). Если поле не заполнено, то фильтр по параметру не применяется, выборка выполняется по любым данным трафика
Поле «Причины завершения сеанса»	Раскрывающийся список с возможными причинами завершения сеанса. По умолчанию в списке выбраны все причины (флаг установлен в каждой строке списка). При выбранном параметре «Отсутствует» выборка производится по записям с неуказанной причиной отключения
Поле «Выбрать ОЗ»	Переключатель для выбора правил отбора IP-адресов устройств, от которых посылается запрос RADIUS-серверу при подключении ОЗ: — «Все» – в отчет попадают данные по всем контролируемым комплексом ОЗ; — «Выбрать» – в отчет попадают данные по всем выбранным пользователем в окне списка ОЗ с возможностью «Контроль доступа» (открывается по нажатию ссылки «Выбрать ОЗ», которая отображается при выборе положения переключателя «Выбрать»); — «Задать вручную» – в отчет попадают данные по всем ОЗ, IP-адрес которых удовлетворяет условию, заданному в поле «IP-адрес» (см. ниже)
Поле «IP-адрес»	Поле для ввода диапазона, подсети или хоста, IP-адреса которых должны попасть в отчет

Поле	Описание
Поле «Интерфейсы объектов защиты»	Поле для ввода названий интерфейсов защиты ОЗ, данные по которым должны попасть в отчет (ввод значений выполняется через символ «,»). Если поле не заполнено, то фильтр по параметру не применяется, выборка выполняется по всем интерфейсам
Поле «Выбрать конечную точку»	Переключатель: — «Все» – в отчет попадают данные по всем контролируемым комплексом контрольным точкам; — «Выбрать» – в отчет попадают данные по всем выбранным пользователем в окне списка конечных точек (открывается по нажатию ссылки «Выбрать конечную точку», которая отображается при выборе положения переключателя «Выбрать»); — «Задать вручную» – в отчет попадают данные по всем ОЗ, IP-адрес которых удовлетворяет условию, заданному в поле «IP-адрес» и «MAC-адрес» (см. ниже)
Поле «IP-адрес»	Поле для ввода хотя бы одного диапазона, подсети или хоста, IP-адреса которого должны попасть в отчет. Добавление строк для ввода значений выполняется по кнопке «Добавить» (+), удаление – по кнопке «Удалить» (🗑)
Поле «MAC-адрес»	Поле для ввода хотя бы одного MAC-адреса конечной точки, которая должна попасть в отчет. Добавление строк для ввода значений выполняется по кнопке «Добавить» (+), удаление – по кнопке «Удалить» (🗑). При вводе MAC-адреса допускается: — допустимо неполное совпадение по вводимым символам по любой группе символов; — ввод символа «*» в любой группе символов, обозначающий «любое значение» в группе. При нажатии кнопки «Выполнить» (см. ниже) незаполненные группы заполняются символом "*"
Элементы управления	
Выполнить	При нажатии на кнопку окно создания шаблона отчета закрывается, отображается сформированный отчет
Отменить	При нажатии на кнопку окно создания шаблона отчета закрывается без применения введенных данных

9 Раздел «События»

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

Подразделы раздела:

- «Центр задач» – содержит сводный список событий, связанных с заявками из раздела «Центр задач»,
- «Объекты сети» – содержит информацию о событиях безопасности, произошедших на ОЗ и конечных точках,
- «Аудит» – список событий, связанных с действиями пользователя при работе с комплексом,
- «Доступ в сеть» – содержит список событий, связанных с попытками аутентификации пользователей на оборудовании и с работой пользователей на устройствах,
- «Защита DNS» – содержит список событий, связанных с защитой DNS-трафика
- «Экспорт журналов в файлы формата CSV и XLSX» – предназначен для выгрузки записей из журналов событий в файлы формата .csv и .xlxs.

Списки событий реализованы в виде таблиц.

Над списком событий располагаются:

- поле поиска (Введите запрос для поиска) – для поиска требуемого события по его данным;
- кнопка «Выбрать период» (Выбрать период) – для поиска требуемого события по периоду времени его фиксации;
- кнопка «Фильтр» (Фильтр) – для задания условий фильтрации списка событий по параметрам;
- кнопка «Экспорт» (Экспорт) – для экспорта отфильтрованного списка событий в файл формата CSV или XLSX (по выбору пользователя);
- кнопка «Колонки» ( ) – для настройки состава отображаемых колонок таблицы событий.

Подробнее описание данных в каждом подразделе отдельно приведено ниже в пунктах 9.1 – 9.8.

9.1 Центр задач

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

Подраздел «Центр задач» (рис. 90) содержит сводный список событий, связанных с заявками из раздела «Центр задач».

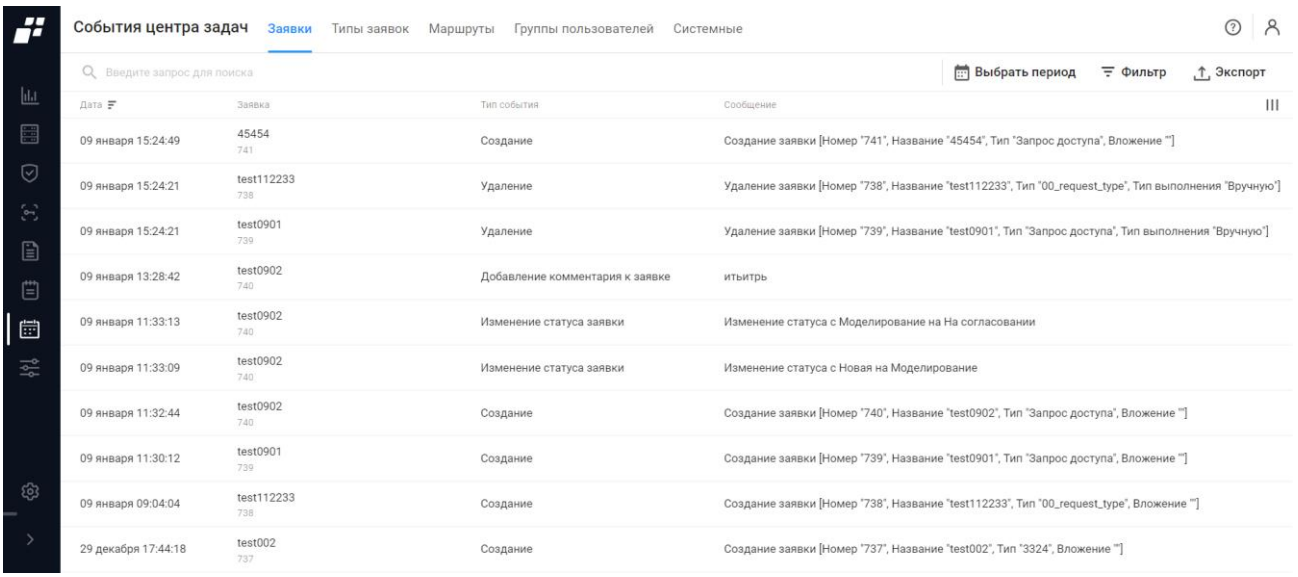


Рисунок 90 – Раздел «События». Подраздел «Центр задач»

Страница подраздела 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;
- «Системные» – содержит события, связанные с изменением настроек заявок, созданных в разделе «Центр задач».

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.

9.2 Объекты сети

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

Подраздел «Объекты сети» (рис. 91) содержит информацию о событиях безопасности, произошедших на ОЗ и конечных точках.

Подраздел содержит вкладки:

— «Объекты защиты»;
— «Конечные точки»;
— «Агенты».

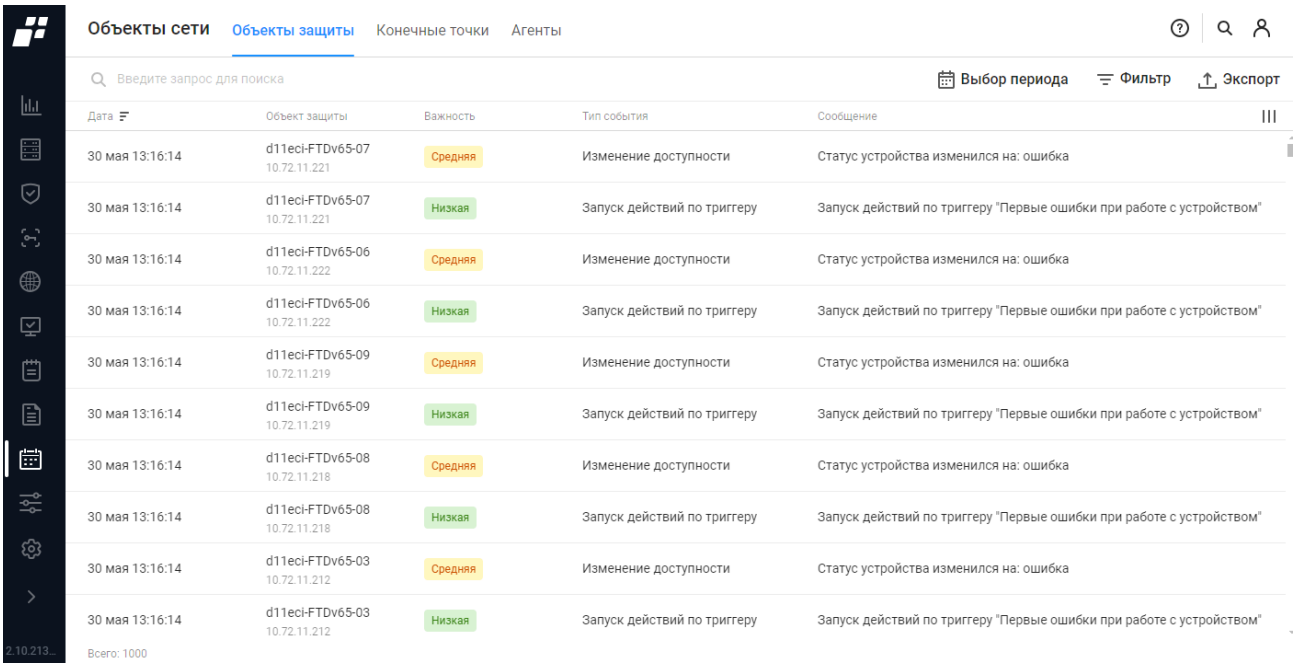


Рисунок 91 – Подраздел «Объекты сети»

9.2.1 Вкладка «Объекты защиты»

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

Вкладка «Объекты защиты» содержит сводный список событий безопасности, полученных от ОЗ с возможностями «Контроль устройств», «Контроль доступа» и «Потоки данных» (см. рис. 91).

Для каждой записи списка отображаются следующие данные:

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

9.2.2 Вкладка «Конечные точки»

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

Вкладка «Конечные точки» содержит сводный список событий безопасности, полученных от конечных точек (рис. 92).

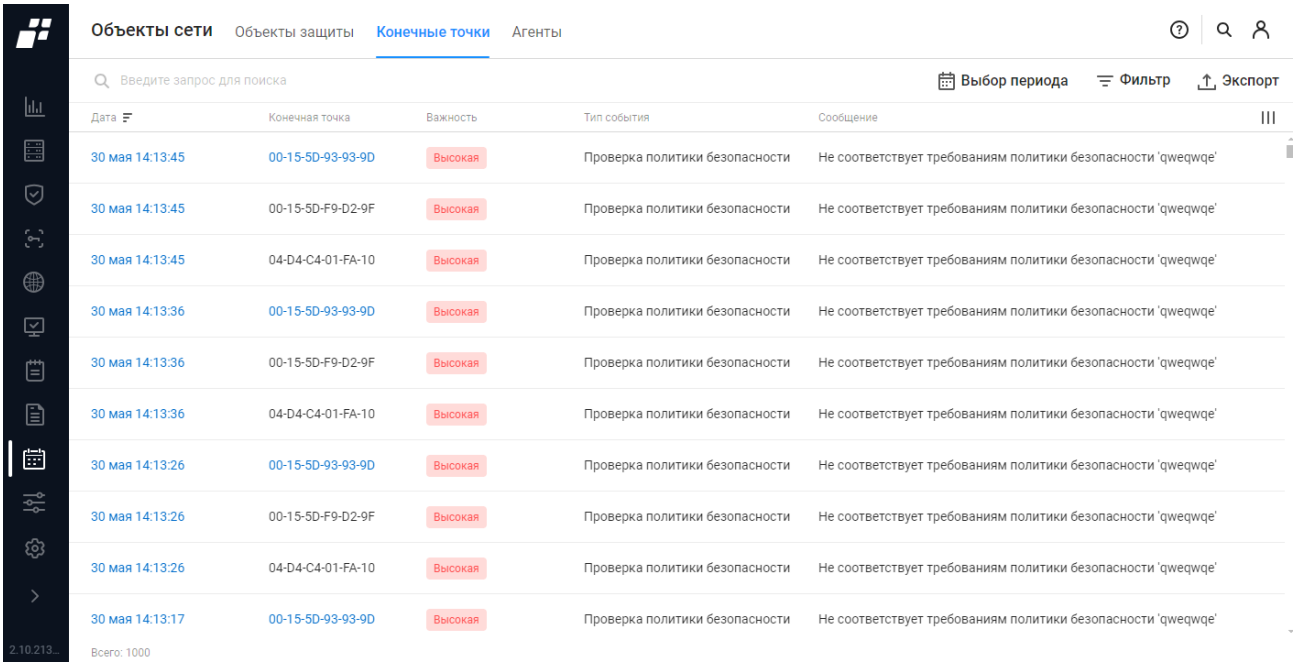


Рисунок 92 – Вкладка «Конечные точки»

Для каждой записи списка отображаются следующие данные:

- дата и время фиксации события. Является ссылкой, при переходе по которой открывается страница с информацией о результатах проверок политик безопасности конечной точки;
- MAC-адрес конечной точки. Является ссылкой, при переходе по которой открывается страница с описанием свойств и атрибутов конечной точки;
- важность зафиксированного события:
  - «Низкая»;
  - «Средняя»;
  - «Высокая».

— тип события;
— краткое описание события.

9.2.3 Вкладка «Агенты»

Вкладка «Агенты» доступна пользователю для работы при наличии лицензии на функциональный модуль «Efros NAC».

Вкладка «Агенты» содержит сводный список событий безопасности, полученных от агентов (рис. 92).

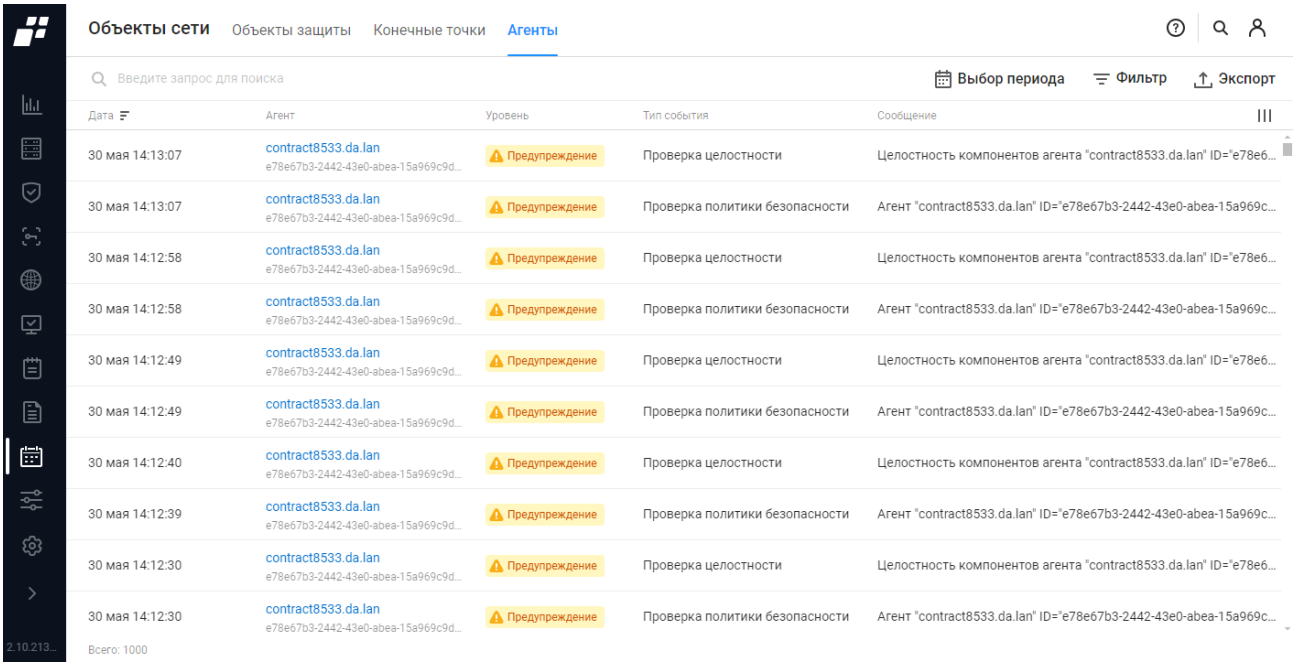


Рисунок 93 – Вкладка «Агенты»

Для каждой записи списка отображаются следующие данные:

— дата и время фиксации события;
— название и идентификатор агента. Является ссылкой, при переходе по которой открывается страница просмотра состояния агента;
— уровень критичности события:
  - «Инфо» – информационное сообщение;
  - «Предупреждение» – предупреждение, не влияет на логику работы приложения;
  - «Ошибка» – непредвиденное поведение.
— тип события;
— краткое описание события.

9.3 Аудит

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

Подраздел «Аудит» содержит список событий, связанных с действиями пользователя при работе с комплексом (рис. 94).

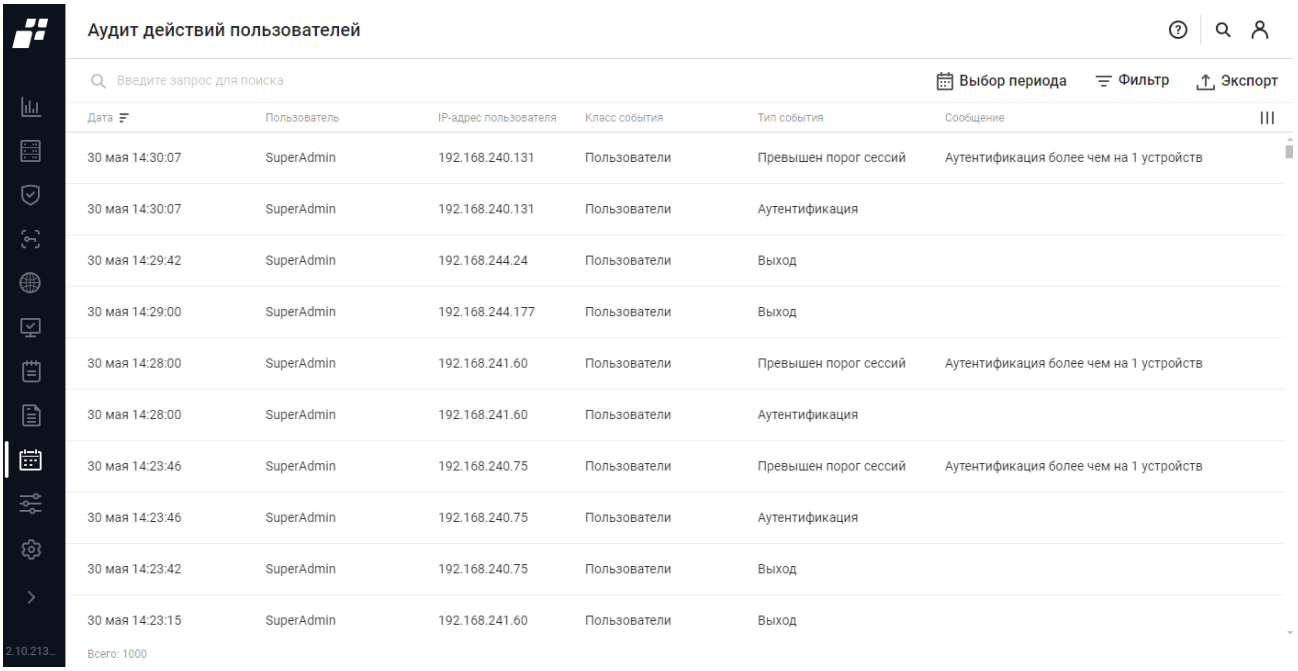


Рисунок 94 – Подраздел «Аудит»

Для каждой записи списка отображаются следующие данные:

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

9.4 Доступ в сеть

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

Подраздел «Доступ в сеть» содержит список событий, связанных с попытками аутентификации пользователей на оборудовании и с работой пользователей на устройствах (рис. 95).

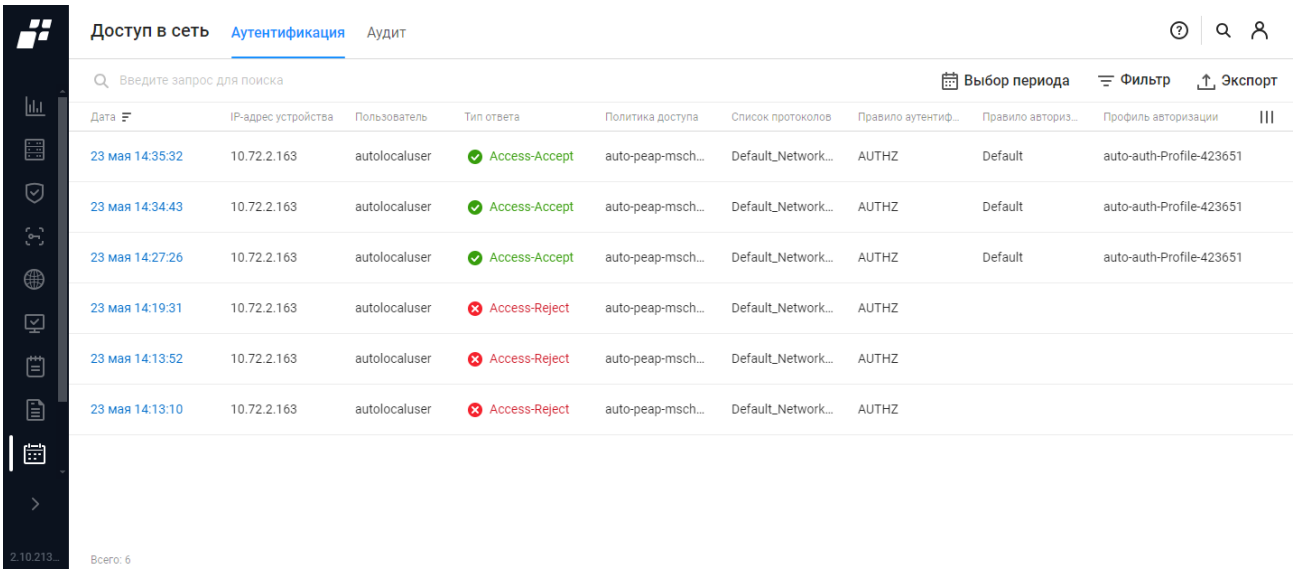


Рисунок 95 – Подраздел «Доступ в сеть»

Страница содержит вкладки:

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

Во вкладке «Аутентификация» дата является ссылкой, при выборе которой открывается окно просмотра данных трассировки запроса на доступ в сеть (рис. 96). В окне отображается результат обработки запроса («Доступ предоставлен» или «Отказ в доступе») и следующие данные:

- IP-адрес устройства, взаимодействующего с сервером аутентификации;
- название интерфейса взаимодействующего с сервером аутентификации устройства, к которому подключен пользователь, запрашивающий доступ в сеть. Если нет данных, то поле не отображается;
- имя пользователя или MAC-адрес устройства, запрашивающего доступ в сеть;
- название сработавшей политики доступа в сеть. Если политика доступа существует (не удалена), то является ссылкой для перехода на страницу карточки политики. В случае отсутствия данных (политика не сработала) отображается текст «Отсутствует»;
- название сработавшего правила аутентификации. В случае отсутствия данных (правило не сработало) отображается текст «Отсутствует»;
- название сработавшего правила авторизации. В случае отсутствия данных (правило не сработало) отображается текст «Отсутствует»
- название профиля авторизации, который был назначен в результате срабатывания правила авторизации. Если профиль авторизации существует (не удален), то является ссылкой для перехода на страницу карточки профиля. В случае отсутствия данных отображается текст «Отсутствует». Справа

расположена кнопка «Просмотреть» (👁), по нажатию которой открывается окно предпросмотра с данными: тип доступа и параметры профиля авторизации (отображаются только параметры, для которых в профиле заданы значения);

— общее имя корневого сертификата. В случае отсутствия данных отображается текст «Отсутствует». Справа расположена кнопка «Просмотреть» (👁), по нажатию которой открывается окно предпросмотра с данными корневого сертификата;

— общее имя клиентского сертификата. В случае отсутствия данных отображается текст «Отсутствует». Справа расположена кнопка «Просмотреть» (👁), по нажатию которой открывается окно предпросмотра с данными клиентского сертификата;

— данные трассировки запроса на доступ в сеть или доступ на оборудование

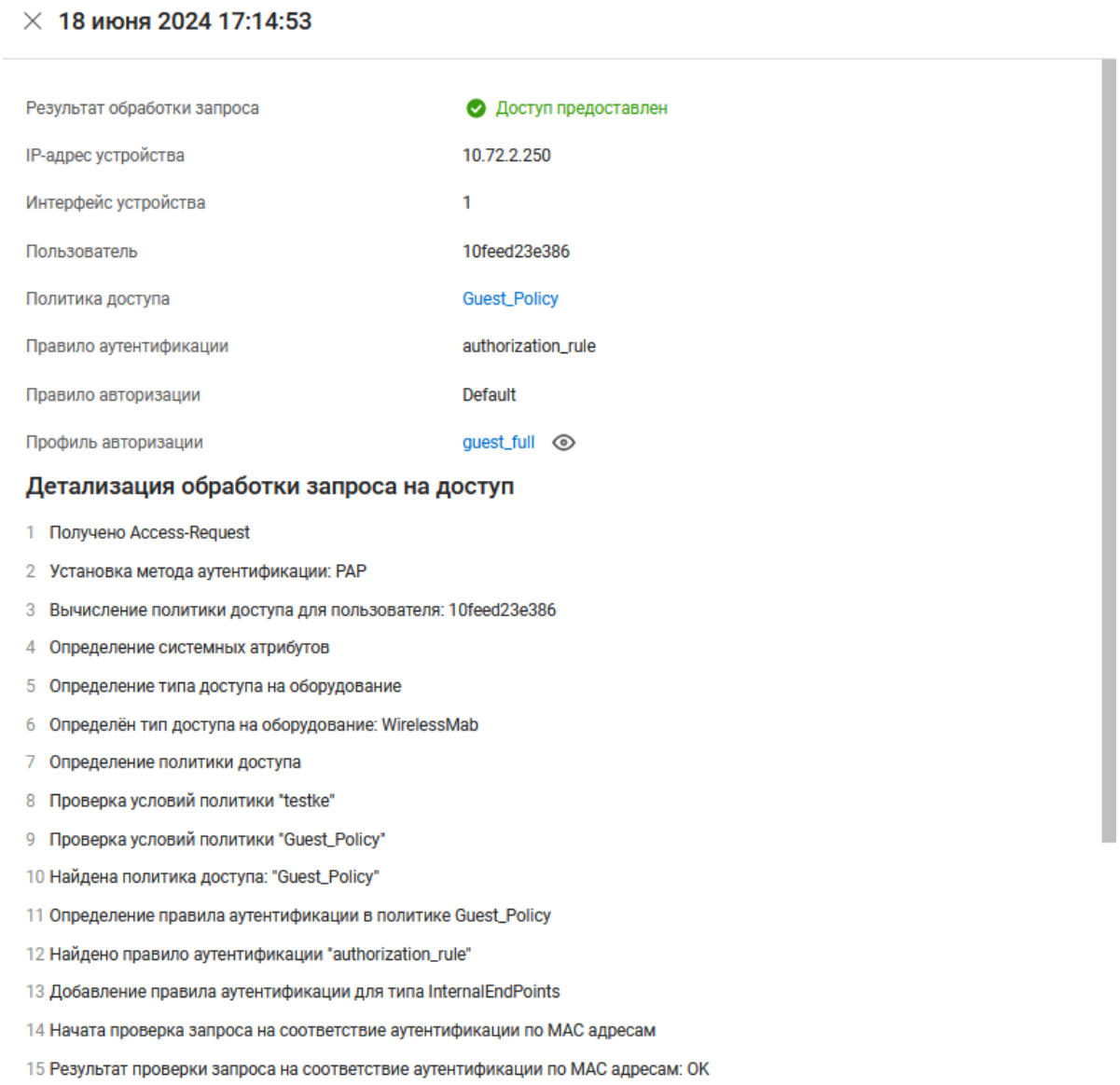


Рисунок 96 – Окно просмотра данных трассировки запроса на доступ в сеть

Названия политики доступа и профиля авторизации отображаются на момент получения события доступа в сеть. В случае, если политика или профиль впоследствии были переименованы или удалены, то название в окне предпросмотра не изменяется/не очищается.

9.5 Доступ на оборудование

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

Подраздел «Доступ на оборудование» содержит список событий, связанных с попытками аутентификации сетевых пользователей на оборудовании, авторизации и с работой на устройствах (рис. 97).

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.

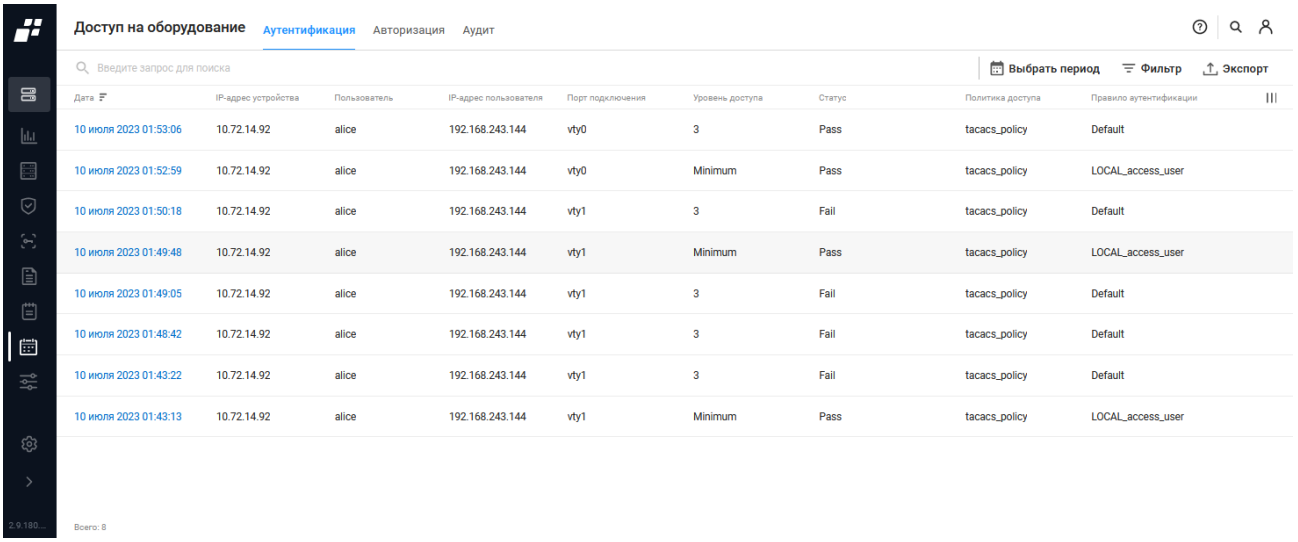


Рисунок 97 – Подраздел «Доступ на оборудование»

9.6 Системные события

Подраздел «Системные события» содержит список общих системных событий комплекса, системных событий возможностей «Контроль доступа» и «Контроль устройств» (рис. 98).

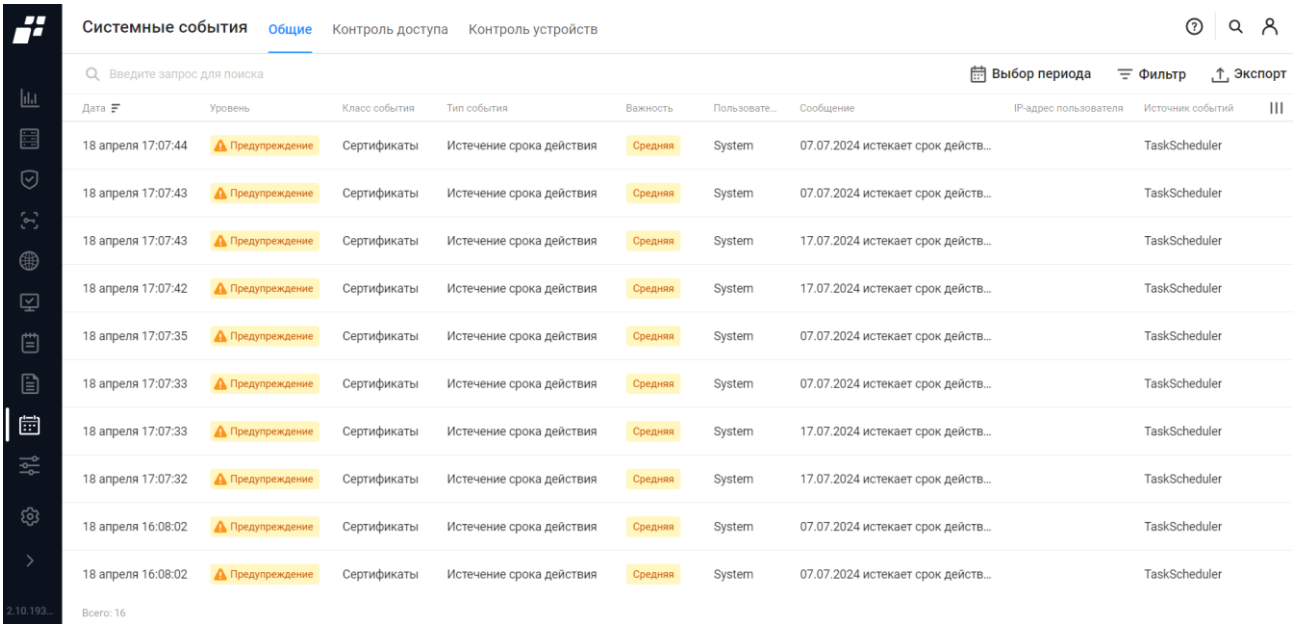


Рисунок 98 – Подраздел «Системные события»

Страница содержит вкладки:

- «Общие» – общие системные события ПК «Efros DO»;
- «Контроль доступа» – системные события модуля «Efros NAC»;
- «Контроль устройств» – системные события модулей «Efros NA», «Efros VC», «Efros FA» и «Efros ICC».

9.6.1 Вкладка «Общие»

На вкладке «Общие» список событий реализован в виде таблицы (см. рис. 98). Для каждой записи списка отображаются следующие данные:

- дата и время фиксации события;
- уровень критичности события:
  - «Инфо» – информационное сообщение;
  - «Предупреждение» – предупреждение, не влияет на логику работы приложения;
  - «Ошибка» – непредвиденное поведение.
- класс события;
- тип события;
- важность:
  - «Низкая»;
  - «Средняя»;

- «Высокая».

— пользователь – имя пользователя ПК «Efros DO» или «System»;
— сообщение – краткое описание события;
— IP-адрес пользователя (по умолчанию колонка скрыта);
— источник события – (по умолчанию колонка скрыта).

9.6.2 Вкладка «Контроль доступа»

Вкладка «Контроль доступа» доступна пользователю при наличии лицензии на функциональный модуль «Efros NAC».

На вкладке «Контроль доступа» список системных событий реализован в виде таблицы (рис. 99). Наименование колонок записей списка аналогичны колонкам вкладки «Общие» (см. п. 9.6.1).

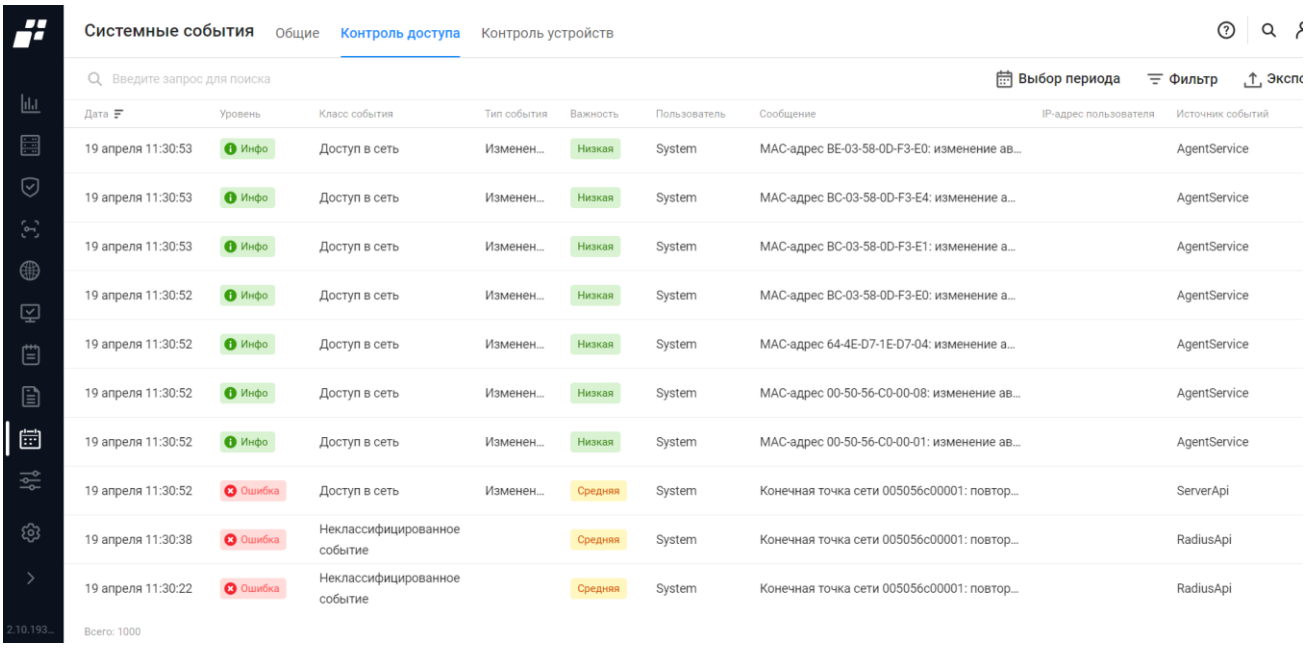


Рисунок 99 – Вкладка «Контроль доступа»

9.6.3 Вкладка «Контроль устройств»

Вкладка «Контроль устройств» доступна пользователю при наличии лицензии хотя бы на один из функциональных модулей: «Efros NA», «Efros VC», «Efros FA» или «Efros ICC».

На вкладке «Контроль устройств» список системных событий реализован в виде таблицы (рис. 100).

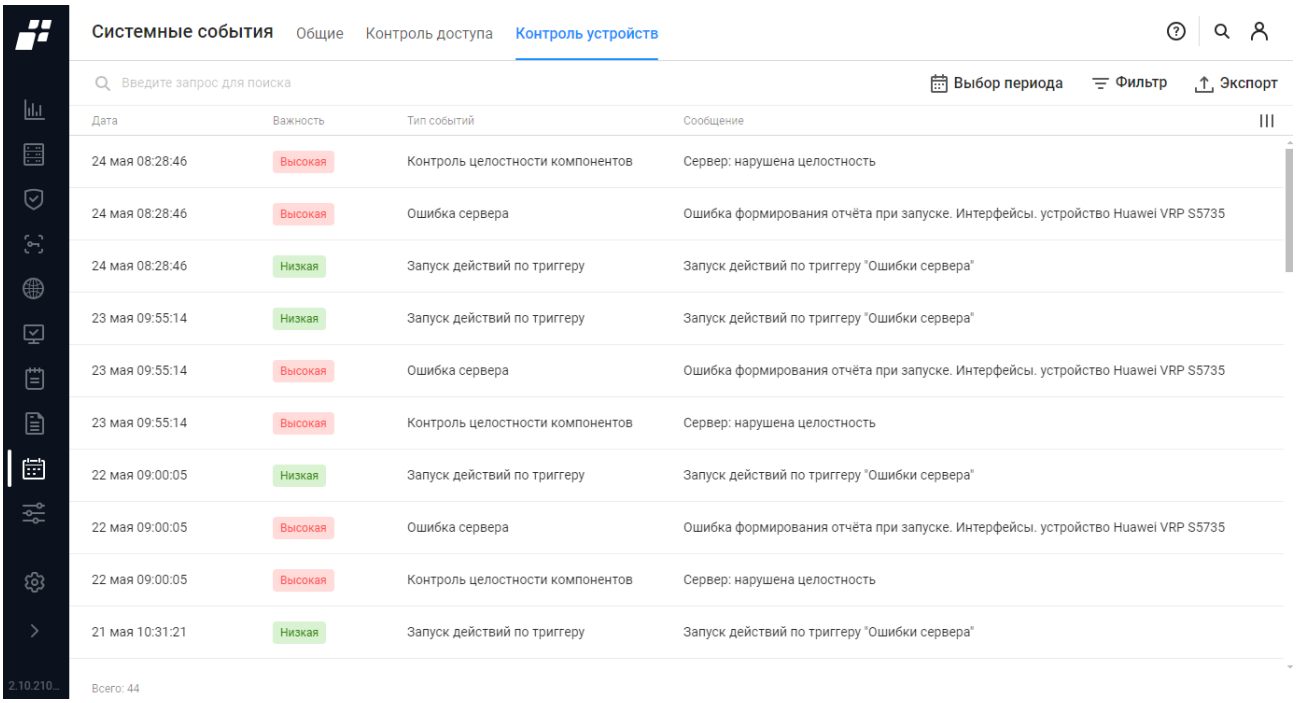


Рисунок 100 – Вкладка «Контроль устройств»

Для каждой записи списка отображаются следующие данные:

- дата и время фиксации события;
- уровень важности события:
  - «Высокое»;
  - «Среднее»;
  - «Низкое».
- тип события;
- сообщение – краткое описание события.

9.7 Защита DNS

Подраздел «Защита DNS» доступен пользователю для работы при наличии лицензии на функциональный модуль «Efros DNS».

Подраздел «Защита DNS» содержит список событий, связанных с защитой DNS-трафика (рис. 101).

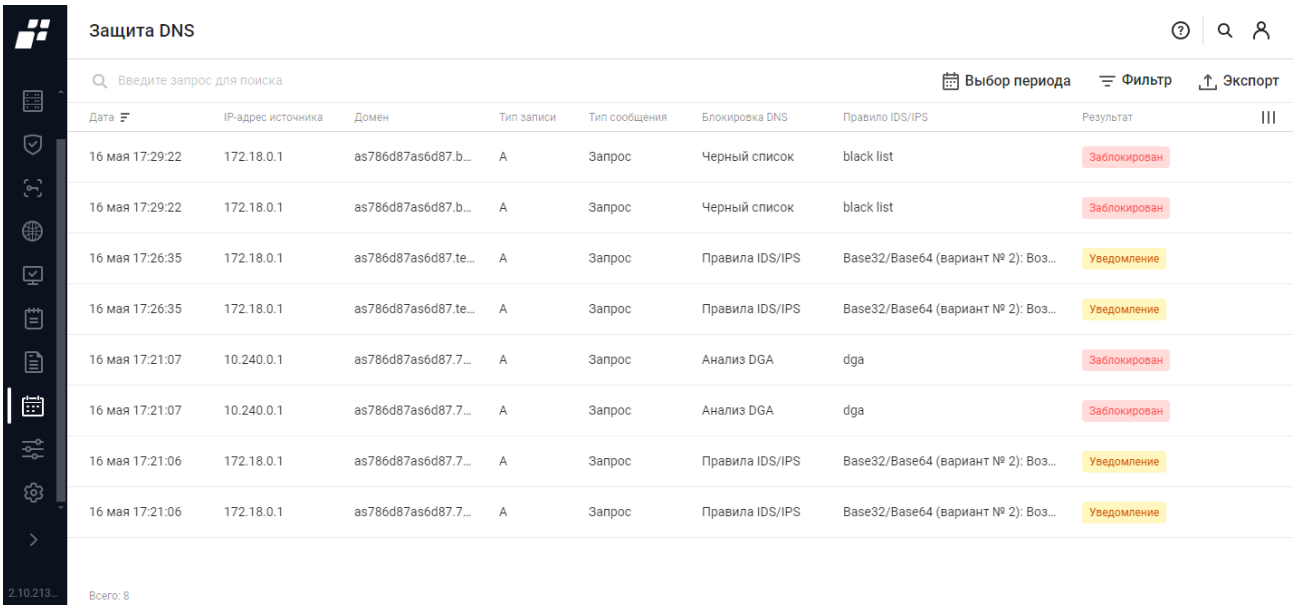


Рисунок 101 – Подраздел «Защита DNS»

Для каждой записи списка отображаются следующие данные:

- дата и время фиксации события;
- IP-адрес источника;
- домен – запрашиваемое доменное имя;
- тип записи:
  - «A» – адресная запись, соответствие между именем и IP-адресом;
  - «AAAA» – адрес в формате IPv6;
  - «NS» – адрес узла, отвечающего за доменную зону, важна для функционирования самой системы доменных имен;
  - «PTR» – соответствие адреса – имени, является обратным соответствием для A и AAAA;
  - «SOA» – указание на авторитетность информации, используется для указания на новую зону;
  - «TXT» – запись произвольных двоичных данных.
- тип сообщения (запрос/ответ);
- блокировка DNS одним из модулей: «Черный список», «Правила IDS/IPS», «Анализ DGA», «Изменение регистра DNS-запроса»;
- правило IDS/IPS – название правила, в результате которого был заблокирован DNS-трафик;
- результат:
  - «Уведомление»;
  - «Заблокирован».

9.8 Экспорт журналов в файлы формата CSV и XLSX

В ПК «Efros DO» реализована функция выгрузки записей из журналов событий в файлы формата .csv и .xlxs. 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) и в раскрывающемся списке выбрать формат файла для загрузки .csv или .xlxs (рис. 102).

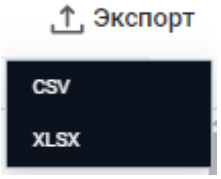


Рисунок 102 – Выбор формата файла для загрузки

После завершения процесса выгрузки записей файл сохранится на локальной ПЭВМ пользователя, 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.

10 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.

10.1 Пользователи

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

Страница подраздела «Пользователи» (рис. 103) содержит вкладки:

- «Пользователи» – список групп пользователей и входящих в них пользователей, зарегистрированных в комплексе. Вкладка активна по умолчанию;
- «Роли» – список ролей для реализации ролевого метода управления доступом к комплексу;
- «Настройки безопасности» – параметры для настройки парольной политики;
- «Active Directory» – список созданных соединений к источнику данных Active Directory.

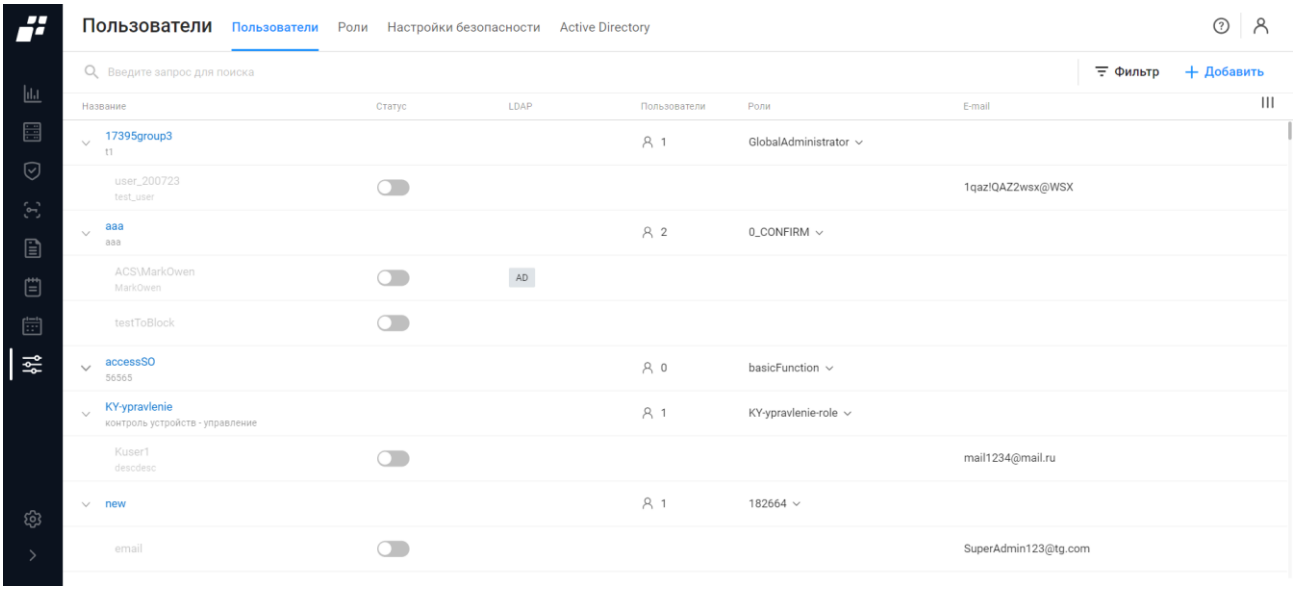


Рисунок 103 – Раздел «Администрирование», подраздел «Пользователи»

10.1.1 Вкладка «Пользователи»

На вкладке «Пользователи» 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);
- кнопка «Фильтр» (Фильтр);
- кнопка «Добавить (+ Добавить);
- кнопка «Колонки» ( ).

При выборе строки с пользователем слева в строке отображается кнопка « » для перемещения пользователя из одной группы в другую. После перемещения строки пользователя в другую группу отображается сообщение об изменении группы пользователя.

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

- «Изменить пароль» ( );
- «Удалить» ( ).

При выборе строки с группой пользователей в правом углу строки появляется кнопка «Удалить» ( ).

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

10.1.1.1 Создание пользователя

Для создания доменного типа пользователя предварительно необходимо произвести настройку подключения к источнику данных Active Directory (подробнее см. п. 0).

Для создания пользователя необходимо выполнить следующие действия:

1) Нажать на странице «Пользователи» кнопку «Добавить» (+ Добавить).
2) В раскрывшемся меню выбрать пункт «Пользователь» (рис. 104).

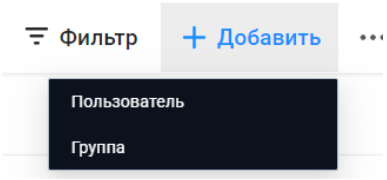


Рисунок 104 – Выбор пункта «Пользователь»

3) Откроется страница «Создание пользователя» (на рис. 105 приведена страница создания пользователя локального типа). Состав и описание полей страницы создания пользователя приведены в таблице 32.

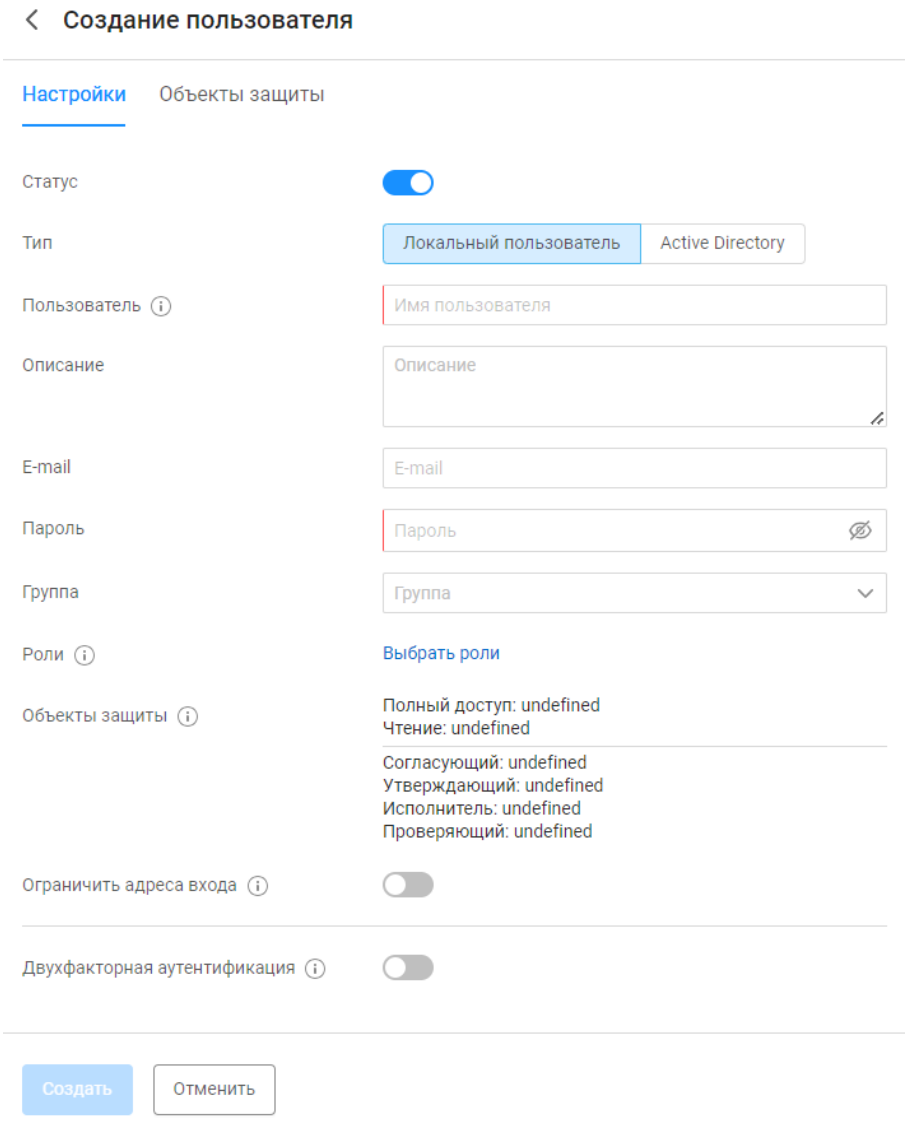


Рисунок 105 – Страница «Создание пользователя». Добавление локального типа пользователя

Таблица 32 – Состав и описание полей страницы создания пользователя

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 для выбора типа добавляемого пользователя. Содержит значения: «Локальный пользователь» и «Active Directory»[9]
Поле «Пользователь»	Для локального типа пользователя – текстовое поле для ввода логина пользователя. Параметры ввода текста: от 1 до 32 символов. Дополнительные символы: буквы латинского алфавита, цифры, «_», «–» Для доменного типа пользователя – раскрывающийся список для выбора логина требуемого пользователя
Поле «Описание»	Для локального типа пользователя – текстовое поле для ввода описания пользователя. Параметры ввода текста: от 1 до 250 любых символов. Для доменного типа пользователя – поле заполняется автоматически после заполнения поля «Пользователь»
Поле «E-mail»	Для локального типа пользователя – в поле указывается почтовый адрес пользователя для привязки к почте аккаунта пользователя комплекса. Для доменного типа пользователя – поле заполняется автоматически после заполнения поля «Пользователь»
Поле «Пароль»	Поле доступно только для локального типа пользователя. Текстовое поле для ввода пароля пользователя. Пароль должен соответствовать требованиям, заданным при настройке парольной политики (подробное описание приведено в п. 10.1.3). При вводе символы пароля заменяются знаком «●». Для просмотра введенного значения необходимо нажать в поле ввода кнопку «Просмотреть» ( )
Поле «Группа»	Раскрывающийся список для выбора группы пользователей, в

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

Поле	Описание
	которую будет входить пользователь. Для отмены вхождения пользователя в группу – навести курсор на поле и нажать отобразившуюся в правой части поля кнопку «Очистить» ( )
Поле «Роли»	Является ссылкой. Позволяет выбрать в окне «Выбор ролей» необходимую роль для пользователя (для доступа к различным разделам комплекса). Для выбора необходимо в окне «Выбор ролей» установить флаг в полях требуемых ролей и нажать кнопку «Выбрать» При вхождении пользователя в группу, ему назначаются роли и привилегии группы. Список назначенных ролей и привилегий доступен только для просмотра
Поле «Объекты защиты»	Поле для выбора ОЗ, которые доступны пользователю. Поле доступно только после создания пользователя (см. п. 10.1.1.2). При вхождении пользователя в группу, доступны объекты защиты группы
Переключатель «Ограничить адреса входа»	Ограничение возможности подключения пользователя к серверу «ПК Efros DO» только с адресов, указанных в поле «Разрешенные IP-адреса» (см. ниже). При вхождении пользователя в группу, действуют ограничения группы, переключатель не активен
Поле «Разрешенные IP-адреса»	Поле отображается только при включении переключателя «Ограничить адреса входа». Раскрывающийся список для выбора подсети, диапазона или хоста. Необходимо ввести данные разрешенных адресов входа. При необходимости добавления нескольких областей разрешенных адресов входа – нажать кнопку «+», при необходимости удалить – нажать кнопку «🗑»
Переключатель «Двухфакторная аутентификация»	Включение прохождения пользователем двухфакторной аутентификации при авторизации в ПК «Efros DO» Предварительно необходимо произвести настройку внешнего сервера RADIUS, настройку системы внешней аутентификации и включить возможность применения

Поле	Описание
	двухфакторной аутентификации на вкладке «Настройки безопасности» (см. п. 10.1.3)
Поле «Система аутентификации»*	Раскрывающийся список для выбора наименования требуемой внешней системы аутентификации
Поле «Метод аутентификации»*	Раскрывающийся список для выбора наименования требуемого метода аутентификации
Поле «Идентификатор пользователя»*	Текстовое поле для ввода идентификатора (имя) пользователя в системе аутентификации, если отлично от текущего. При заполнении поля, идентификатор будет использован при отправке запроса на проверку второго фактора в систему аутентификации. Параметры ввода текста: от 1 до 50 любых символов
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
* Поле отображается только при включении переключателя «Двухфакторная аутентификация»	

4) Заполнить поля страницы данными пользователя.
5) Нажать кнопку «Создать».
6) Назначить, при необходимости, пользователю права доступа к ОЗ и роли для работы с заявками (ответственность) в соответствии с п. 10.1.1.2.

10.1.1.2 Редактирование пользователя

Для редактирования пользователя необходимо выполнить следующие действия:

1) Нажать на странице вкладки «Пользователи» (см. рис. 103) на запись созданного пользователя.
2) Редактирование пользователя на вкладке «Настройки» аналогично созданию пользователя (см. п. 10.1.1.1)
3) Перейти на вкладку «Объекты защиты».
4) Для настройки прав доступа на ОЗ – выбрать установкой флагов требуемые ОЗ и нажать над таблицей ОЗ кнопку « Права доступа » (рис. 106). В раскрывшемся списке выбрать необходимые права доступа – «Отсутствуют», «Чтение», «Полный» или «Наследовать».

Во вкладке «Объекты защиты» пользователю с привилегией «Пользователи / Пользователи - Управление» в списке ОЗ доступны все подключенные к комплексу ОЗ.

Настройка ответственности пользователя необходима для последующего применения в заявках раздела «Центр задач».

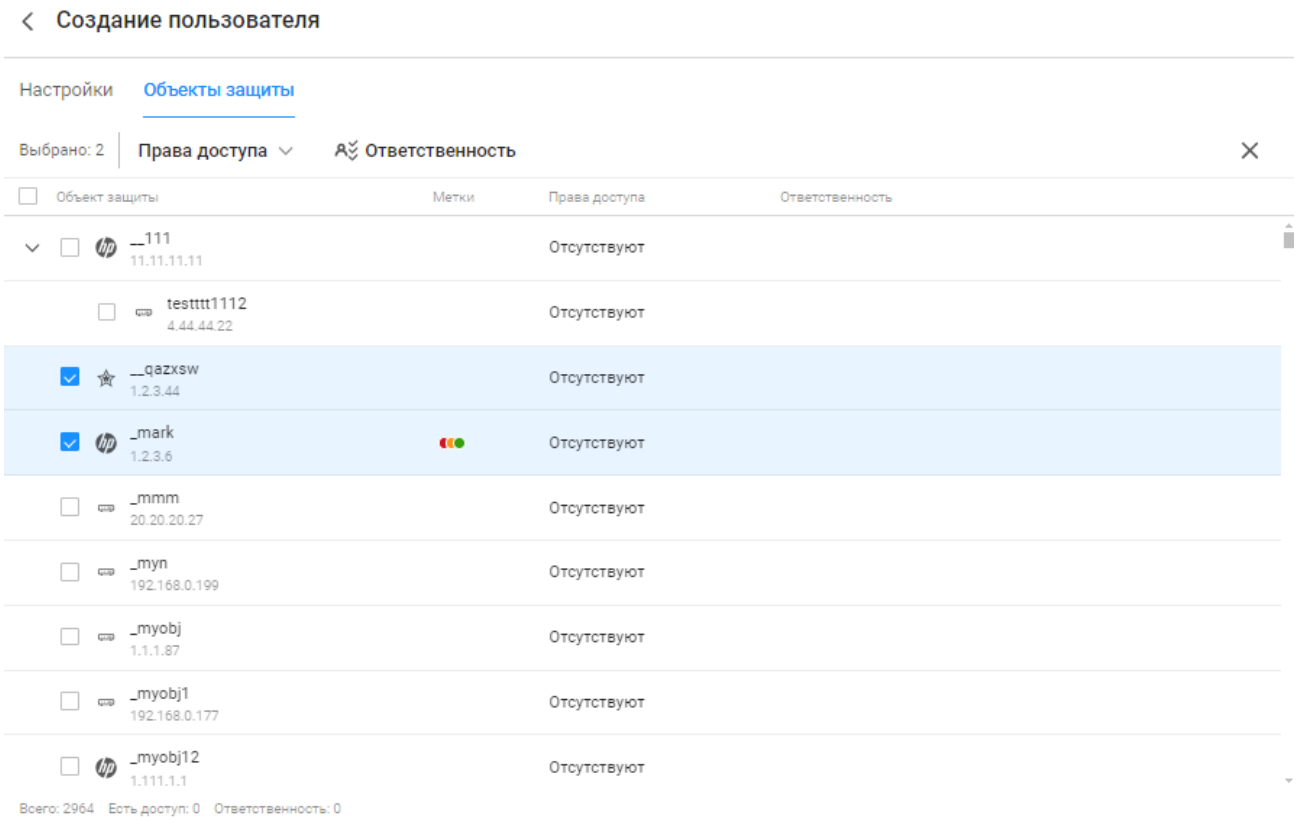


Рисунок 106 – Страница «Создание пользователя», вкладка «Объекты защиты»

5) Настроить ответственность пользователя, для чего выбрать установкой флагов требуемые ОЗ и нажать над таблицей ОЗ кнопку « Ответственность ». Откроется окно настройки ответственности пользователя (рис. 107).

6) Выбрать установкой флага требуемые типы ответственности и нажать кнопку «Назначить».

Для объектов защиты с правами доступа «Чтение» или «Полный доступ» ответственность будет переопределена на выбранный список значений.

При назначении ответственности без выбора значений, будет установлено «Отсутствует».

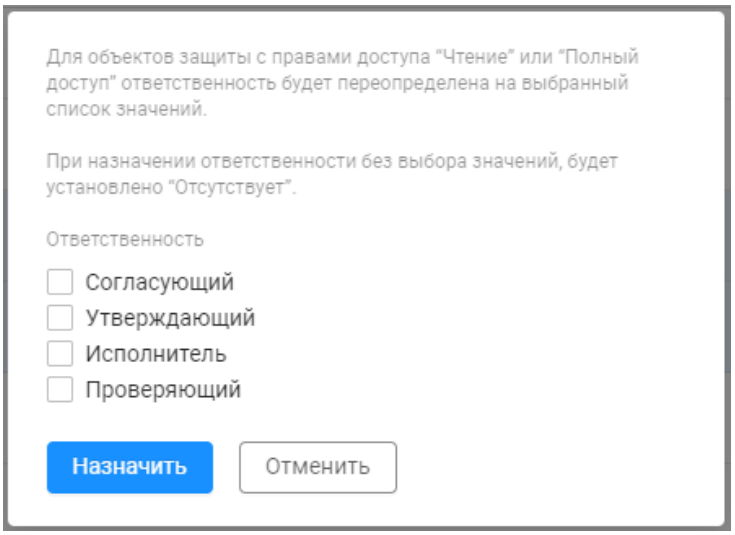


Рисунок 107 – Окно настройки ответственности пользователя

7) Вернуться на вкладку «Настройки» проверить значения поля «Объекты защиты» (рис. 108) и нажать кнопку «Сохранить».

Полный доступ: 1267
Чтение: 4

Согласующий: 2
Утверждающий: 4
Исполнитель: 5
Проверяющий: 2

Рисунок 108 – Назначенные права доступа на ОЗ и ответственность пользователей

10.1.1.3 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 кнопку «Добавить» (+ Добавить).
2) В раскрывшемся меню выбрать пункт «Группу» (см. рис. 104).
3) Откроется страница «Создание группы» (рис. 109). Заполнить странице необходимыми параметрами и нажать кнопку «Создать». Состав и описание полей страницы приведены в таблице 33.
4) Назначить, при необходимости, группе права доступа к ОЗ и роли пользователей для работы с заявками (ответственность). Правила назначения аналогичны правилам для пользователей (см. п. 10.1.1.2).

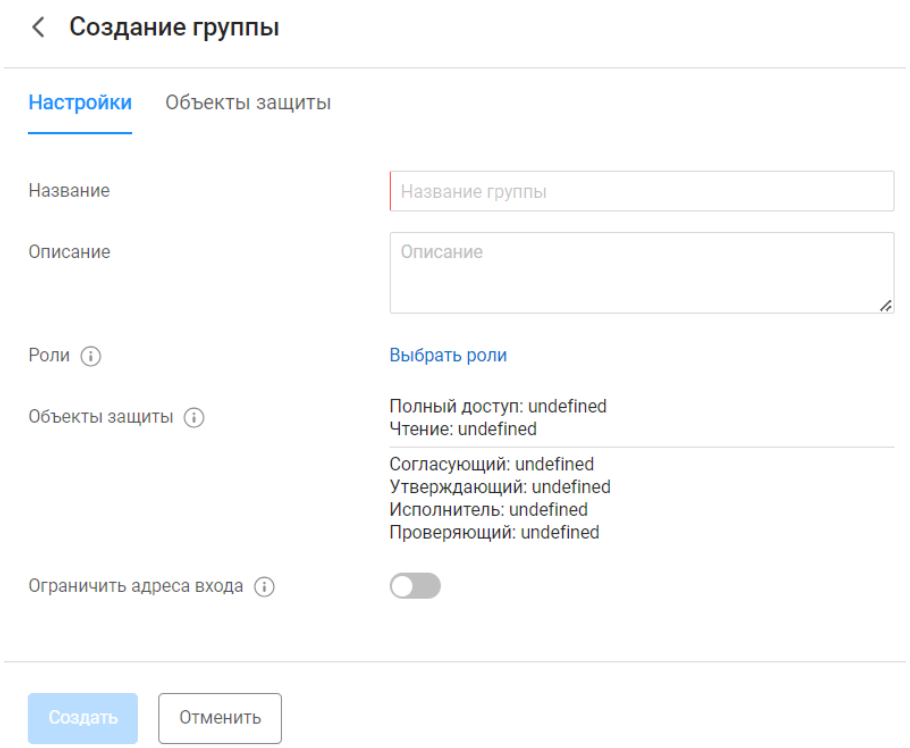


Рисунок 109 – Страница «Создание группы»

Таблица 33 – 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» необходимую роль для группы пользователей (для доступа к различным разделам комплекса). Для выбора необходимо в окне «Выбор ролей» установить флаг в полях требуемых ролей и нажать кнопку «Выбрать»
Поле «Объекты защиты»	Поле для выбора ОЗ, которые доступны пользователю. Поле доступно только после создания группы
Переключатель «Ограничить адреса входа»	Ограничение возможности подключения пользователя к серверу «ПК Efros DO» только с адресов, указанных в поле «Разрешенные IP-адреса» (см. ниже)
Поле «Разрешенные IP-адреса»	Поле отображается только при включении переключателя «Ограничить адреса входа». Раскрывающийся список для выбора подсети, диапазона или хоста. Необходимо ввести данные разрешенных адресов

Поле	Описание
	входа. При необходимости добавления нескольких областей разрешенных адресов входа – нажать кнопку «+», при необходимости удалить – нажать кнопку «🗑»
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

10.1.2 Вкладка «Роли»

Вкладка «Роли» содержит список ролей для реализации ролевого метода управления доступом к комплексу (рис. 110). Доступ к функциональности комплекса определяется наличием привилегии доступа к конкретной функции каждого подключаемого модуля.

Для редактирования доступны все роли, кроме «GlobalAdministrator».

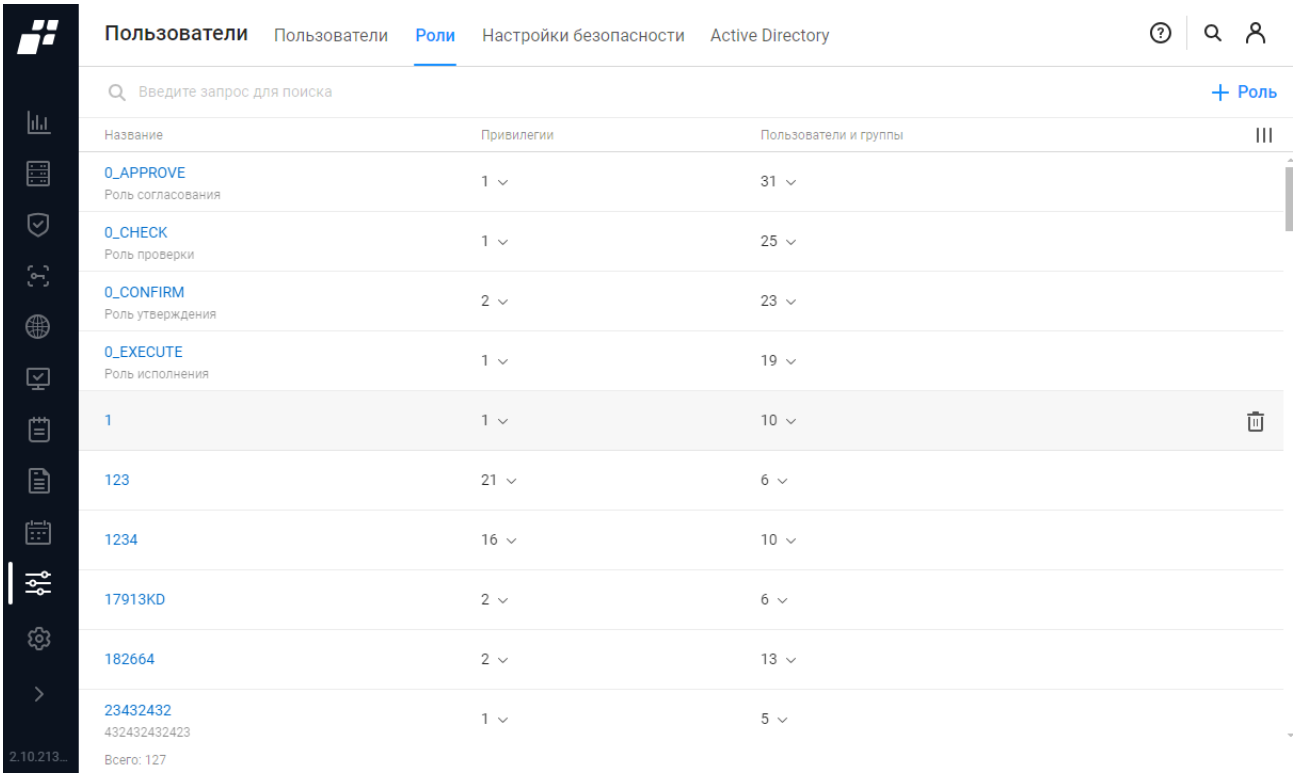


Рисунок 110 – Вкладка «Роли»

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

- название роли. Позволяет перейти на страницу редактирования роли;
- описание роли;
- количество назначенных привилегий роли. Является раскрывающимся списком с перечнем привилегий. Привилегии сгруппированы по категориям и для каждой указан уровень доступа «Просмотр» или «Управление»;
- количество пользователей и групп пользователей с данной ролью. Является раскрывающимся списком со списком групп и входящих в них пользователей (пользователи в статусе «Активный» отмечены пиктограммой «●»).

Над списком ролей располагаются:

- поле поиска (Введите запрос для поиска);
- кнопка «Роль» (+ Роль) для перехода в окно создания новой роли пользователя.

При выборе строки роли в правом углу строки появляется кнопка «Удалить» ( ).

10.1.2.1 Создание роли

Для создания новой роли необходимо выполнить следующие действия:

1) Нажать кнопку «Роль» (+ Роль).
2) Откроется страница «Создание роли пользователя» (рис. 111). Необходимо заполнить поля требуемыми параметрами и нажать кнопку «Создать». Состав и описание полей страницы приведены в таблице Таблица 34.

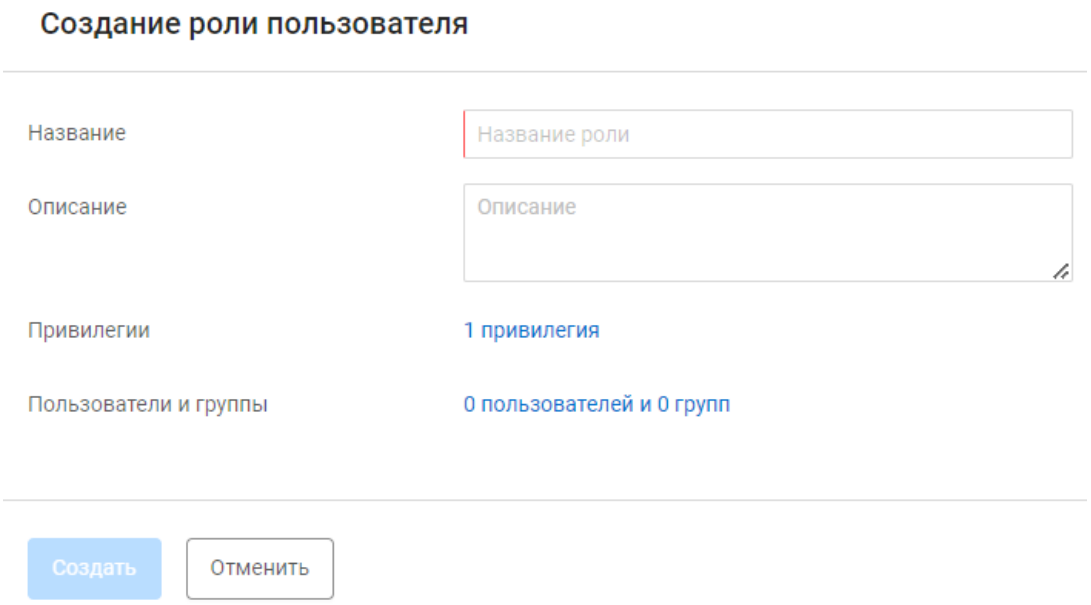


Рисунок 111 – Страница «Создание роли пользователя»

Таблица 34 – 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»	Является ссылкой. По умолчанию поле содержит ссылку «1 привилегия». Для добавления новых привилегий необходимо нажать на ссылку, в открывшемся окне со списком выбрать установкой флагов требуемые привилегии, назначить им уровень доступа «Просмотр» (только просмотр данных) или «Управление» (внесение изменений в данные) и нажать кнопку «Выбрать». Текст ссылки изменится на количество выбранных привилегий
Поле «Пользователи и группы»	Является ссылкой. По умолчанию поле содержит ссылку «0 пользователей и 0 групп». Для добавления пользователей необходимо нажать на ссылку, в открывшемся окне со списком пользователей, зарегистрированных в комплексе, установкой флагов требуемые группы пользователей и отдельных пользователей и нажать кнопку «Выбрать». Текст ссылки изменится на количество выбранных пользователей и групп пользователей
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

10.1.3 Вкладка «Настройки безопасности»

Для настройки безопасности необходимо выполнить следующие действия:

1) Перейти на вкладку «Настройки безопасности» (рис. 112). Состав и описание полей страницы приведены в таблице 35.
2) Ввести в поля страницы требуемые значения.
3) Нажать кнопку «Сохранить». После чего введенные параметры будут сохранены в БД ПК «Efros DO» и будут применяться при авторизации пользователей и при смене пароля.

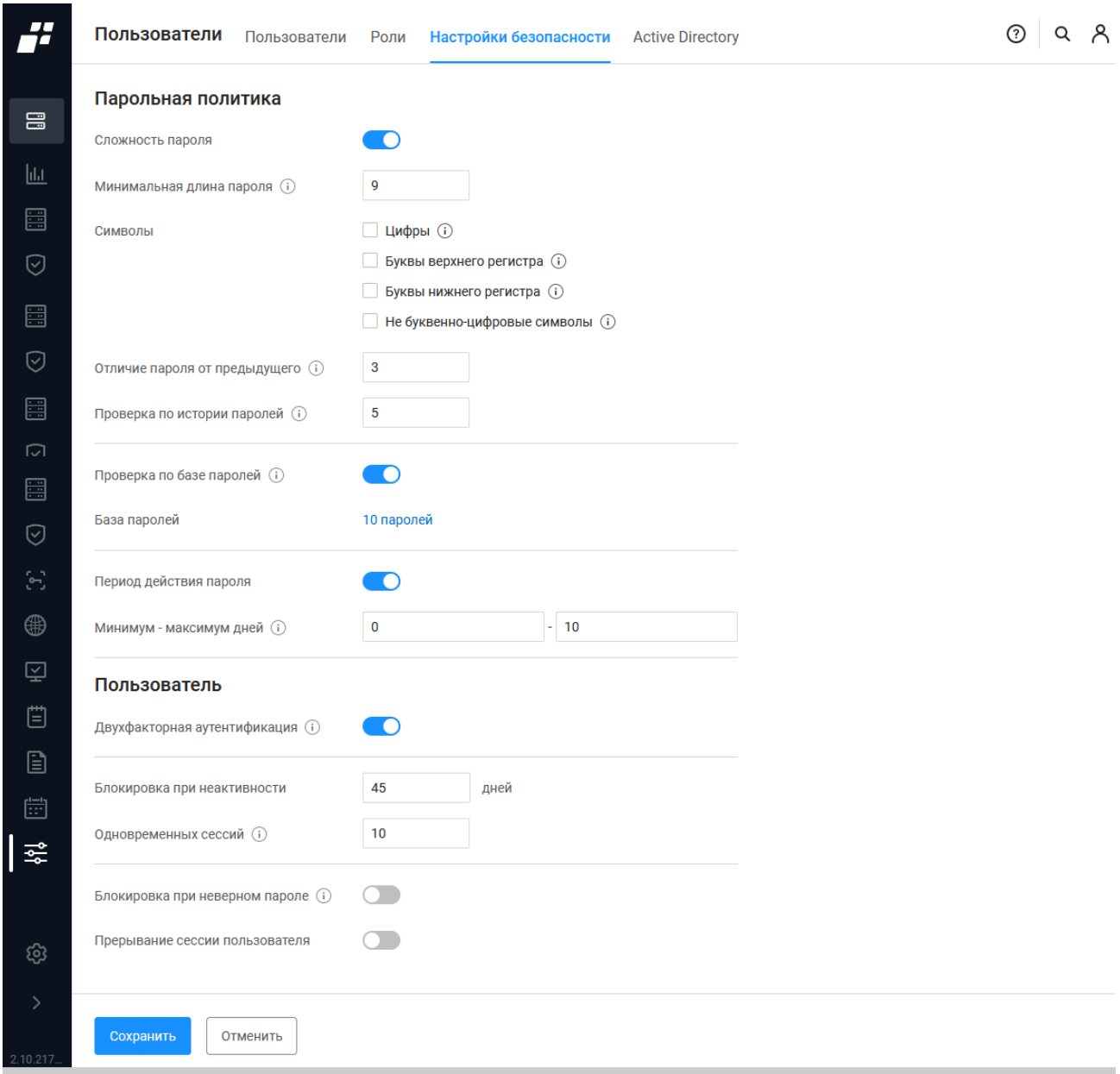


Рисунок 112 – Вкладка «Настройки безопасности»

Таблица 35 – Состав и описание полей вкладки «Настройки безопасности»

Поле	Описание
Блок полей «Парольная политика»	
Поле «Сложность пароля»	Переключатель: — «Активен» ( ) – применить настройки сложности для паролей сетевых пользователей; — «Неактивен» ( ) – настройки сложности для паролей сетевых пользователей не применяются. При активации переключателя появляются дополнительные

Поле	Описание
	поля
Поле «Минимальная длина пароля»	Числовое поле для ввода минимального количества знаков, которые должны содержаться в пароле сетевого пользователя. Допустимые значения: от 8 до 30. Значение по умолчанию: 8
Поле «Символы»	Поле для выбора обязательных символов, которые должны содержаться в пароле: — «Цифры» – пароль должен содержать хотя бы одну цифру; — «Буквы верхнего регистра» – пароль должен содержать хотя бы одну латинскую заглавную букву (от A до Z); — «Буквы нижнего регистра» – пароль должен содержать хотя бы одну латинскую строчную букву (от a до z); — «Не буквенно-цифровые символы» – пароль должен содержать хотя бы один не буквенно-цифровой символ. Допустимые для использования в ПК «Efros DO» символы приведены в подсказке, которая открывается по нажатию кнопки «ⓘ»
Поле «Отличие пароля от предыдущего»	Числовое поле для ввода количества знаков пароля, которые должны отличаться от предыдущего. Допустимые значения: от 0 до 3. Значение по умолчанию: 3
Поле «Проверка по истории паролей»	Числовое поле для ввода количества новых уникальных паролей до повторного использования сохраненного ранее пароля. Допустимые значения: от 1 до 10. Значение по умолчанию: 5
Поле «Проверка по базе паролей»	Переключатель: — «Активен» () – применить проверку по базе паролей; — «Неактивен» () – проверка по базе паролей не применяется. При активации переключателя появляется дополнительное поле «База паролей»
Поле «База паролей»	Содержит ссылку. При переходе открывается окно «Изменение списка паролей». Пользователь имеет

Поле	Описание
	возможность очистить список популярных паролей, изменить и удалить внесенные ранее, добавить новые пароли. Пароль пользователя ПК «Efros DO» не должен содержать слова из заданного списка популярных паролей
Поле «Период действия пароля»	Переключатель: — «Активен» ( ) – применить настройки параметров периода действия паролей; — «Неактивен» ( ) – настройки параметров периода действия паролей не применяются. При активации переключателя появляется дополнительное поле «Минимум-максимум дней»
Поле «Минимум-максимум дней»	Числовое поле для ввода следующих значений: — «Минимум» – период времени (в днях), в течение которого пользователь не может изменять пароль. Чтобы разрешить изменять пароль сразу, установите первое значение «0». Допустимые значения: от 0 до 60; — «Максимум» – период времени (в днях), в течение которого пароль будет действительным. Допустимые значения: от 1 до 90
Блок полей «Пользователь»	
Поле «Двухфакторная аутентификация»	Переключатель: — «Активен» ( ) – включить прохождение пользователем двухфакторной аутентификации при авторизации в ПК «Efros DO»; — «Неактивен» ( ) – выключить прохождение пользователем двухфакторной аутентификации. Предварительно необходимо произвести настройку внешнего сервера RADIUS и настройку системы внешней аутентификации
Поле «Блокировка при неактивности»	Числовое поле для ввода количества дней неактивности пользователя, после которого он будет заблокирован. Допустимые значения: от 1 до 45. Значение по умолчанию: 45
Поле «Одновременных сессий»	Числовое поле для ввода количества одновременных сессий на разных устройствах/ браузерах. Допустимые значения: от 10 до 30.

Поле	Описание
	Значение по умолчанию: 15
Поле «Блокировка при неверном пароле»	Переключатель: — «Активен» () – включить временную блокировку при превышении заданного количества неверных попыток ввода пароля; — «Неактивен» () – запретить временную блокировку входа. При активации переключателя появляются дополнительные поля «Неверных вводов пароля подряд» и «Период блокировки»
Поле «Неверных вводов пароля подряд»	Числовое поле для ввода количества неуспешных попыток ввода пароля. Допустимые значения: от 3 до 4 После превышения указанного количества неуспешных попыток авторизации пользователь блокируется на время, указанное в поле «Период блокировки»
Поле «Период 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 3 до 30
Поле «Прерывание сессии пользователя»	Переключатель: — «Активен» () – разрешить прерывание сессии пользователя при превышении времени бездействия; — «Неактивен» () – запретить прерывание сессии пользователя. При активации переключателя появляется дополнительное поле «Период неактивности»
Поле «Период неактивности»	Числовое поле для ввода максимального периода неактивности, после которого сессия пользователя будет заблокировано
Элементы управления	
Сохранить	При нажатии кнопки введенные изменения применяются
Отменить	При нажатии кнопки настройки остаются без применения изменений

10.1.4 Вкладка «Active Directory»

Вкладка «Active Directory» позволяет пользователю комплекса работать (создавать/удалять/редактировать соединения) со списком подключений к источнику AD (рис. 113).

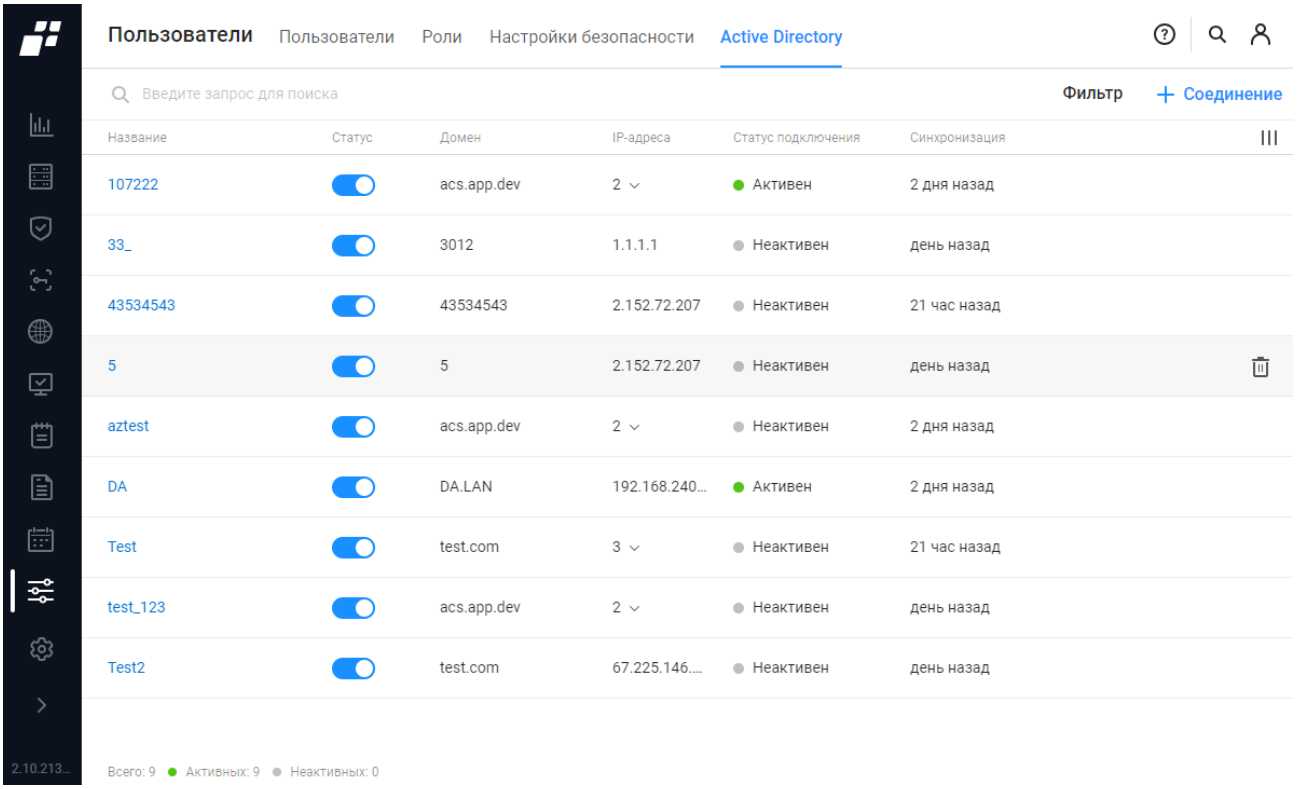


Рисунок 113 – Вкладка «Active Directory»

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

- название – название соединения в ПК «Efros DO». Является ссылкой, при переходе по которой открывается окно для редактирования данных соединения;
- статус. Переключатель:
  - « » – соединение активно;
  - « » – соединение неактивно.
- домен – имя домена для автоматического определения IP-адресов серверов служб каталогов;
- IP-адреса – IP-адреса серверов служб каталогов, с которыми будет осуществляться синхронизация пользователей и групп. Колонка заполняется автоматически, если корректно заполнено поле «Домен» и доступен сервер DNS;
- статус подключения;
- дата и время последней синхронизации.

Над списком подключений располагаются:

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

При выборе строки с соединением в правом углу строки появляется кнопка «Удалить» ( ) для удаления выбранного соединения.

В нижней части страницы отображается информация об общем количестве соединений, о количестве активных и неактивных соединений.

10.1.4.1 Создание Active Directory соединения

Для создания нового соединения Active Directory необходимо:

1) Нажать кнопку «Соединение» (Соединение).
2) Откроется окно «Создание Active Directory соединения» (рис. 114). Заполнить поля окна необходимыми параметрами и нажать кнопку «Создать». Состав и описание полей страницы приведены в таблице 36.

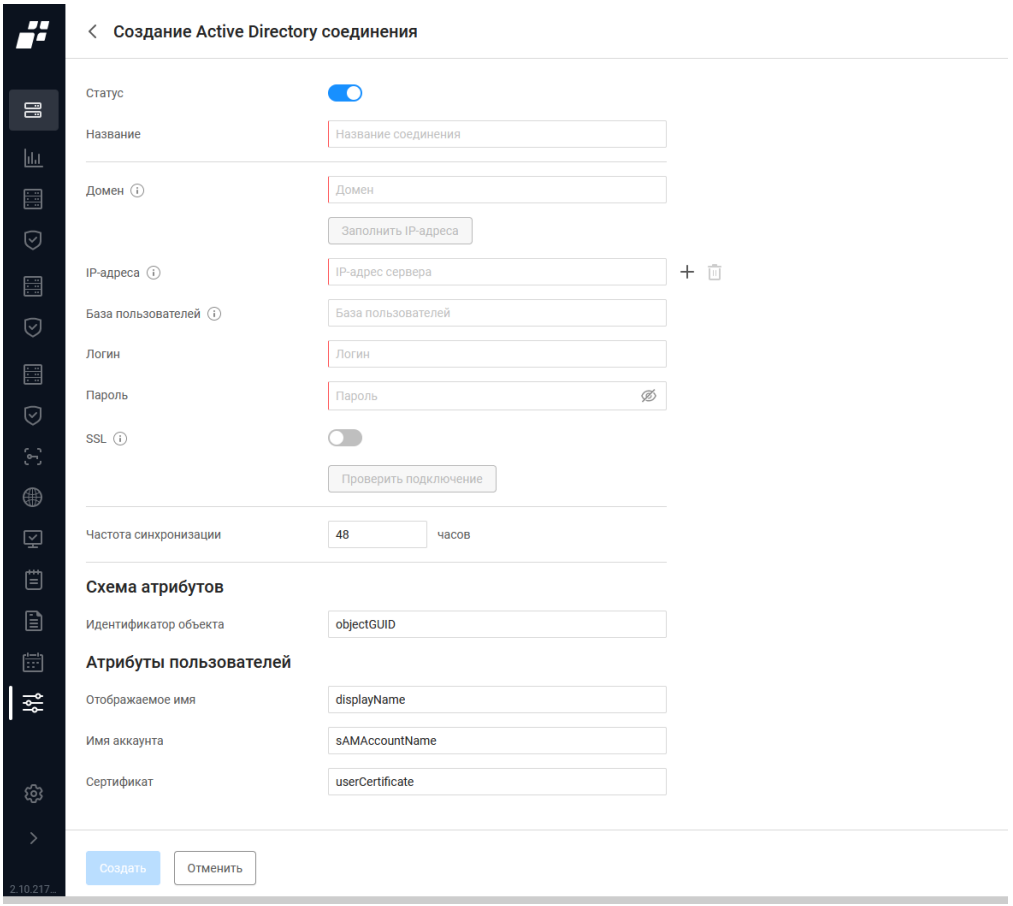


Рисунок 114 – Страница «Создание Active Directory соединения»

Таблица 36 – Состав и описание полей страницы «Создание Active Directory соединения»

Поле	Описание
Поле «Статус»	Переключатель: — «Активен» ( ) – соединение активно; — «Неактивен» ( ) – соединение неактивно
Поле «Название»	Поле для ввода названия соединения. Параметры ввода текста: от 1 до 50 символов. Допустимые символы: буквы латинского алфавита, цифры, «_», «–»
Поле «Домен»	Поле для ввода имени домена. Параметры ввода текста: от 1 до 50 символов. Допустимые символы: буквы латинского алфавита, цифры, «_», «–»
Кнопка «Заполнить IP-адреса»	По нажатию кнопки выполняется автоматический поиск IP-адреса сервера домена, указанного в поле «Домен». Если поиск завершится успешно, то будет автоматически заполнено поле «IP-адреса» (см. ниже), иначе отобразится сообщение об ошибке
Поле «IP-адреса»	Поле для ввода IP-адресов серверов служб каталогов, с которыми будет осуществляться синхронизация пользователей и групп. Указанные серверы должны быть доступны по следующим портам: — 389 – при использовании протокола LDAP; — 636 – при использовании протокола LDAPS. Заполняются автоматически по нажатию кнопки «Заполнить IP адреса», если корректно заполнено поле «Домен» и доступен сервер DNS
Поле «База пользователей»	Уровень, с которого будет осуществляться поиск пользователей в дереве служб каталогов. Если поле не заполнено, поиск выполняется по всему дереву служб каталогов. Пример: ou=users, dc=dev, dc=local
Поле «Логин»	Поле для ввода логина пользователя, настраивающего подключение. Допустимые символы: только буквы, цифры и символы, исключая: \/"[]:|<>+=;,?*@
Поле «Пароль»	Поле для ввода пароля пользователя, настраивающего подключение. Параметры ввода текста: от 1 до 500 любых символов

Поле	Описание
Поле «SSL»	Переключатель, активирует взаимодействие со службой каталогов по протоколу LDAPS
Кнопка «Проверить подключение»	При нажатии кнопки выполняется проверка подключения к источнику AD с указанными выше параметрами
Поле «Частота синхронизации»	Поле для ввода времени синхронизации данных с сервером каталогов (в часах)
Поле «Идентификатор объекта»	Текстовое поле. Заполнено по умолчанию. Поле доступно для редактирования
Группа полей «Атрибуты пользователей»	
Поле «Отображаемое имя»	Текстовое поле. Заполнено по умолчанию. Поле доступно для редактирования
Поле «Имя аккаунта»	Текстовое поле. Заполнено по умолчанию. Поле доступно для редактирования
Поле «Сертификат»	Текстовое поле. Заполнено по умолчанию. Поле доступно для редактирования
Элементы управления	
Создать	При нажатии кнопки выполняется сохранение внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу без сохранения внесенных данных

10.2 Лицензия

Подраздел «Лицензия» предоставляет пользователю комплекса информацию о наличии лицензии на продукт и сроках ее действия (рис. 115). Состав и описание полей страницы подраздела «Лицензия» приведены в таблице 37.

По окончании 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

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

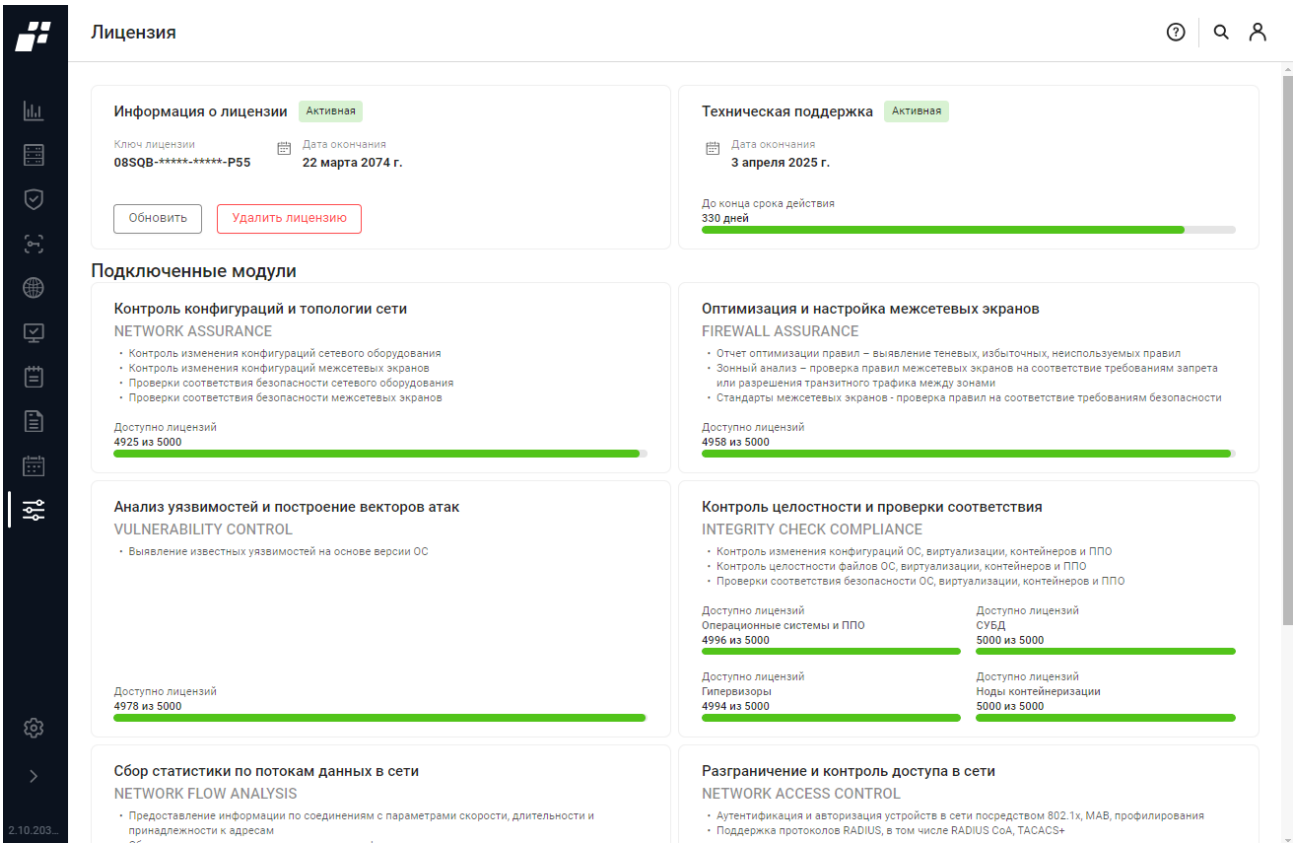


Рисунок 115 – Страница подраздела «Лицензия»

Таблица 37 – 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 «Удалить лицензию»	Позволяет удалить лицензию
Поле «Техническая поддержка»	Содержит следующую информацию: — статус технической поддержки; — вид технической поддержки; — дата окончания технической поддержки; — количество оставшихся дней до окончания технической поддержки
Блок полей «Подключенные	Содержит следующую информацию: — название модуля;

Поле	Описание
модули»	— описание функций; — количество доступных лицензий на оборудование для каждого модуля

10.3 Сертификаты

Подраздел «Сертификаты» позволяет работать со списками SSL-сертификатов (рис. 116).

После установки ПК «Efros DO» в комплексе используются самоподписанные корневой, промежуточный и серверный сертификаты (далее – предустановленные сертификаты).

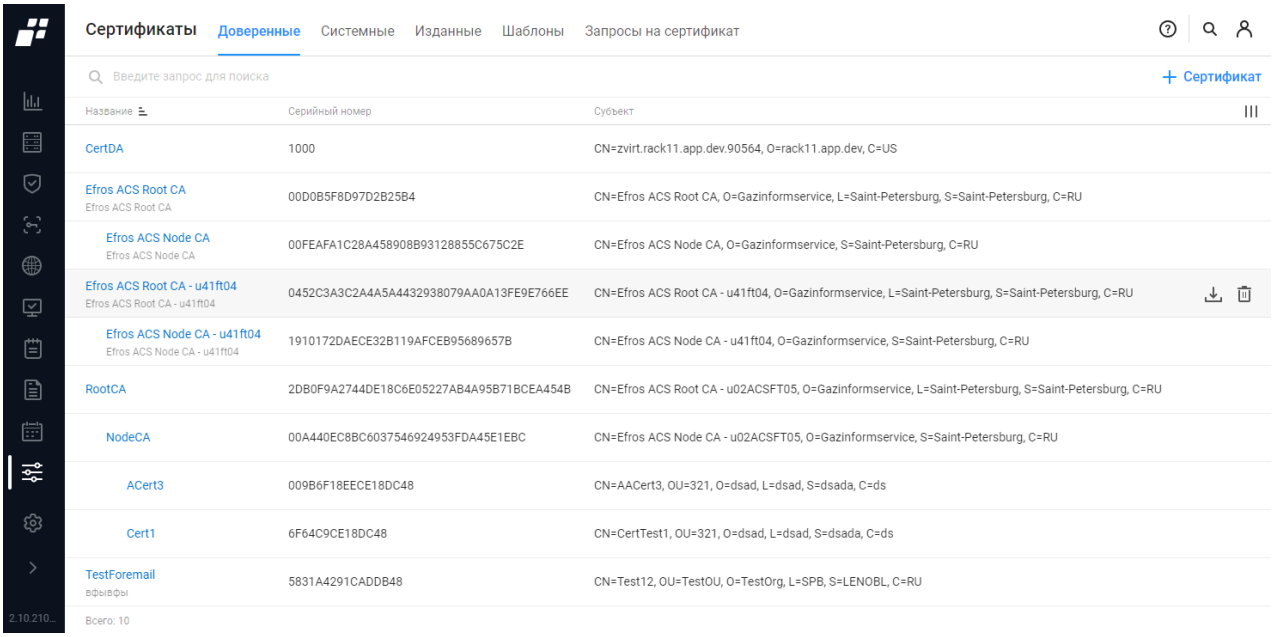


Рисунок 116 – Подраздел «Сертификаты». Вкладка «Доверенные»

Страница подраздела содержит следующие вкладки:

- «Доверенные» – предназначена для ведения списка корневых и промежуточных сертификатов;
- «Системные» – предназначена для ведения списка серверных сертификатов;
- «Изданные» – предназначена для ведения списка выпущенных в ПК «Efros DO» серверных и клиентских сертификатов;
- «Шаблоны» – предназначена для ведения шаблонов сертификатов, которые используются для выпуска клиентских и серверных сертификатов на вкладке «Изданные»;

— «Запросы на сертификат» – предназначена для ведения списка запросов на сертификаты.

10.3.1 Вкладка «Доверенные»

Вкладка «Доверенные» предназначена для ведения списка корневых и промежуточных сертификатов.

На странице список сертификатов реализован в виде таблицы (см. рис. 116). Корневые и промежуточные корневые сертификаты, находящиеся в одной цепочке, отображаются иерархически.

Для каждой записи списка отображаются следующие данные:

— название сертификата, присвоенное при импортировании;
— серийный номер, присвоенный центром сертификации;
— данные субъекта сертификата.

Над таблицей списка сертификатов располагаются:

— поле поиска (Введите запрос для поиска);
— кнопка «Сертификат» (+ Сертификат);
— кнопка «Колонки» ( ).

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

— «Удалить» ( );
— «Экспортировать» ( ).

10.3.1.1 Ведение списка доверенных сертификатов

Для добавления сертификата пользователю необходимо:

1) Нажать кнопку «Сертификат» (+ Сертификат).
2) Откроется окно «Создание сертификата» (рис. 117). Заполнить поля окна необходимыми параметрами и нажать кнопку «Создать».

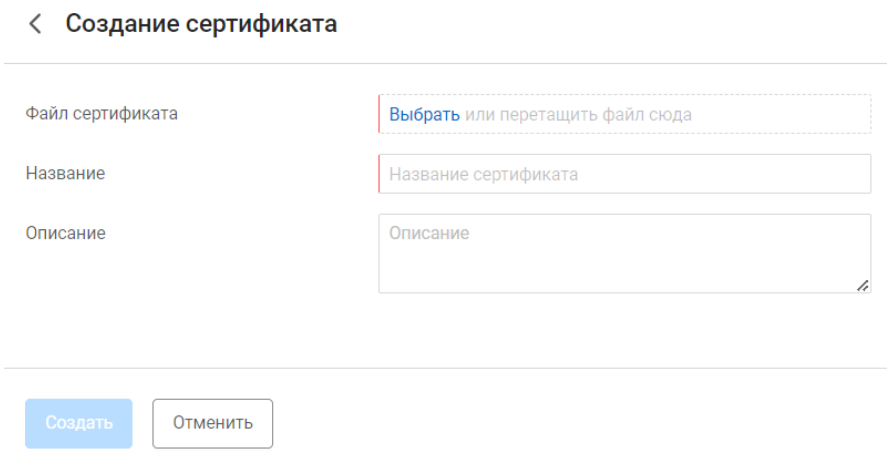


Рисунок 117 – Окно «Создание сертификата» на вкладке «Доверенные сертификаты»

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. 118):
— просмотреть данные сертификата;
— внести требуемые изменения и нажать кнопку «Сохранить». Окно редактирования сертификата закроется, внесенные изменения будут сохранены.

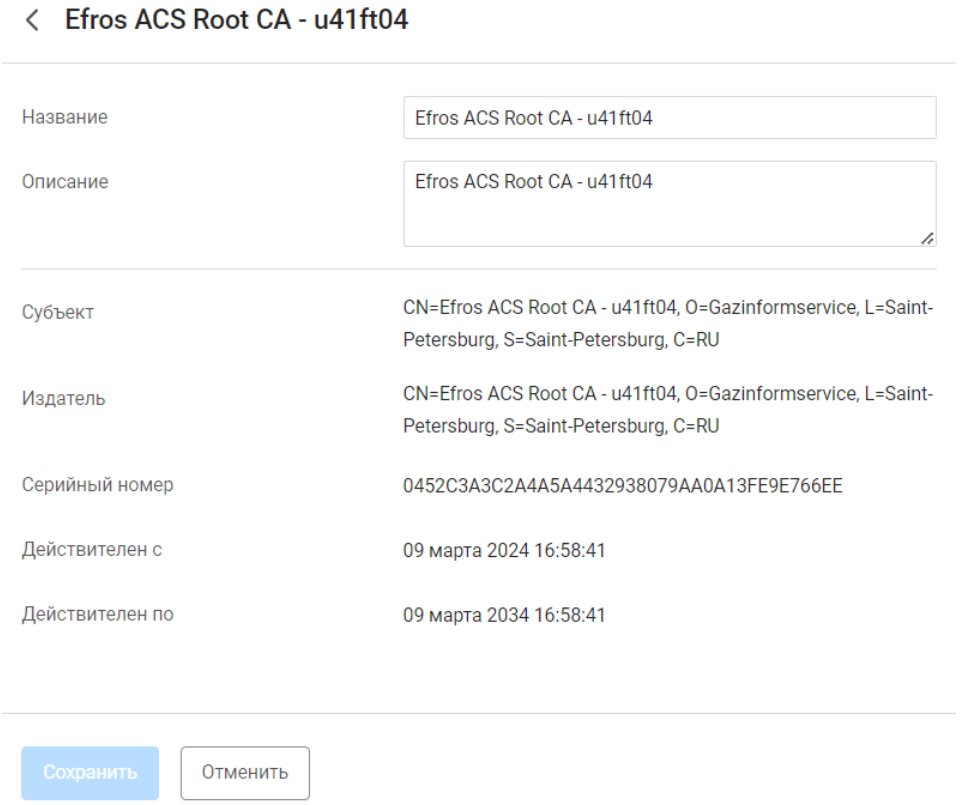


Рисунок 118 – Окно редактирования сертификата

Предустановленные сертификаты не доступны для удаления и внесения изменений.

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

10.3.2 Вкладка «Системные»

Вкладка «Системные» предназначена для ведения списка серверных сертификатов. 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.

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

На вкладке «Системные» список сертификатов реализован в виде таблицы (рис. 119).

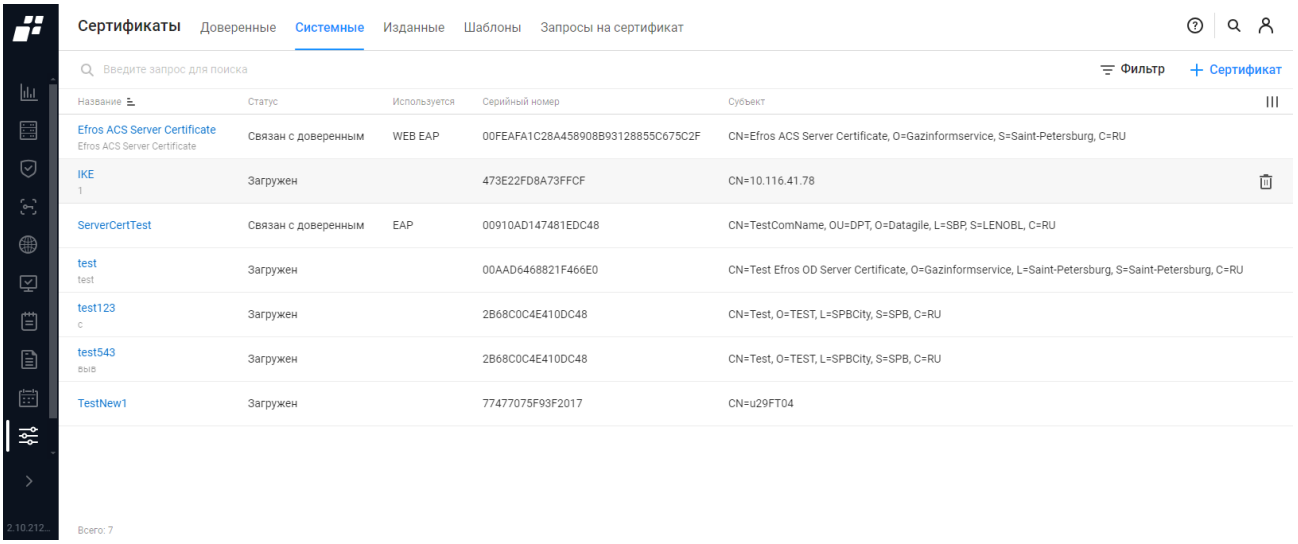


Рисунок 119 – Вкладка «Системные»

Для каждой записи списка отображаются следующие данные:

— название сертификата, присвоенное при импортировании;

— статус сертификата:
  - «Загружен» – не найден связанный с ним корневой сертификат;
  - «Связан с корневым» – серверный сертификат связан с корневым.

— 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 сертификатов располагаются:

— поле поиска (Введите запрос для поиска);

— кнопка «Сертификат» (+ Сертификат);

— кнопка «Колонки» ( ).

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

10.3.2.1 Ведение списка системных сертификатов

Добавление серверных сертификатов выполняется автоматически после привязки к запросу сертификата, полученного от центра сертификации (см. п. 10.3.5), либо путем импорта уже имеющегося в организации серверного сертификата в БД комплекса.

Создание серверного сертификата выполняется аналогично созданию корневых сертификатов (см. п. 10.3.1.1), за исключением того, что в окне «Создание сертификата» (рис. 120):

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

Предустановленные серверные сертификаты недоступны для удаления и внесения изменений.

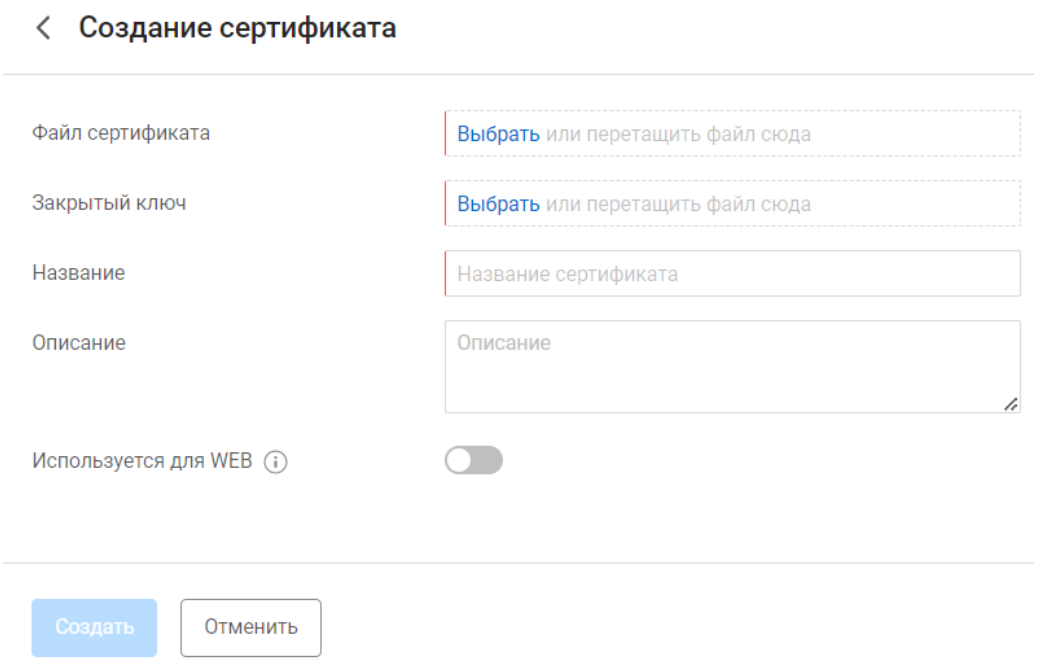


Рисунок 120 – Окно «Создание сертификата» на вкладке «Системные сертификаты»

10.3.3 Вкладка «Изданные»

Вкладка «Изданные» доступна пользователю для работы при наличии лицензии на функциональный модуль «Efros NAC»

Вкладка «Изданные» предназначена для ведения списка выпущенных в ПК «Efros DO» серверных и клиентских сертификатов.

После установки ПК «Efros DO» список изданных 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 сертификата.

На вкладке «Изданные» список сертификатов реализован в виде таблицы (рис. 121).

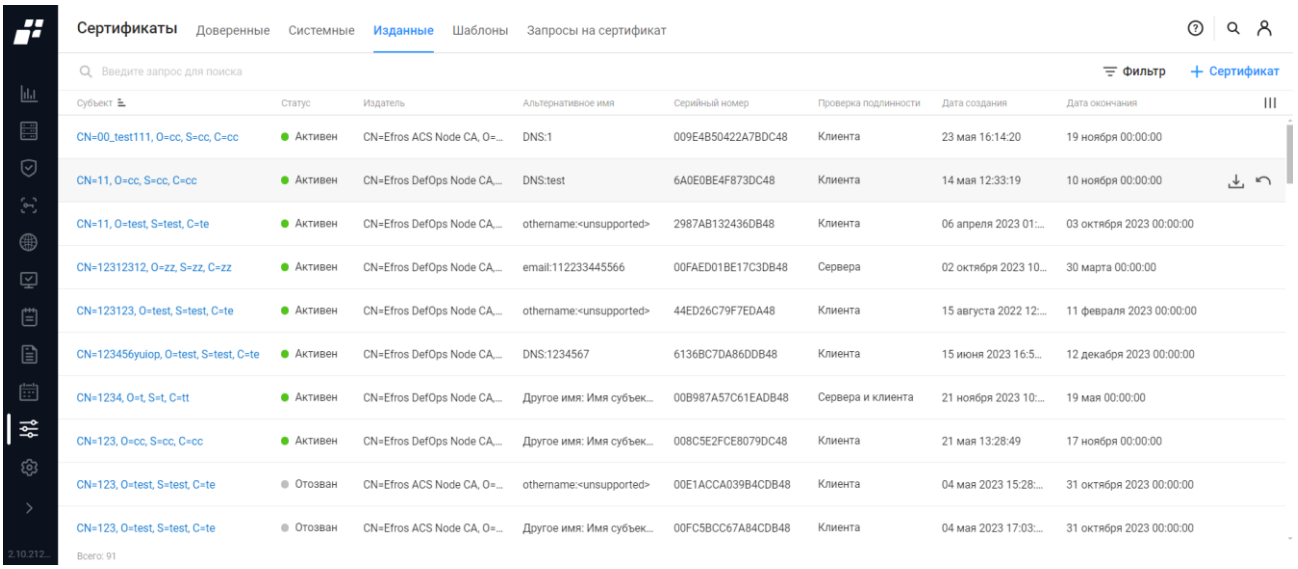


Рисунок 121 – Вкладка «Изданные»

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 комплексе;
- на чьей стороне осуществляется проверка подлинности;
- дата создания сертификата;
- дата окончания срока действия сертификата.

Над списком сертификатов располагаются:

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

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

- «Экспортировать» ( );
- «Отозвать» ( ).

10.3.3.1 Ведение списка изданных сертификатов

Для успешного выпуска сертификата необходимо создать шаблон. Более подробно о создании шаблона написано в п. 10.3.4.

Для выпуска нового сертификата необходимо:

1) Нажать кнопку «Сертификат» (+ Сертификат) над таблицей клиентских сертификатов.
2) Откроется окно создания нового сертификата (рис. 122).

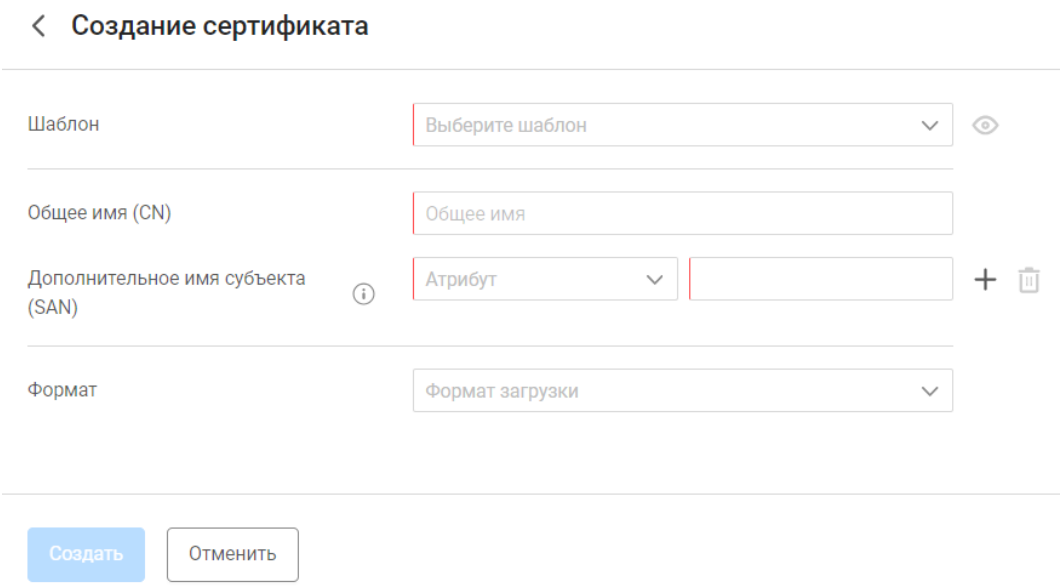


Рисунок 122 – Страница «Создание сертификата» на вкладке «Изданные»

3) Выбрать в поле «Шаблон» название шаблона, на основе которого будет создаваться сертификат.
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» один из параметров:

- «DNS» – имена доменов, дополнительно к указанным в поле «Subject»;
- «E-mail (Имя RFC822)» – E-mail адрес владельца сертификата;
- «IP-адрес» – IP-адрес, который может использоваться в качестве альтернативного имени хоста вместо имени, указанного в поле «Subject»;
- «MAC-адрес (Имя RFC822)» – MAC-адрес владельца сертификата;
- «URI» – строка символов, идентифицирующая уникальный ресурс по его адресу (URL) или имени (URN);

- «Имя участника-пользователя» – дополнительная информация о владельце сертификата, может быть заполнено с помощью формата «Subject» Distinguished Name (DN).

— 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 окончании процесса отобразится соответствующее сообщение.

Выпущенный сертификат будет внесен в список изданных 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.

10.3.4 Вкладка «Шаблоны»

На вкладке «Шаблоны» список сертификатов реализован в виде таблицы (рис. 123).

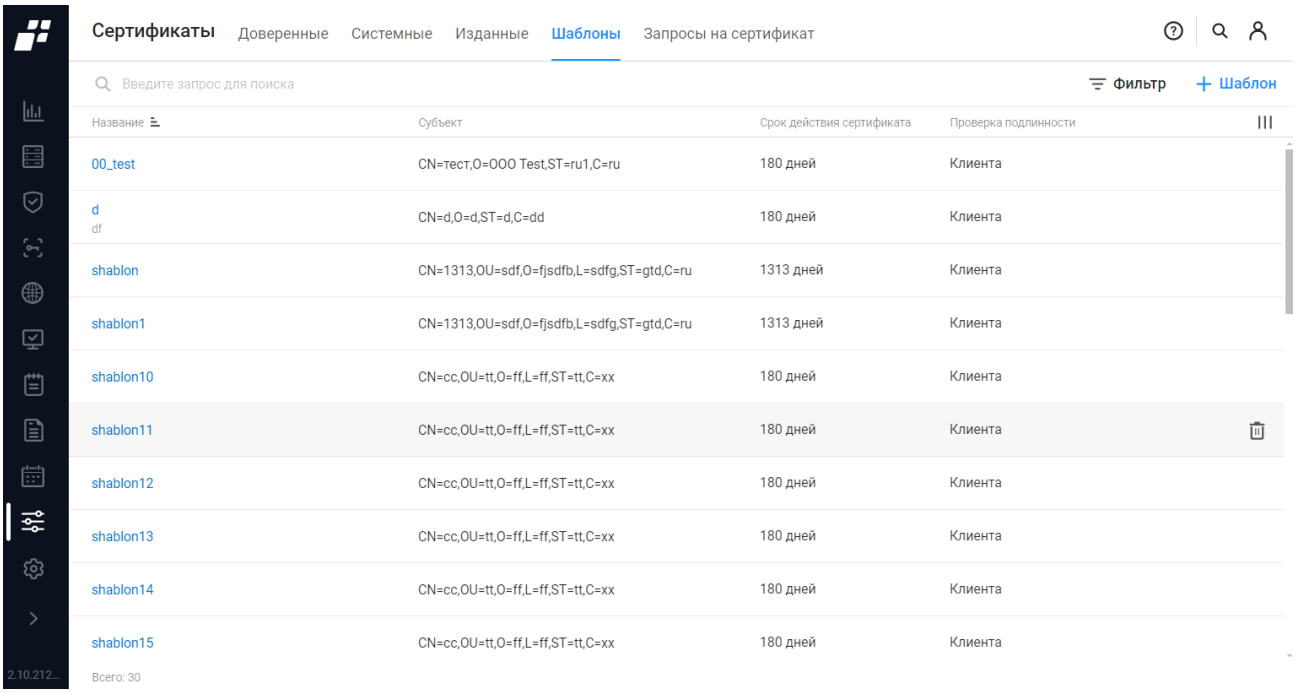


Рисунок 123 – Вкладка «Шаблоны»

Для каждой записи списка отображаются следующие данные:

- название шаблона;
- данные субъекта сертификата;
- срок действия сертификата;
- на чьей стороне осуществляется проверка подлинности.

Над таблицей списка шаблонов сертификатов располагаются:

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

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

10.3.4.1 Ведение списка шаблонов сертификатов

Для добавления нового шаблона клиентского сертификата необходимо:

1) Нажать кнопку «Шаблон» (+ Шаблон).
2) Откроется страница «Создание шаблона» (рис. 124). Заполнить поля необходимыми параметрами и нажать кнопку «Создать».

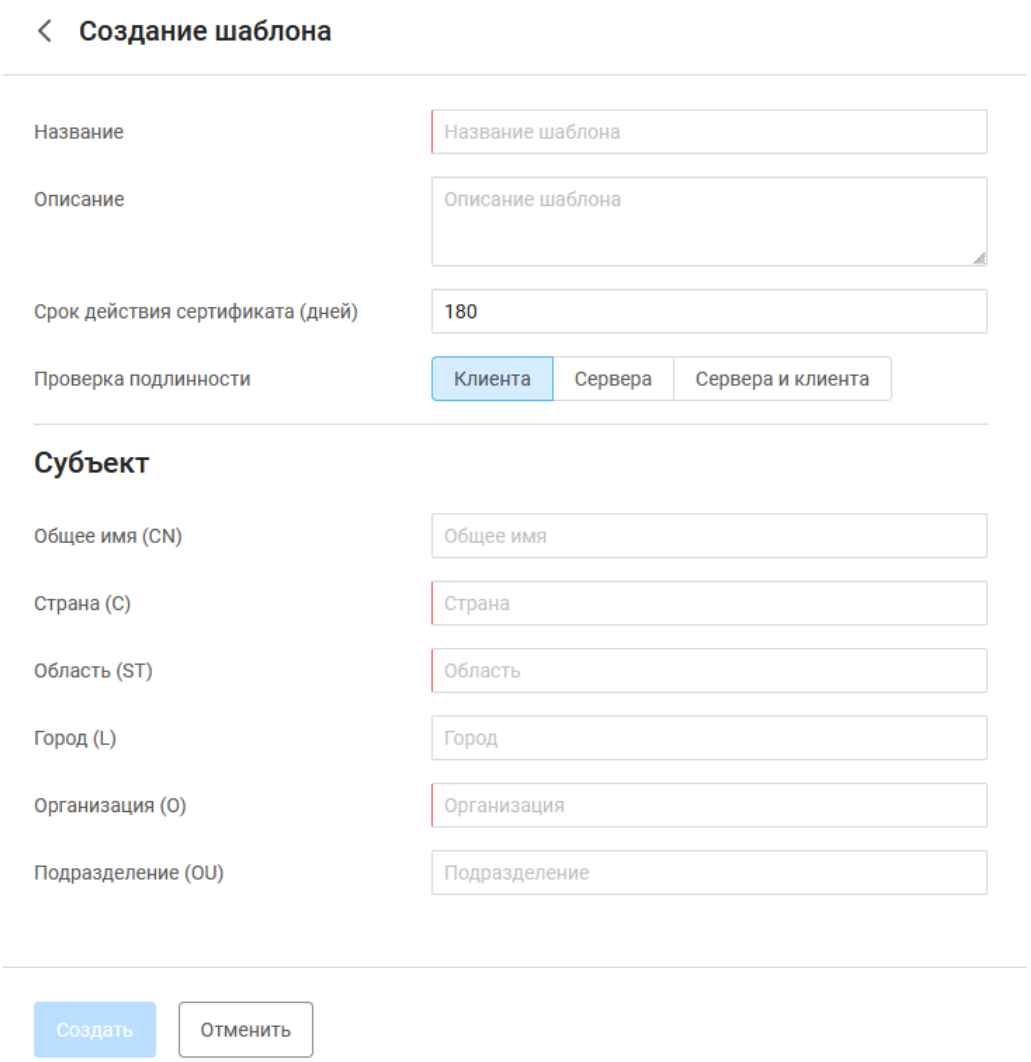


Рисунок 124 – Страница «Создание шаблона»

10.3.5 Вкладка «Запросы на сертификаты»

На вкладке «Запросы на сертификаты» список запросов реализован в виде таблицы (рис. 125).

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.

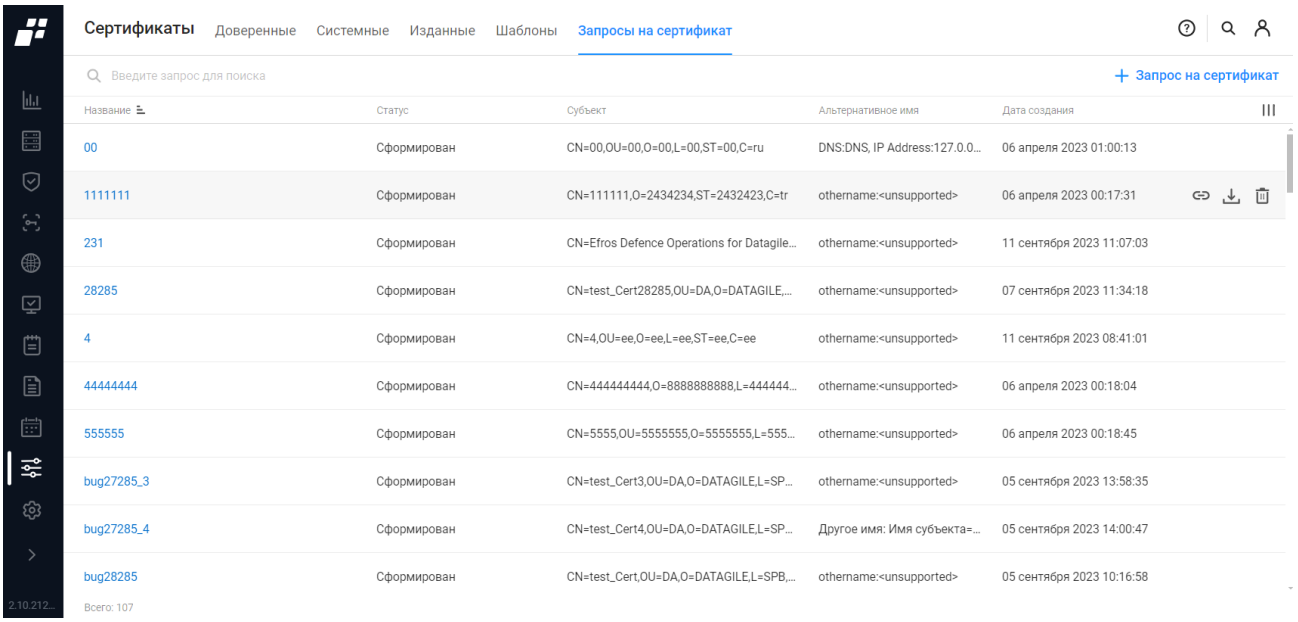


Рисунок 125 – Вкладка «Запросы на сертификат»

Над списком запросов располагаются:

- поле поиска (Введите запрос для поиска);
- кнопка «Запрос на сертификат» (+ Запрос на сертификат);
- кнопка «Колонки» ( ).

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

- «Привязать» ( );
- «Экспортировать» ( );
- «Удалить» ( ).

10.3.5.1 Ведение списка запросов на сертификаты

Для формирования нового запроса на сертификат необходимо:

1) Нажать кнопку «Запрос на сертификат» (+ Запрос на сертификат).
2) Откроется страница «Создание запроса на сертификат» (рис. 126). Заполнить поля необходимыми данными и нажать кнопку «Создать».

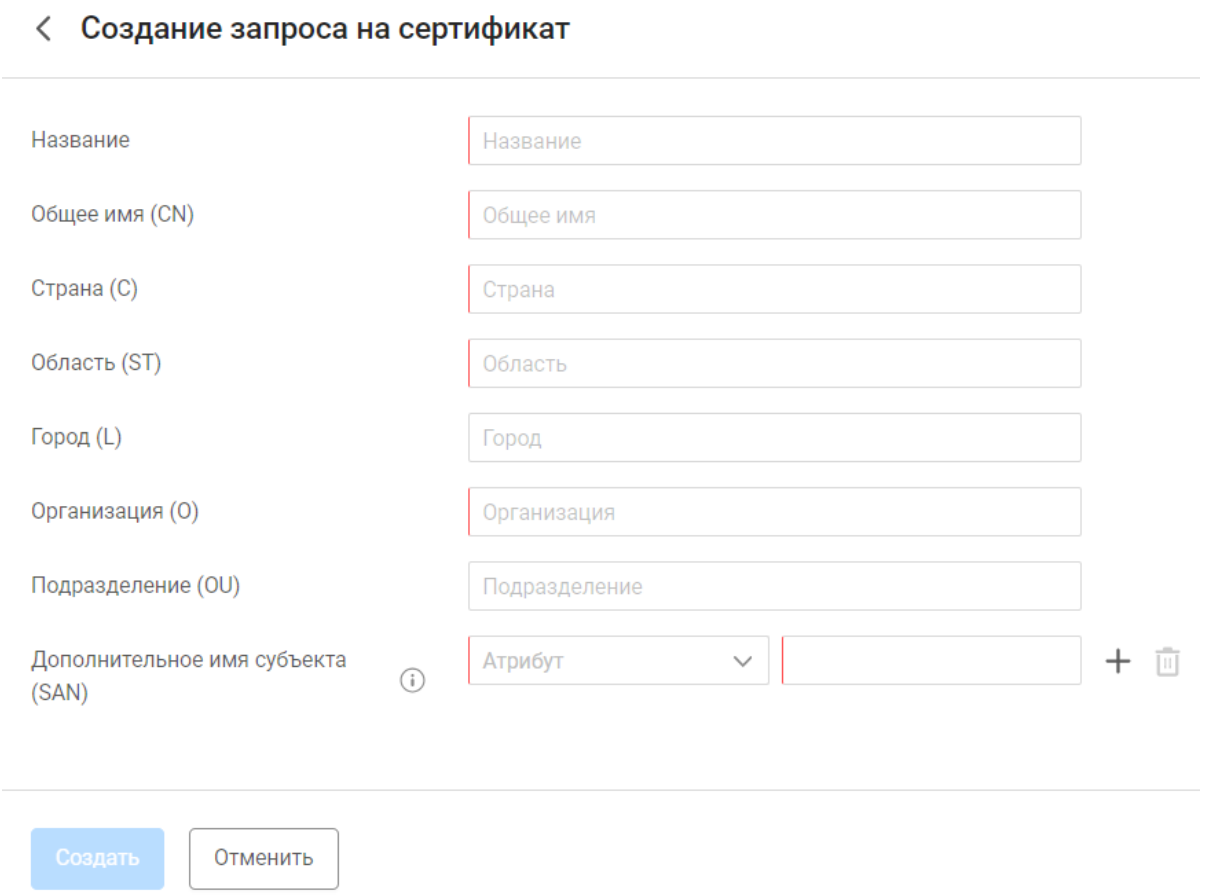


Рисунок 126 – Окно «Создание запроса на сертификат»

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. 127).

Кнопка «Копировать» предназначена для копирования текста запроса в буфер обмена.

Для экспорта запроса на локальную ЭВМ в виде файла 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.

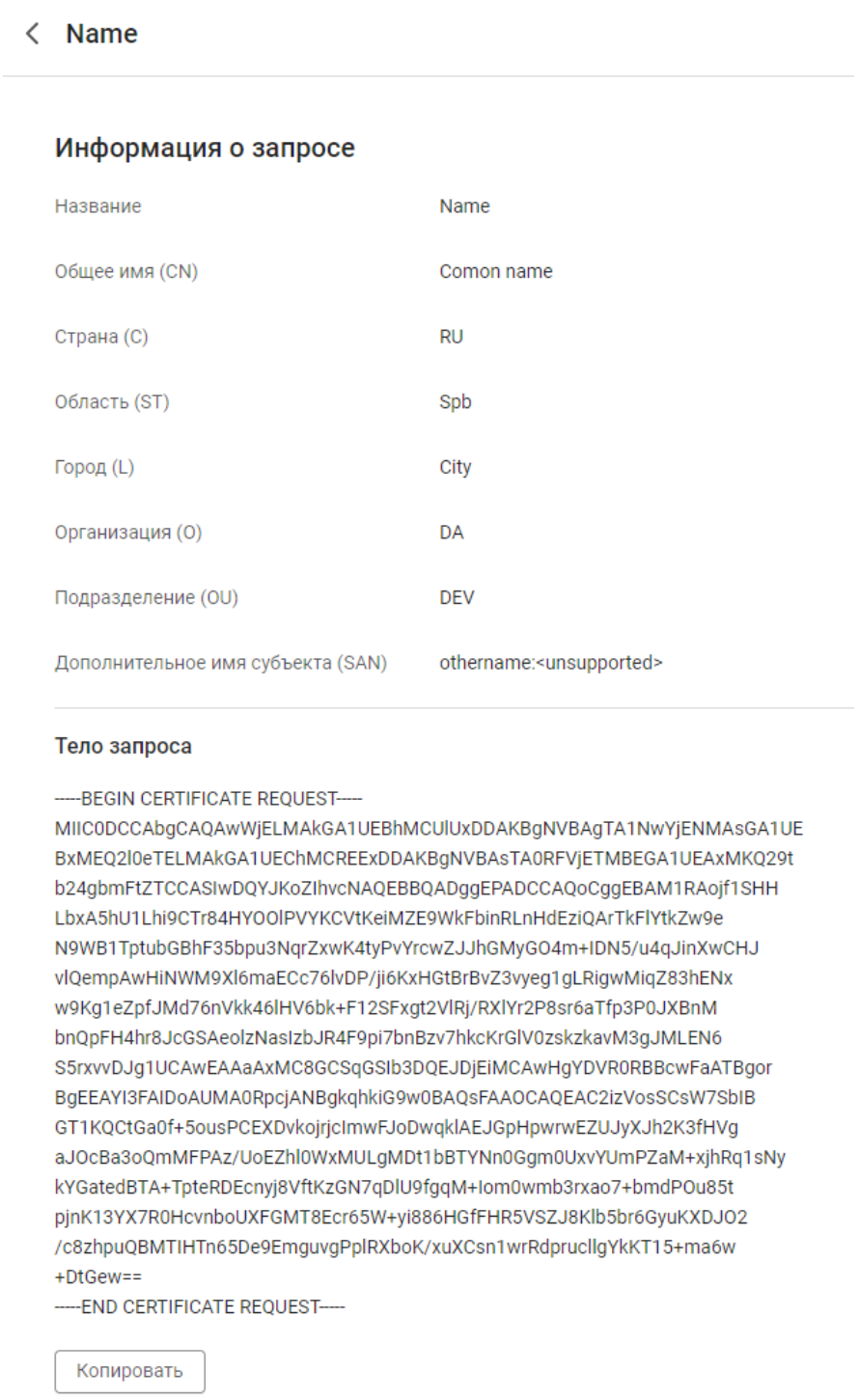


Рисунок 127 – Окно «Информация о запросе»

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. 128) выбрать файл сертификата, нажав ссылку «Выбрать» и выбрав в стандартном окне ОС требуемый файл.

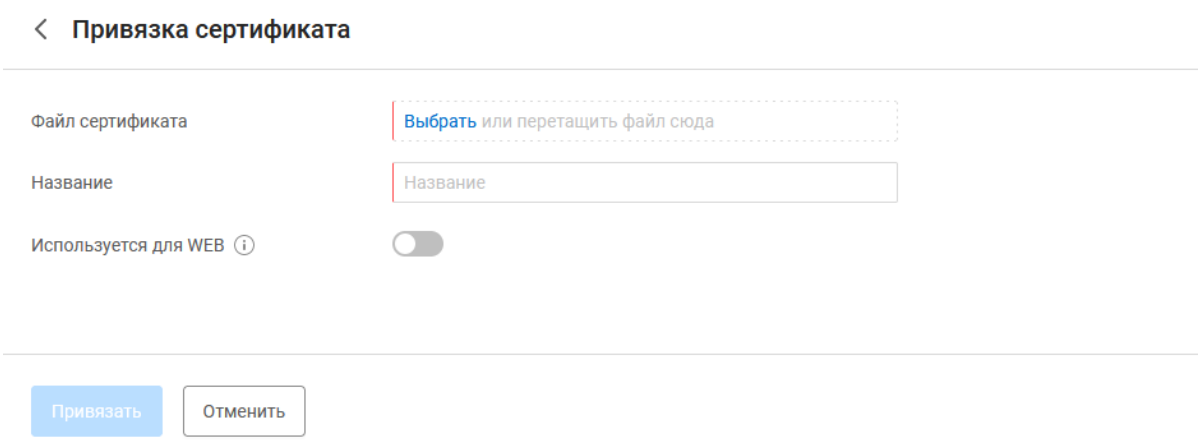


Рисунок 128 – Окно привязки сертификата к запросу

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

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 системных сертификатов.

10.4 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:
  - «Восстановление пароля» – система отправляет код для восстановления пользователю, запросившему восстановление пароля;
  - «Оповещение об окончании расчета векторов атак» – система отправляет оповещение об окончании расчета.

— Задачи по расписанию:

- «Обновить базу уязвимостей» – обновление уязвимостей для установленных модулей;
- «Оповестить об истечении срока действия сертификата» – оповещение пользователя об истечении срока действия системного или доверенного сертификата за количество дней, указанное в параметре задачи;
- «Оповестить о блокировке учетной записи» – оповещение пользователя об истечении срока действия системного или доверенного сертификата за количество дней, указанное в параметре задачи;
- «Оповестить об окончании действия пароля» – оповещение пользователя о сроке окончания действия пароля за кол-во дней, указанных в параметре задачи;
- «Очистить активные сеансы конечных точек» – освободить лицензию 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»;
- «Синхронизировать с внешними источниками» – задание для периодического запуска синхронизации LDAP.

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. 129).

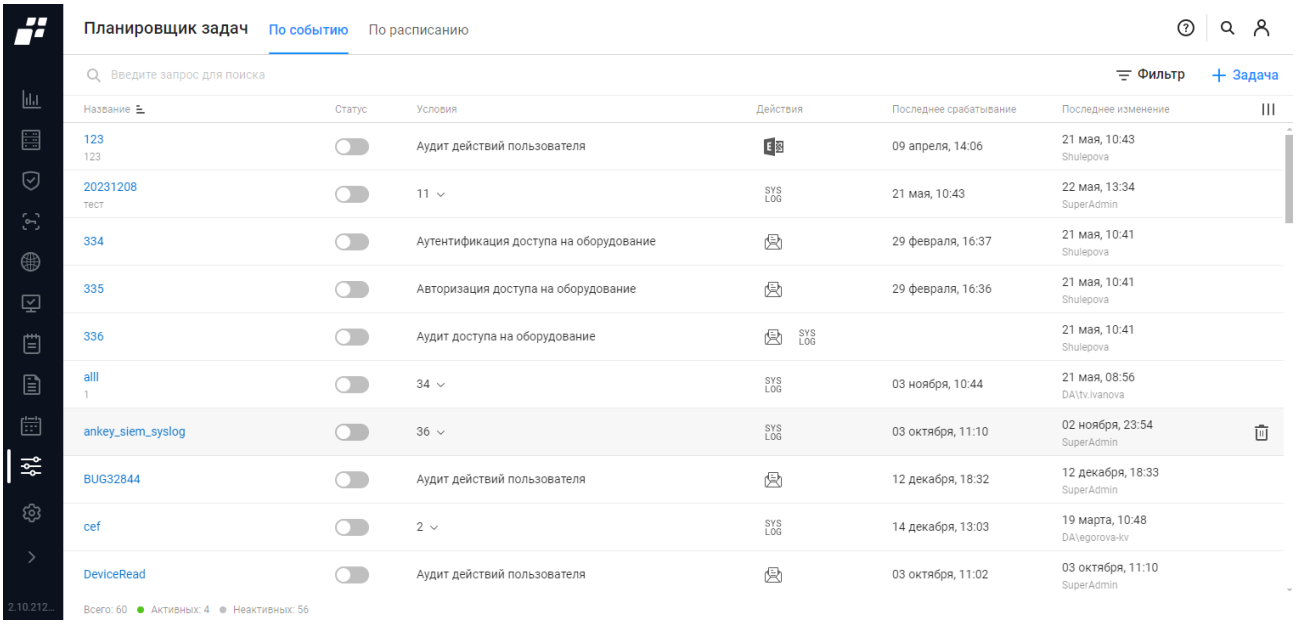


Рисунок 129 – Подраздел «Планировщик». Вкладка «По событию»

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.

10.4.1 Вкладка «По событию»

На вкладке «По событию» 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;
- статус. Переключатель, отображает активность задачи (включен или выключен);
- название условия или количество условий, если их больше одного. Количество является раскрывающимся списком. Условия задаются при создании задачи;
- действия: «Отправить сообщение» (), «Отправить сообщение через Exchange» (), «Отправить Syslog-сообщение» (SYS LOG), «Отправить в Apache Kafka» ();
- последнее срабатывание. Отображается дата и время последнего срабатывания обработчика события;
- последнее изменение. Отображается дата и время, а также логин пользователя, совершившего последнее изменение обработчика события.

Над списком задач располагаются:

- поле поиска (Введите запрос для поиска);
- кнопка «Фильтр» (Фильтр);
- кнопка «Задача» (+ Задача) для создания задачи по событию;
- кнопка «Колонки» ().

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

10.4.1.1 Создание задачи по событию

Для добавления задачи по событию необходимо выполнить следующие действия:

1) Нажать кнопку «Задача» (+ Задача).
2) Откроется страница «Создание задачи по событию» (рис. 130). Заполнить на странице необходимые параметры. Состав и описание полей страницы приведены в таблице 38.

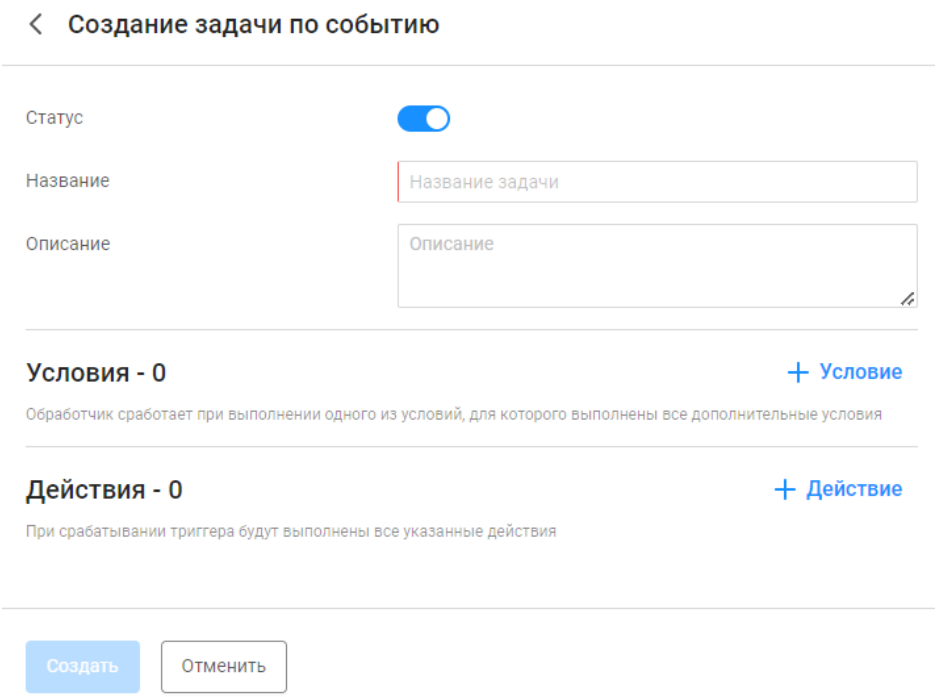


Рисунок 130 – Страница «Создание задачи по событию»

Таблица 38 – 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 «Условие» (+ Условие) для выполнения правил обработки событий
Поле «Действия»	Выбор типа выполняемого действия через кнопку «Действие» (+ 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. Перечень доступных типов событий приведен в таблице 39.

Таблица 39 – Типы событий

Категория события	Тип события
Контроль доступа	— Аутентификация доступа на оборудование; — Авторизация доступа на оборудование; — Аудит доступа на оборудование; — Аутентификация доступа в сеть
Контроль трафика	— События триггера «утилизация по интерфейсу»; — События триггера «утилизация по подсети»
Обнаружение	— Событие автоматического обнаружения ОЗ; — SNMP сканирование – обнаружение ОЗ
Системные	— Системные события «Контроль доступа»; — Системные события «Общие»; — Аудит действий пользователя; — Ошибки сервера
Агенты	— Контроль агентов; — Проверка соответствия требованиям безопасности; — Установка и обновление
Управление устройствами	— Восстановление конфигурации; — Выполнение конфигурирования; — Выполнение операций
Контроль изменений	— Загрузка отчета; — Изменение отчета; — Изменение результата проверки; — Контроль целостности компонентов; — Нарушение целостности
Виртуализация	— Proxmox Запуск (завершение) компонентов виртуальной среды; — Proxmox Доступ субъектов доступа к компонентам виртуальной среды; — KVM Доступ субъектов доступа к компонентам виртуальной среды; — KVM Запуск/завершение компонентов; — zVirt Доступ субъектов доступа к компонентам виртуальной среды; — zVirt Запуск (завершение) компонентов виртуальной среды; — zVirt Изменений правил разграничения доступа к компонентам среды виртуализации; — Скала-Р Уведомление;

Категория события	Тип события
	— Скала-Р Запуск (завершение) работы компонентов виртуальной среды; — Скала-Р Изменений правил разграничения доступа к компонентам среды виртуализации; — Скала-Р Доступ субъектов доступа к компонентам виртуальной среды
Неклассифицированные	— SNMP Trap сообщение; — Запуск Windows агента; — Обновление словаря уязвимостей; — Изменение доступности; — Syslog сообщение

4) Для добавленного условия нажать ссылку «Дополнительные условия» и из раскрывающегося списка значений выбрать параметр события, для которого задается условие. В зависимости от вида выбранного параметра в окне отобразится ряд вариантов значений (рис. 131).

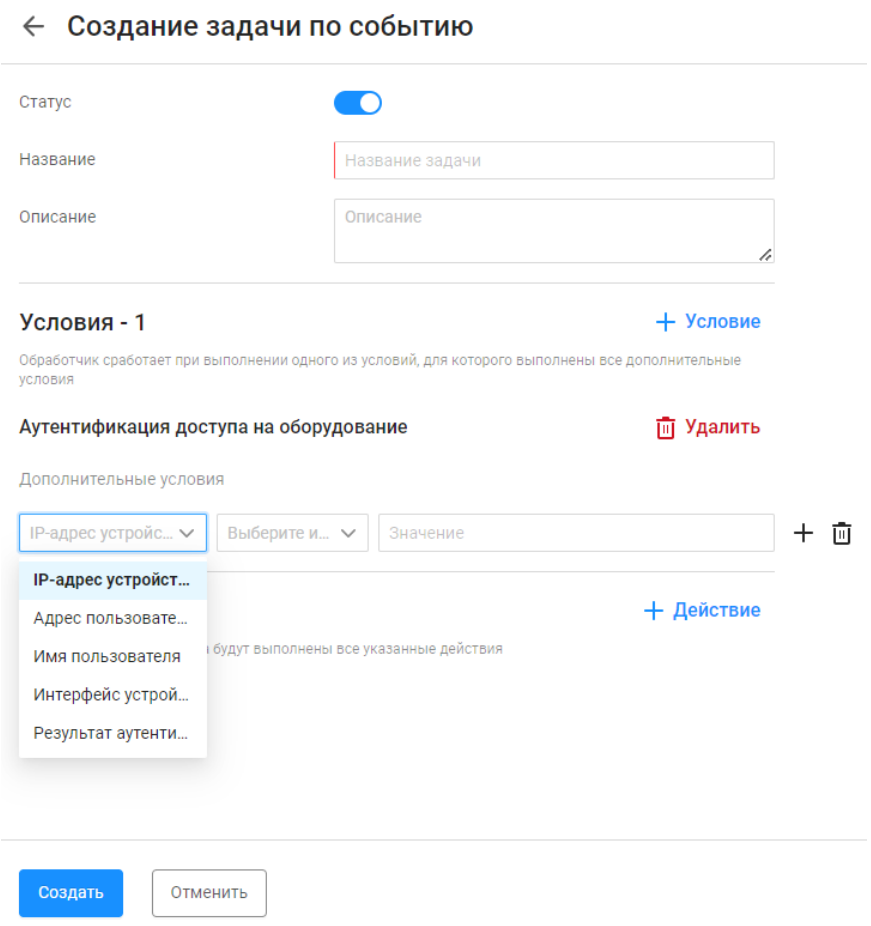


Рисунок 131 – Выбор дополнительных условий

5) Повторить действия перечислений 3, 4 для добавления всех необходимых условий.

6) В поле «Действия» нажать кнопку «Действие» (+ Действие). В раскрывшемся списке выбрать тип действия, которое будет выполнено в комплексе в ответ на произошедшее событие (рис. 132).

7) Задать для выбранного действия параметры отправки сообщений:

— для действий «Отправить письмо» и «Отправить письмо через Exchange» – ввести в дополнительных полях (рис. 133) параметры отправки письма: выбрать список получателей (выбираются установкой флагов в окне со списком пользователей комплекса, которое открывается по нажатию ссылки «Выбрать пользователей и группы», выбор сохраняется после нажатия кнопки «Выбрать»), заполнить поля «Тема письма» и «Дополнительные адреса». Для проверки отправки письма – нажать кнопку «Отправить тестовое письмо»;

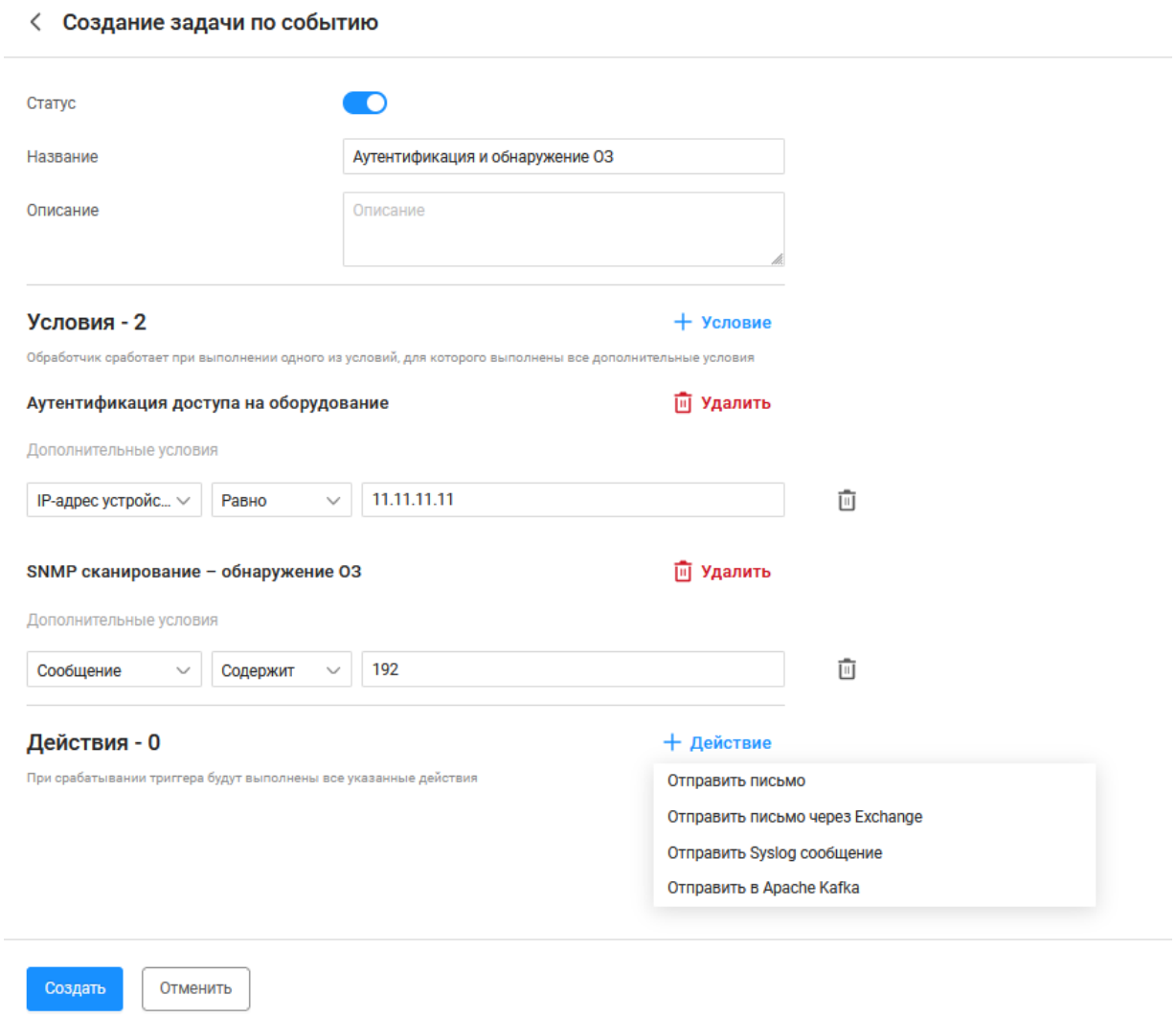


Рисунок 132 – Окно выбора действий для задачи по событию

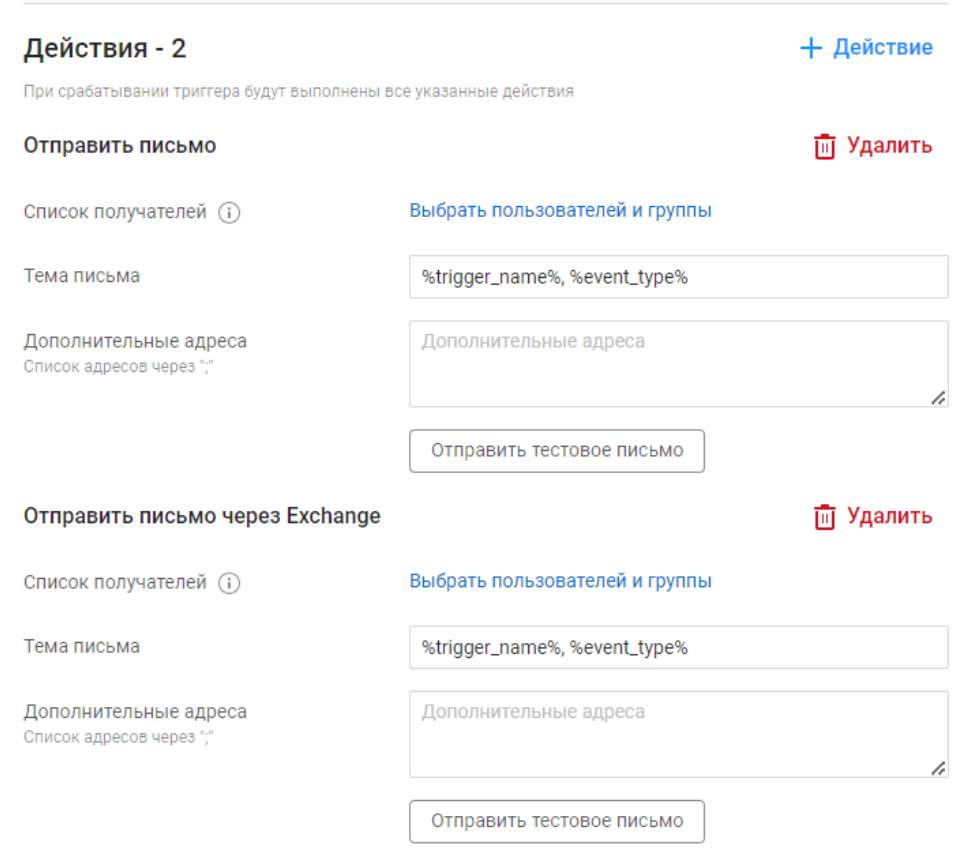


Рисунок 133 – Параметры отправки письма

— для действия «Отправить Syslog сообщение» – ввести в дополнительных полях (рис. 134) параметры отправки Syslog сообщения: адрес сервера, протокол: TCP или UDP, порт сервера, выбрать формат и уровень сообщения:
  - RFC 3164 (уровни: Alert, Critical, Debug, Emergency, Error, Information, Notice, Warning);
  - RFC 5424 (уровни: Alert, Critical, Debug, Emergency, Error, Information, Notice, Warning; дополнительные атрибуты);
  - CEF (уровни: High, Low, Medium, Unknown, Very-High).

— Для проверки отправки Syslog сообщения – нажать кнопку «Отправить тестовое сообщение»;

— для действия «Отправить в Apache Kafka» – ввести в дополнительных полях (рис. 135) параметры отправки сообщения в Apache Kafka: адрес сервера и порт, название топика, порт сервера, выбрать установкой переключателя наличие и тип аутентификации:
  - «Отсутствует»;
  - «PLAIN» (пользователь и пароль);
  - «SHA-256» (пользователь и токен);
  - «SHA-512» (пользователь и токен).

— Для проверки отправки сообщения в Apache Kafka – нажать кнопку «Отправить тестовое сообщение».

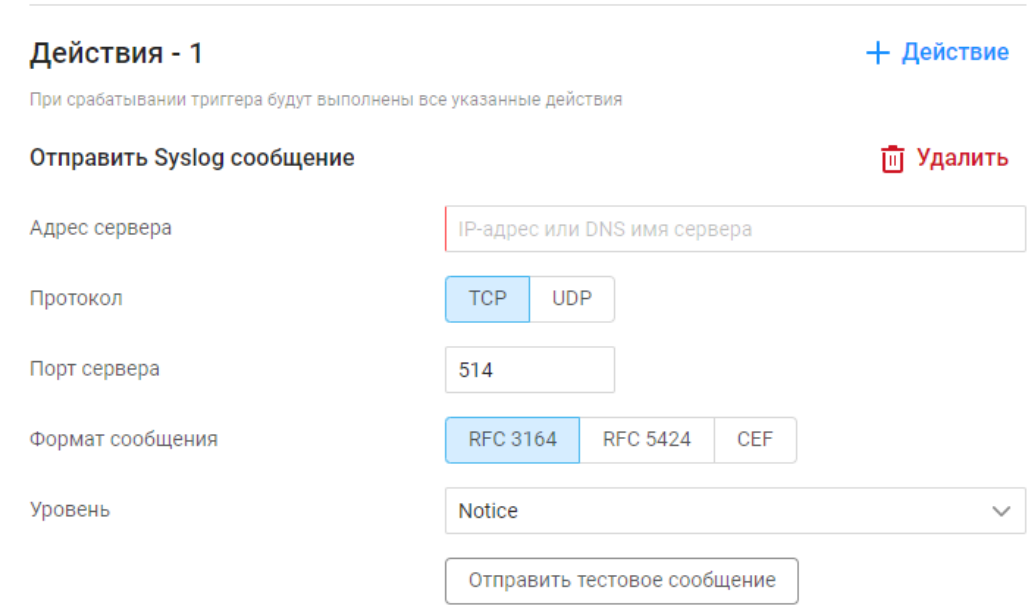


Рисунок 134 – Параметры отправки Syslog сообщения

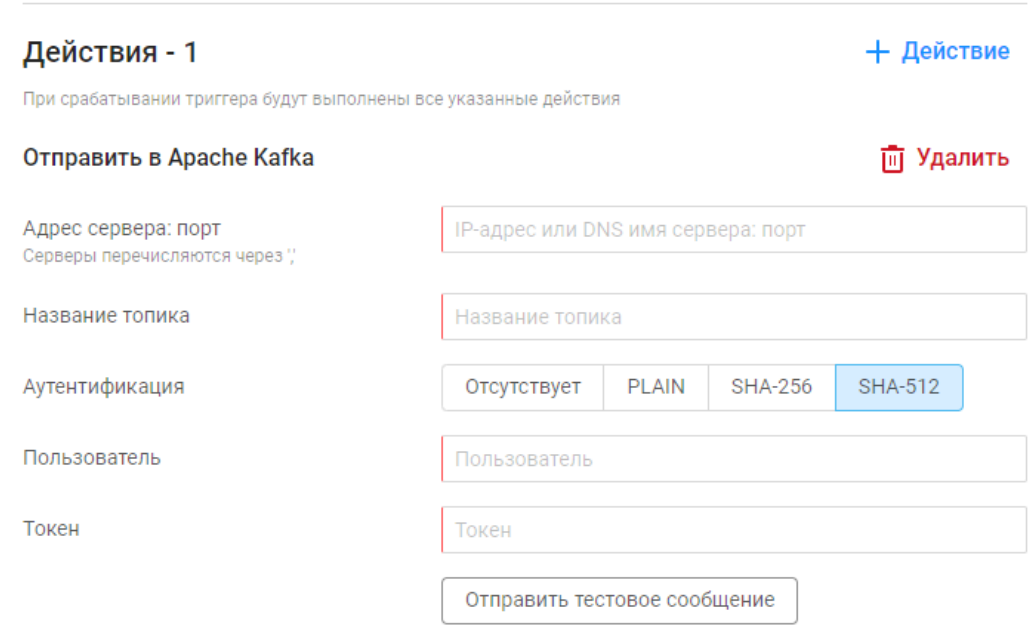


Рисунок 135 – Параметры отправки сообщения в Apache Kafka

8) Нажать кнопку «Создать».

10.4.2 Вкладка «По расписанию»

На вкладке «По расписанию» список задач по расписанию реализован в виде таблицы (рис. 136).

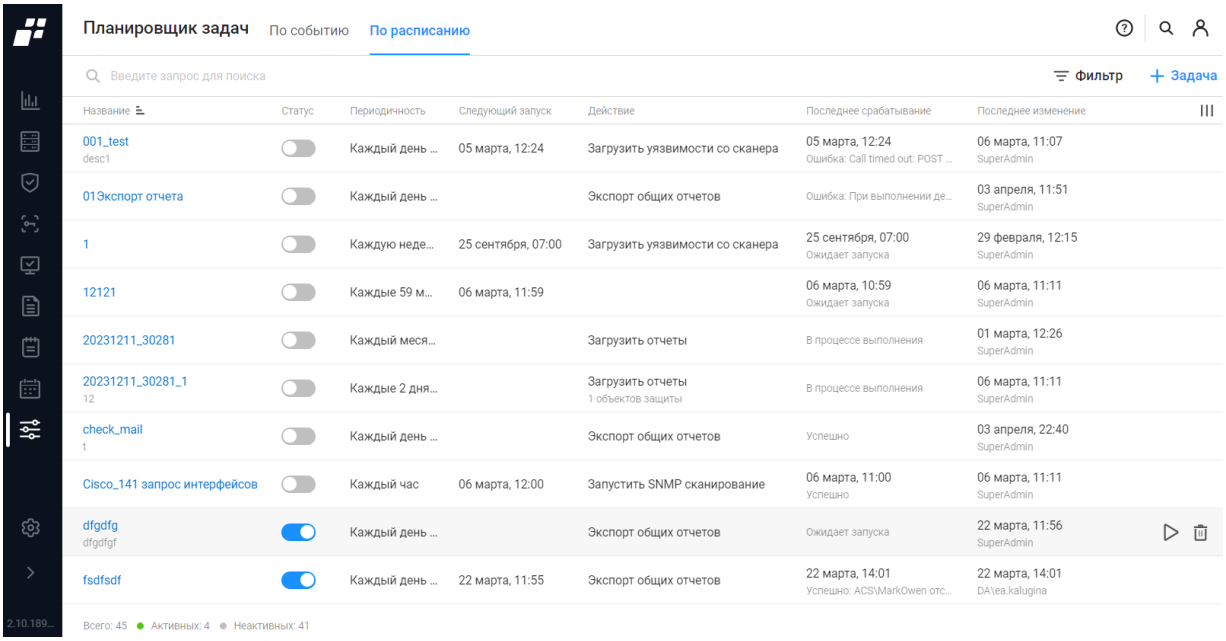


Рисунок 136 – Страница «Планировщик задач». Вкладка «По расписанию»

Для каждой записи списка отображаются следующие данные:

- название и описание задачи по выполнению расписания. Является ссылкой, при переходе по которой открывается окно редактирования расписания;
- статус. 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;
- последнее срабатывание. Отображается дата и время последнего срабатывания обработчика события 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);
- кнопка «Добавить задачу» (+ Задача);
- кнопка «Колонки» ( ).

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

«Удалить» ( ) для удаления задачи и кнопка «Запустить выполнение задачи» ( ), если задача включена.

10.4.2.1 Создание задачи по расписанию

Для создания новой задачи по расписанию необходимо выполнить следующие действия:

1) Нажать кнопку « + Задача ».
2) Откроется страница «Создание задачи по расписанию» (рис. 137). Заполнить на странице необходимые параметры и нажать кнопку «Создать». Состав и описание полей страницы приведены в таблице 40.

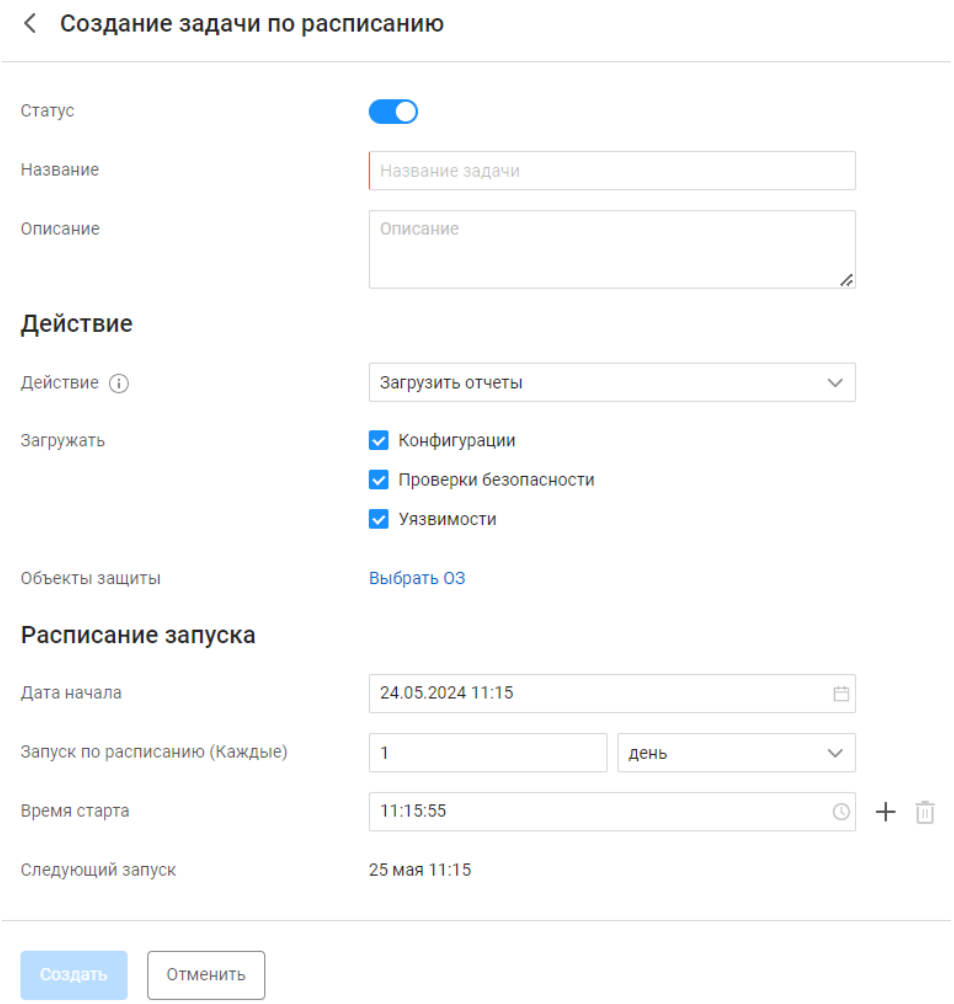


Рисунок 137 – Страница «Создание задачи по расписанию»

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

Поле	Описание
Поле «Статус»	Переключатель: — «Активен» ( ) – задача активна;

Поле	Описание
	— «Неактивен» ( ) – 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»; — «Загрузить уязвимости со сканера»; — «Запустить SNMP сканирование»; — «Экспорт общих отчетов». Состав дополнительных полей зависит от выбранного действия (см. ниже)
Дополнительные поля для действия «Загрузить отчеты». Для других действий см. таблицы 41, 42 и 43	
Поле «Загружать»	Предназначено для выбора объектов для загрузки по расписанию. Состав переключателей: — «Конфигурации»; — «Проверки безопасности»; — «Уязвимости»
Поле «Объекты защиты»	Является ссылкой. При переходе открывается окно для выбора ОЗ
Группа полей «Расписание запуска»	
Поле «Дата начала»	Поле для ввода даты и времени начала применения расписания
Поле «Запуск по расписанию (Каждые)»	Поле для настройки временных параметров запуска расписания. Состав полей группы зависит от выбранного временного интервала: минута, час, день, неделя, месяц
Поле «Время старта»	Поле для ввода времени 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

Поле	Описание
	списка задач без сохранения внесенных данных

Состав и описание полей действия «Загрузить уязвимости со сканера» (рис. 138) приведены в таблице 41.

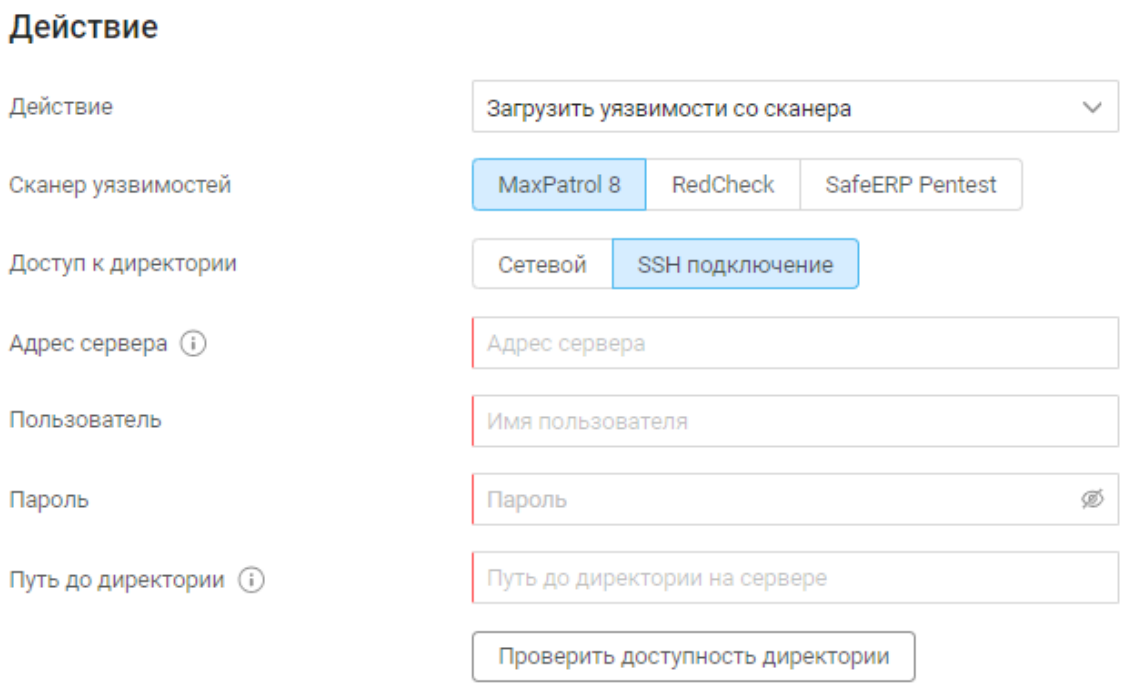


Рисунок 138 – Дополнительные поля для действия «Загрузить уязвимости со сканера»

Таблица 41 – Состав и описание дополнительных полей для действия «Загрузить уязвимости со сканера»

Поле	Описание
Поле «Сканер уязвимостей»	Переключатель: — «MaxPatrol 8»; — «RedCheck»; — «SafeERP Pentest». При изменении в поле значения изменяется набор дополнительных полей (см. ниже)
Группа полей для сканера уязвимостей «MaxPatrol 8»	
Поле «Доступ к директории»	Переключатель: — «Сетевой»; — «SSH подключение». При в поле изменении значения изменяется набор

Поле	Описание
	дополнительных полей (см. ниже)
Дополнительные поля для «MaxPatrol 8», доступ «Сетевой»	
Поле «Путь до директории»	Текстовое поле для ввода пути до директории, из которой забираются отчеты сканирования в формате .xml Пример формата ввода: \\[имя сервера]\\[имя директории] Сетевая директория должна быть доступна ПК «Efros DO»
Поле «Подключение»	Переключатель: — «Пользователь и пароль». Необходимо указать пользователя и пароль для доступа к директории; — «Анонимно»
Дополнительные поля для «MaxPatrol 8», доступ «SSH подключение»	
Поле «Адрес сервера»	Текстовое поле для ввода адреса сервера и нестандартного порта ssh. Пример формата ввода: [Адрес сервера]:[порт]
Поле «Пользователь»	Логин пользователя для доступа в директорию
Поле «Пароль»	Пароль пользователя для доступа в директорию
Поле «Путь до директории»	Текстовое поле для ввода пути до директории, из которой забираются отчеты сканирования в формате .xml Пример формата ввода: /[корневой каталог]/[имя директории]
Группа полей для сканера уязвимостей «RedCheck»	
Поле «URL API»	Поле для выбора префикса (http:// или https://) и ввода URL для вызова API, с помощью которого забираются отчеты сканирования
Поле «Пользователь»	Логин пользователя для доступа к API
Поле «Пароль»	Пароль пользователя для доступа к API
Группа полей для сканера уязвимостей «SafeERP Pentest»	
Поле «URL API»	Поле для выбора префикса (http:// или https://) и ввода URL для вызова API, с помощью которого выполняется получение токена и формирования списка агентов SafeERP Pentest
Поле «Пользователь»	Логин пользователя для доступа к API
Поле «Пароль»	Пароль пользователя для доступа к API
Поле «Агент»	Поле для выбора агента SafeERP Pentest, который будет

Поле	Описание
	выполнять сканирование целей При настройке расписаний запуска необходимо учитывать, что один агент SafeERP Pentest может выполнять сканирования только последовательно. Если агент находится в процессе сканирования, то запрос на запуск нового сканирования будет отклонен
Поле «Цели сканирования»	Поле для выбора в раскрывающемся списке подсеть, диапазон или хост и ввода IP-адресов для сканирования. При необходимости добавления нескольких областей адресов нужно нажать кнопку « + », при необходимости удалить – нажать кнопку « 🗑 »
Поле «Всего целей сканирования»	Количество IP-адресов для сканирования. Рассчитывается автоматически. Максимальное количество IP-адресов: 1000
Поле «Порты сканирования»	Поле для выбора протокола (TCP или UDP) и ввода списка портов сканирования. Допустимо указывать диапазон портов с использованием символов «,» и «-». Пример: 22,23,45-47. При необходимости добавления нескольких областей портов нужно нажать кнопку « + », при необходимости удалить – нажать кнопку « 🗑 ». При сохранении порты для одинаковых протоколов объединяются в одну строку
Элементы управления	
Проверить доступность директории	При нажатии кнопки выполняется проверка доступности директории
Проверить подключение	При нажатии кнопки выполняется проверка подключения
Получить список агентов	При нажатии кнопки выполняется проверка доступности сервиса и отображение подключенных агентов SafeERP Pentest

Состав и описание полей действия «Запустить SNMP сканирование» (рис. 139) приведены в таблице 42.

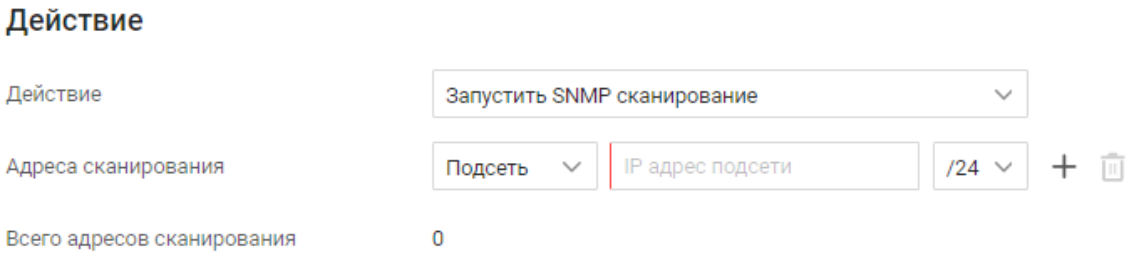


Рисунок 139 – Дополнительные поля для действия «Запустить SNMP сканирование»

Таблица 42 – Состав и описание дополнительных полей для действия «Запустить SNMP сканирование»

Поле	Описание
Поле «Адреса сканирования»	Поле для выбора в раскрывающемся списке подсеть, диапазон или хост и ввода IP-адресов для сканирования. При необходимости добавления нескольких областей адресов нужно нажать кнопку « + », при необходимости удалить – нажать кнопку « 🗑 »
Поле «Всего адресов сканирования»	Количество IP-адресов для сканирования. Рассчитывается автоматически

Состав и описание полей действия «Экспорт общих отчетов» (рис. 140) приведены в таблице 43.

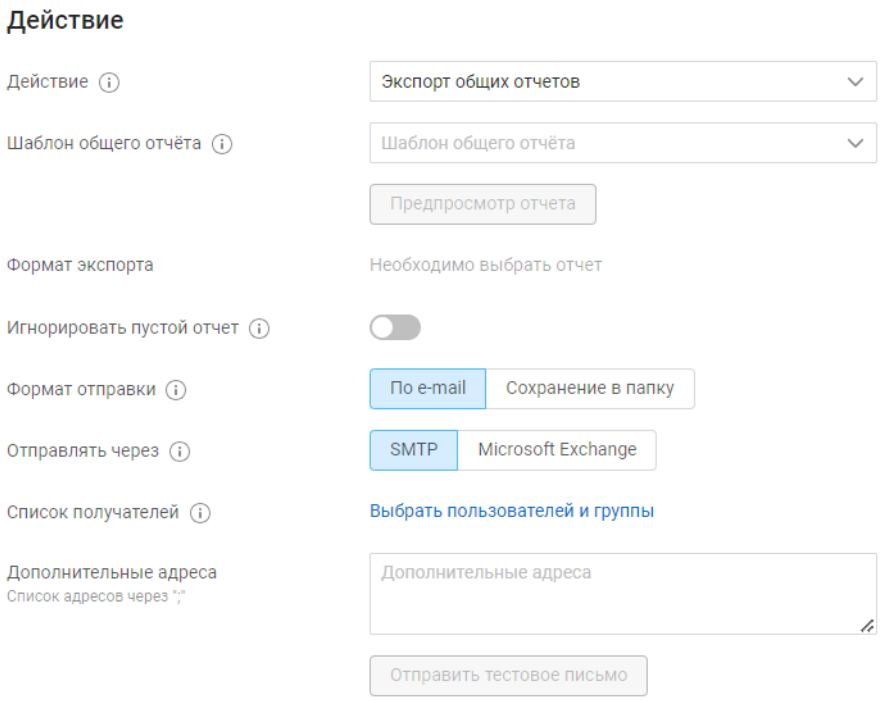


Рисунок 140 – Дополнительные поля для действия «Экспорт общих отчетов»

Таблица 43 – Состав и описание дополнительных полей для действия «Экспорт общих отчетов»

Поле	Описание
Поле «Шаблон общего отчёта»	Раскрывающийся список для выбора пользовательского или встроенного шаблона отчета
Поле «Формат экспорта»	Переключатель для выбора формата экспортируемого отчета. Для выбранного отчета могут быть доступны следующие форматы экспорта: pdf, xlxs, csv, xlm, docx и др.
Поле «Игнорировать пустой отчет»	Переключатель: — «Активен» ( ) – не экспортировать отчет без данных; — «Неактивен» ( ) – экспортировать все отчеты, в том числе без данных
Поле «Формат отправки»	Переключатель: — «По e-mail» – файл отчета отправляется на указанный адрес; — «Сохранение в папку» – файл отчета сохраняется в указанную папку. При изменении значения в поле изменяется набор дополнительных полей (см. ниже) Для отправки «По e-mail» предварительно необходимо выполнить настройку почтовых серверов («Настройки» → «Почтовые серверы» (см. п. 11.6))
Группа полей для формата отправки «По e-mail»	
Поле «Отправлять через»	Переключатель: — «SMTP» – отправка отчетов через SMTP; — «Microsoft Exchange» – отправка отчетов через Microsoft Exchange
Поле «Список получателей»	Является ссылкой. При переходе открывается окно для выбора пользователей и групп
Поле «Дополнительные адреса»	Поле для ввода дополнительных e-mail адресов. При наличии нескольких адресов вводить через «;»
Группа полей для формата отправки «Сохранение в папку»	
Поле «Доступ к директории»	Переключатель: — «Сетевой»;

Поле	Описание
	— «SSH подключение». При изменении значения в поле изменяется набор дополнительных полей (см. ниже)
Дополнительные поля для доступа «Сетевой»	
Поле «Путь до директории»	Текстовое поле для ввода пути до директории. Пример формата ввода: \\[имя сервера]\[имя директории] Сетевая директория должна быть доступна ПК «Efros DO»
Поле «Подключение»	Переключатель: — «Пользователь и пароль». Необходимо указать пользователя и пароль для доступа к директории; — «Анонимно»
Дополнительные поля для доступа «SSH подключение»	
Поле «Адрес сервера»	Текстовое поле для ввода адреса сервера. Пример формата ввода: [Адрес сервера]:[порт]
Поле «Пользователь»	Логин пользователя для доступа в директорию
Поле «Пароль»	Пароль пользователя для доступа в директорию
Поле «Путь до директории»	Текстовое поле для ввода пути до директории. Пример формата ввода: /[корневой каталог]/[имя директории]
Элементы управления	
Предпросмотр отчета	При нажатии кнопки откроется окно предпросмотра отчета выбранного шаблона отчета
Отправить тестовое письмо	При нажатии кнопки на e-mail отправится тестовое письмо
Проверить доступность директории	При нажатии кнопки выполняется проверка доступности директории

11 Раздел «Настройки»

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

Раздел «Настройки» 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.

11.1 TACACS+ и RADIUS

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

Подраздел «TACACS+ и RADIUS» 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:

- 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. 141). Состав и описание полей подраздела приведены в таблице 44.

Для настройки контроля доступа пользователю необходимо внести на странице необходимые изменения в параметры и нажать кнопку «Сохранить».

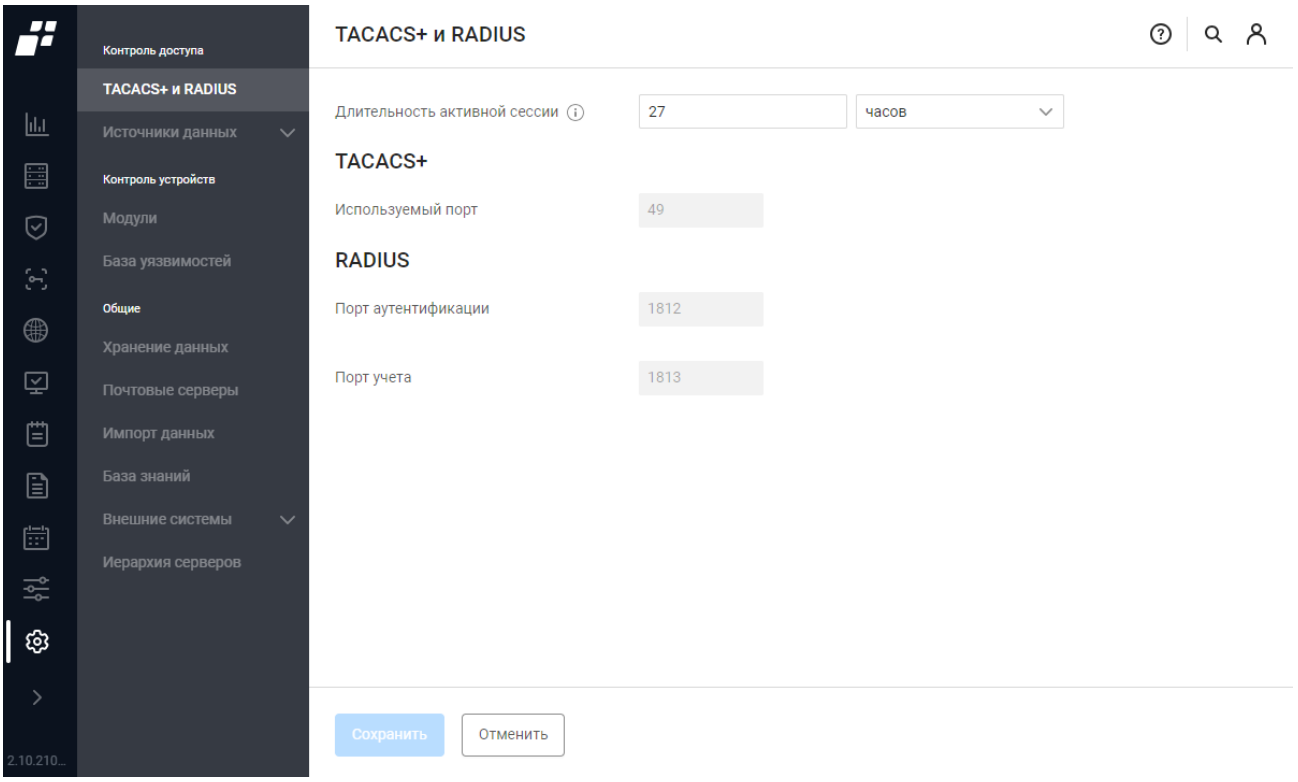


Рисунок 141 – Подраздел «TACACS+ и RADIUS»

Таблица 44 – Состав и описание полей страницы подраздела «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+. Значение по умолчанию: 49
*Группа полей протокола RADIUS	
Поле «Порт аутентификации»	Номер порта прослушивания пакетов аутентификации. По умолчанию прослушиваются все сервера в сети (значение «*») и порт прослушивания – 1812
Поле «Порт учета»	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 не доступны для редактирования	

11.2 Источники данных

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

11.2.1 Источник данных LDAP

Подраздел «Источники данных: LDAP» 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. 142).

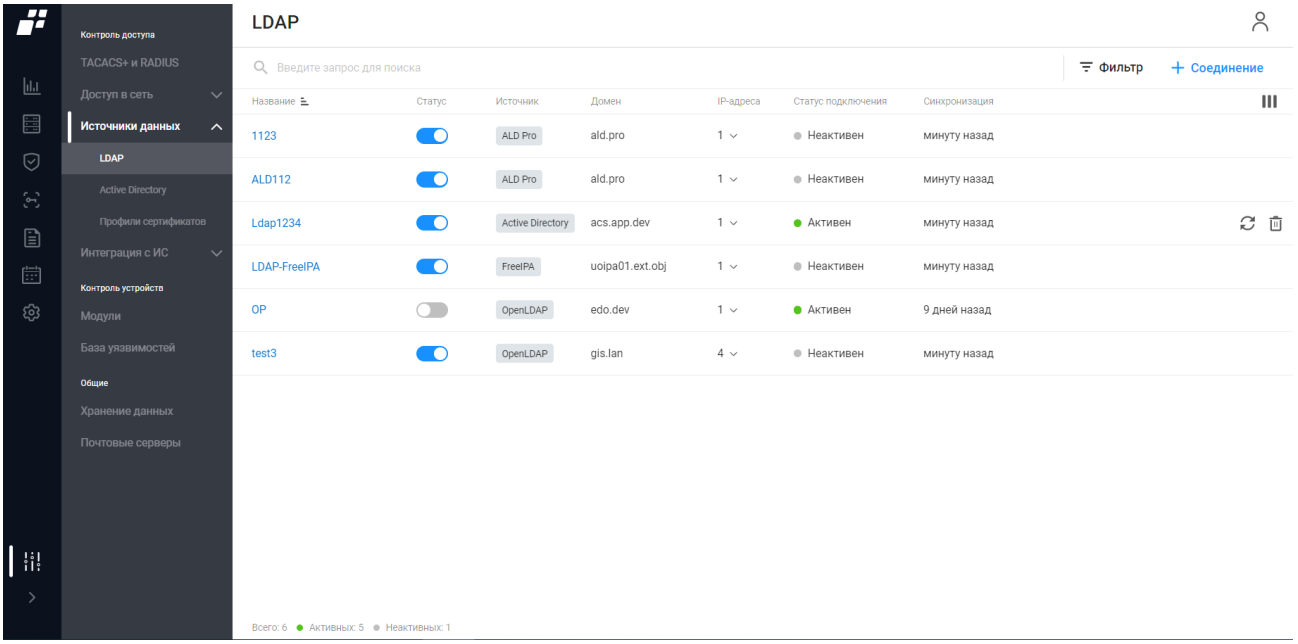


Рисунок 142 – Подраздел «Источники данных». Вкладка «LDAP»

На вкладке «LDAP» список соединений реализован в виде таблицы. Для каждой записи списка отображаются следующие данные:

- название устанавливаемого соединения;
- статус соединения (активно/неактивно);
- источник данных;
- домен;

— IP-адрес иди количество IP-адресов (является раскрывающимся списком с IP-адресами);
— статус подключения;
— дата последней синхронизации данных.

Над списком соединений расположены:

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

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.

11.2.1.1 Создание нового соединения LDAP

Для создания нового подключения к LDAP-серверу администратору необходимо:

1) Нажать кнопку «Соединение» (+ Соединение). Откроется страница «Создание LDAP соединения» (рис. 143).
2) Заполнить поля необходимыми параметрами и нажать кнопку «Создать». Состав и описание полей страницы приведены в таблице 45.
3) 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.

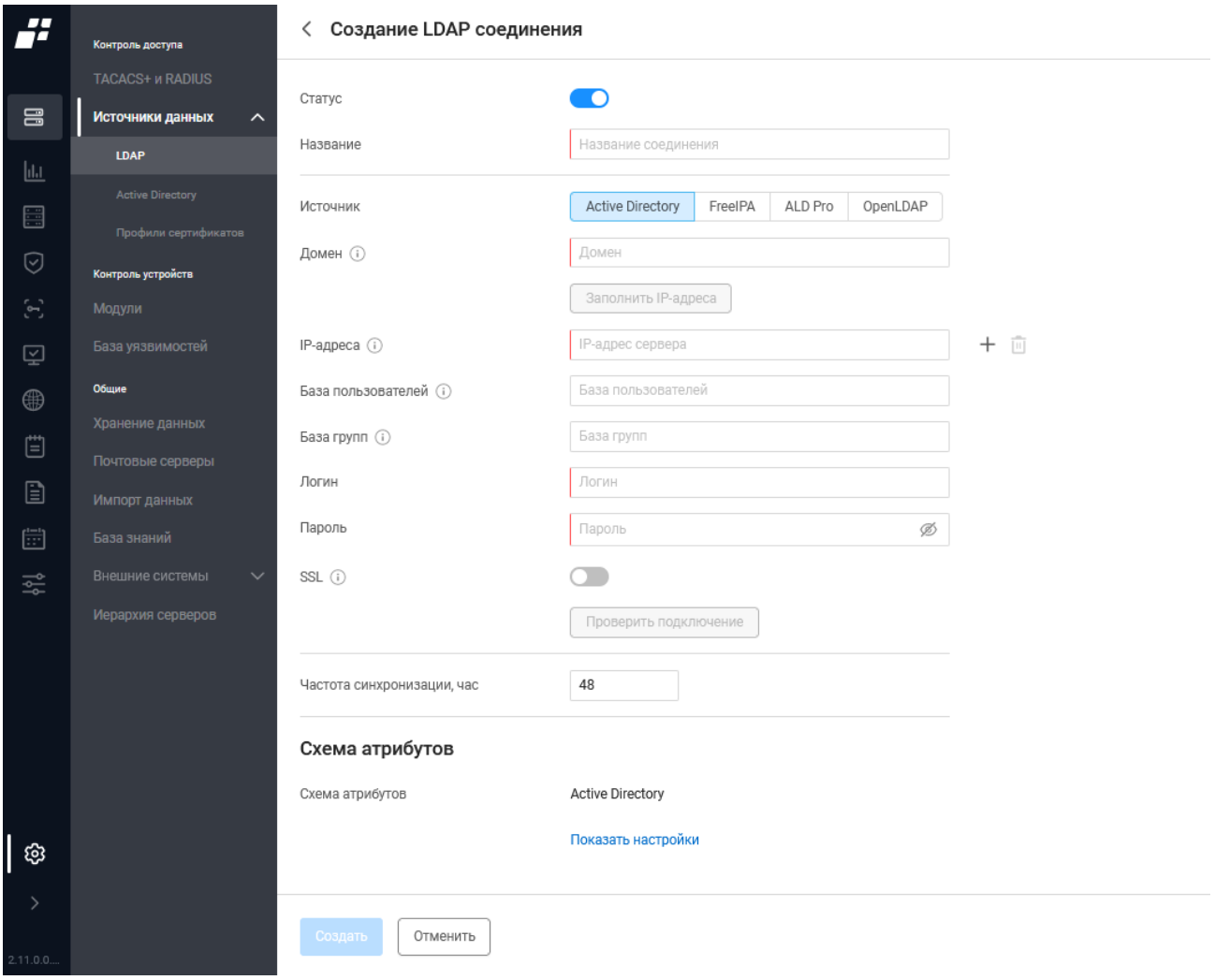


Рисунок 143 – Страница «Создание LDAP соединения»

Таблица 45 – Состав и описание полей страницы «Создание LDAP соединения»

Поле	Описание
Поле «Статус»	Содержит переключатель с двумя положениями: — «Включено» ( ) – соединение включено; — «Выключено» ( ) – соединение 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»	Переключатель для выбора типа источника данных: — «Active Directory»; — «FreeIPA»; — «ALD Pro»; — «OpenLDAP» В зависимости от выбранного источника, по умолчанию

Поле	Описание
	будет использована соответствующая схема атрибутов. При необходимости, ее можно отредактировать самостоятельно (подробнее см. ниже)
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
Кнопка «Заполнить IP-адреса»	Становится активна после заполнения поля «Домен» (см. выше). По нажатию кнопки автоматически заполняется поле «IP-адреса» (см. ниже). Если определить автоматически IP-адреса не удалось, то отобразится сообщение об ошибке
Поле «IP-адреса»	IP-адреса серверов служб каталогов для синхронизации пользователей и групп. Определяются автоматически после нажатия кнопки «Заполнить IP-адреса, если корректно заполнено поле «Домен» и доступен сервер DNS, или могут быть заданы вручную. При необходимости добавления нескольких IP-адресов нужно нажать кнопку « + », при необходимости удалить – нажать кнопку « 🗑 ». 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: cn=users,cn=accounts,dc=ald,dc=pro.
Поле «База групп»	Поле для ввода уровня, с которого будет осуществляться

Поле	Описание
	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 синхронизации, час»	Поле для ввода числового значения времени обновления подключения (от 1 до 4368 часов)
Группа полей «Схема атрибутов»	
Поле «Схема атрибутов»	Отображается выбранный ранее в поле «Тип источника» тип LDAP-сервера. Содержит ссылку «Показать настройки». При переходе по ссылке появляются поля, которые содержат значения по умолчанию. При подключении к новой службе каталогов администратору необходимо проверить их на соответствие. Состав настроек: 1) Идентификатор объекта. 2) Атрибуты пользователей: — «Отображаемое имя»; — «Имя аккаунта»;

Поле	Описание
	— «Группы пользователя»; — «Сертификат». 3) 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

11.2.2 Источник данных Active Directory

Вкладка «Active Directory» подраздела «Источники данных» предназначена для настройки параметров работы модуля интеграции «Efros NAC» с контроллером домена, в котором хранятся учетные записи сетевых устройств, контролируемых модулем интеграции «Efros NAC» (рис. 144).

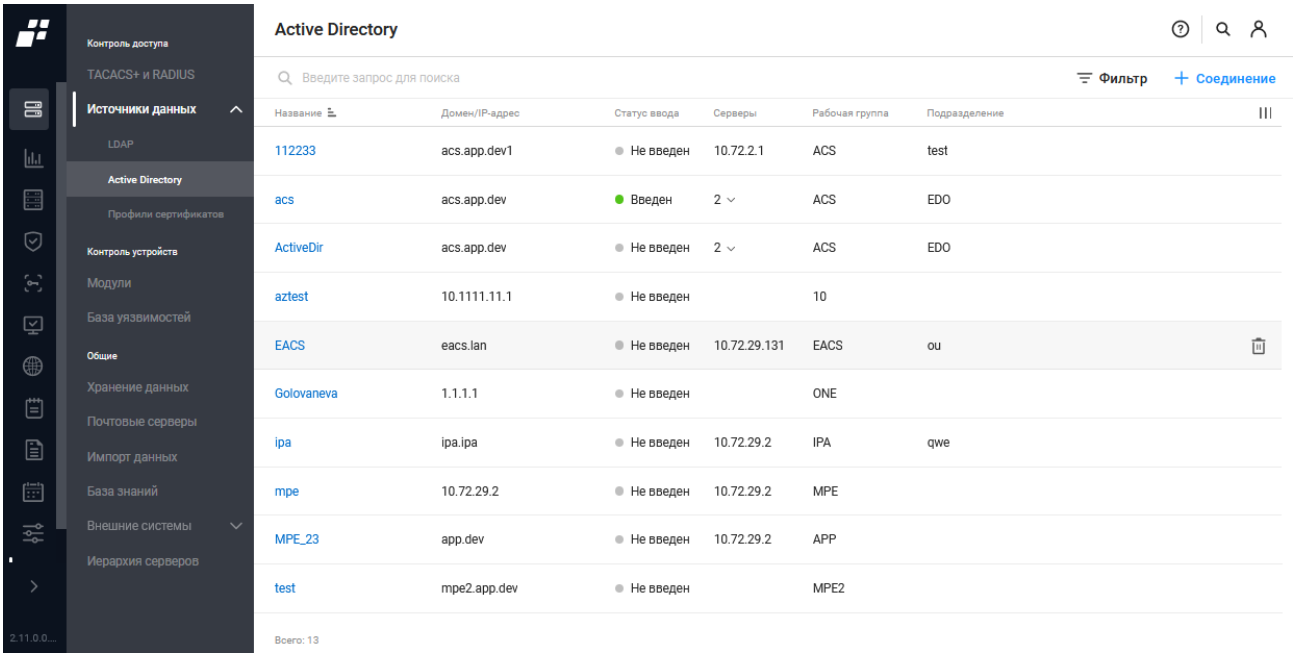


Рисунок 144 – Подраздел «Источники данных». Вкладка «Active Directory»

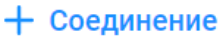
На странице вкладки список соединений реализован в виде таблицы. Для каждой записи списка отображаются следующие данные:

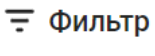
— наименование устанавливаемого соединения;
— имя или IP-адрес домена, к которому подключается сервер ПК «Efros DO»;
— статус ввода ПК «Efros DO» сервера в домен;

— сервер аутентификации или количество серверов аутентификации (является раскрывающимся списком с серверов аутентификации);
— имя рабочей группы;
— учетная запись сервера ПК «Efros DO» в определенном подразделении.

Над списком соединений располагаются:

— поле поиска (

 );
— кнопка «Соединение» (

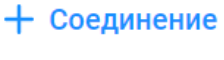
 );
— кнопка «Фильтр» (

 );
— кнопка «Колонки» ().

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

11.2.2.1 Создание нового соединения Active Directory

Для выполнения настройки подключения к серверу аутентификации необходимо:

1) Нажать кнопку «Соединение» (

).
2) Откроется страница «Создание Active Directory соединения» (рис. 145). Заполнить поля необходимыми параметрами. Состав и описание полей страницы приведены в таблице 46.
3) Нажать кнопку «Ввести в домен». Будет запущен процесс ввода сервера в домен.
4) 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» в окне, аналогичном окну ввода в домен (см. рис. 145). При этом параметры подключения, установленные ранее, не удаляются и могут быть применены для повторного ввода сервера в домен или изменены.

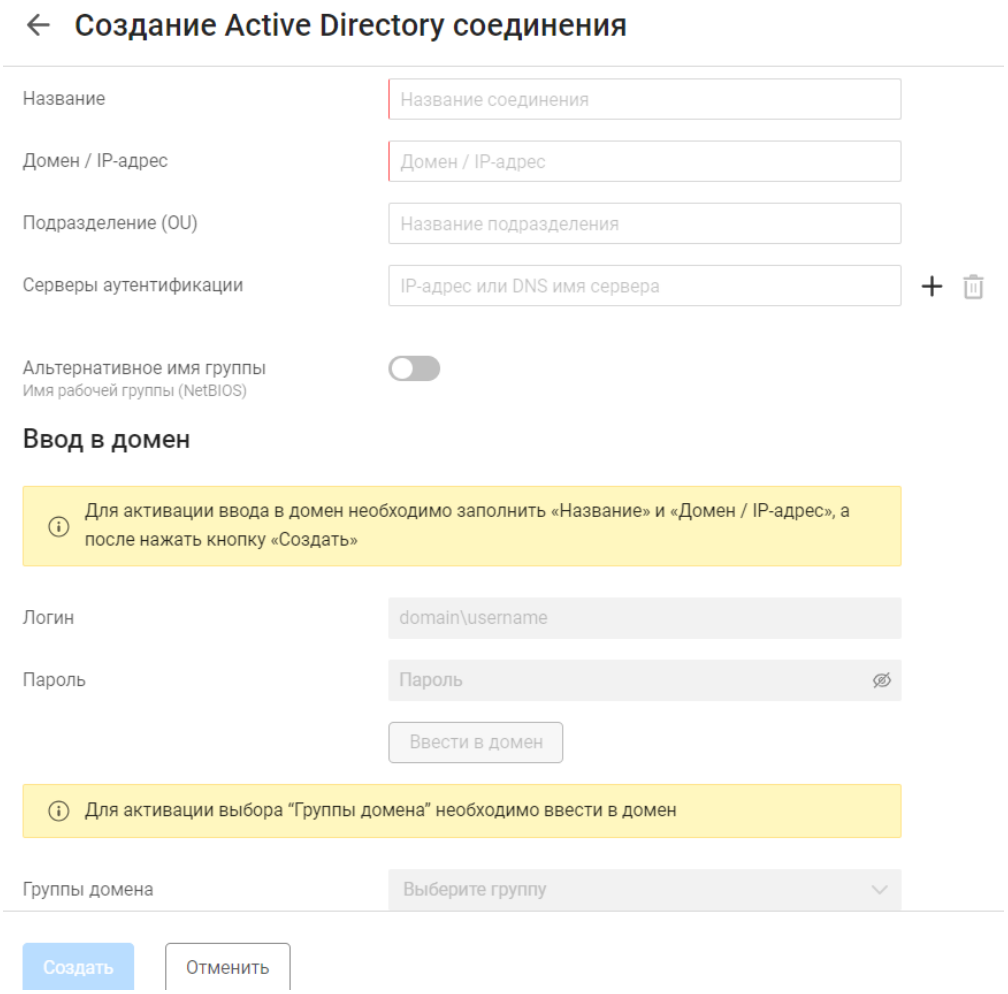


Рисунок 145 – Страница «Создание Active Directory соединения»

Таблица 46 – 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».

Поле	Описание
	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, «_», «–». При необходимости добавления нескольких IP-адресов или DNS имен сервера нужно нажать кнопку « + », при необходимости удалить – нажать кнопку « 🗑 »
Поле «Альтернативное имя группы»	Переключатель: — «Используется» ( ) – при подключении к серверу аутентификации используется имя рабочей группы (NetBIOS); — «Не используется» ( ). При включенном положении переключателя отображается дополнительное поле для ввода альтернативного имени 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». Доступен для заполнения только после создания соединения с указанными выше параметрами (после нажатия кнопки «Создать»)	
Поле «Логин»	Поле для ввода логина пользователя, настраивающего подключение. Параметры ввода текста: от 1 до 256 любых символов
Поле «Пароль»	Поле для ввода пароля пользователя, настраивающего подключение. Параметры ввода текста: от 1 до 500 любых символов
Кнопка «Ввести в домен»	Запуск процесса ввода сервера в домен
Поле «Группы домена»	Содержит ссылку, при выборе которой открывается окно выбора групп пользователей домена. Группы выбираются установкой флага в полях требуемых групп во вкладке «Поиск по домену». Выбранные группы отображаются во вкладке «Выбранные». Изменения сохраняются по нажатию в окне кнопки «Изменить»
Элементы управления	
Создать	При нажатии кнопки выполняется сохранение внесенных данных

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

11.2.3 Профили сертификатов

Вкладка «Профили сертификатов» подраздела «Источники данных» предназначеан для ведения (создание/удаление/редактирование) списка профилей сертификатов, используемых при настройке политик аутентификации в политиках доступа устройств (рис. 146).

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

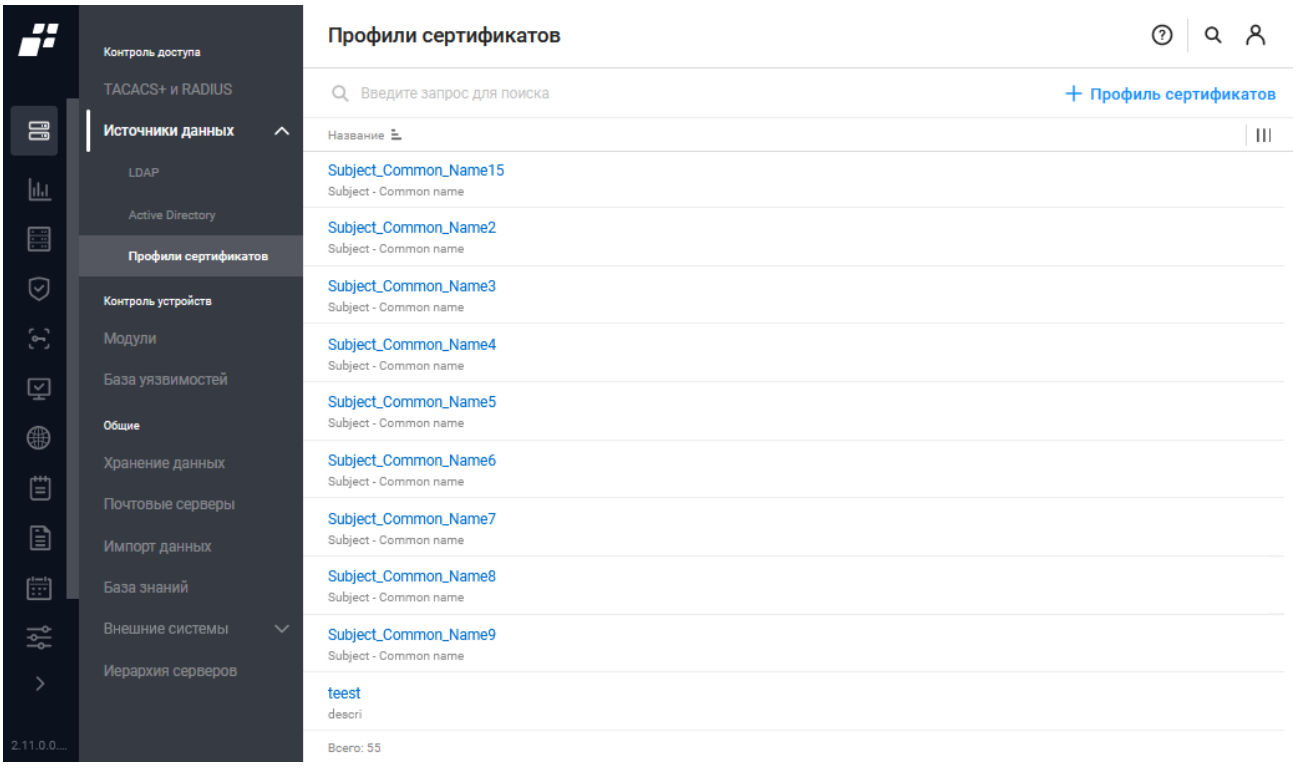


Рисунок 146 – Подраздел «Источники данных». Вкладка «Профили сертификатов»

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);
- кнопка «Профиль сертификатов» (+ Профиль сертификатов);
- кнопка «Колонки» ( ).

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

11.2.3.1 Создание нового профиля сертификата

Для создания профиля сертификата пользователю необходимо:

1) Нажать кнопку «Профиль сертификатов» (+ Профиль сертификатов).
2) Откроется страница «Создание профиля сертификатов» (см. рис. 147). Заполнит страницу необходимыми параметрами и нажать кнопку «Создать». Состав и описание полей окна приведены в таблице 47.

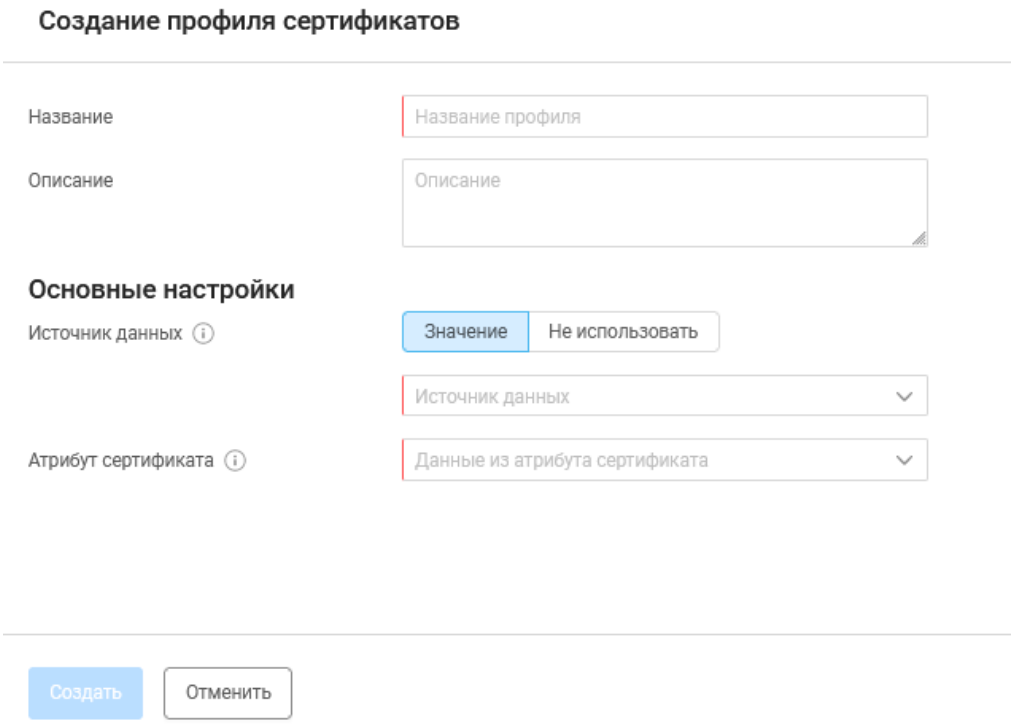


Рисунок 147 – Окно «Создание профиля сертификатов»

Таблица 47 – 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, «_», «–»
Основные настройки	

Поле	Описание
Поле «Источник данных»	Переключатель: — «Значение» – проверка сертификата будет производиться; — «Не использовать» – проверка атрибута сертификата не производится. При выборе положения «Значение» становится доступно поле со списком для выбора источника данных для проверки атрибута сертификата. Список содержит значения: — InternalUsers (сетевые пользователи); — InternalEndPoints (разрешенные MAC-адреса); — данные списка LDAP с префиксом «(LDAP)»; — данные списка Active Directory с префиксом «(DOMAIN)»
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

11.3 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».

Подраздел «Модули» предоставляет пользователю комплекса информацию о всех внешних модулях, подключенных к комплексу.

Модули соединяют сервер комплекса с устройствами по различным коммуникационным протоколам. Типы модулей ПК «Efros DO» бывают:

— модули сетевые;
— модули виртуализации;
— модули операционных систем;
— модули сервисные;

— модули приложения;
— пользовательские модули.

11.3.1 Просмотр установленных модулей

На странице вкладки «Сетевые» подраздела «Модули» список модулей реализован в виде таблицы (рис. 148). В названии вкладки указано, сколько модулей активно на данный момент.

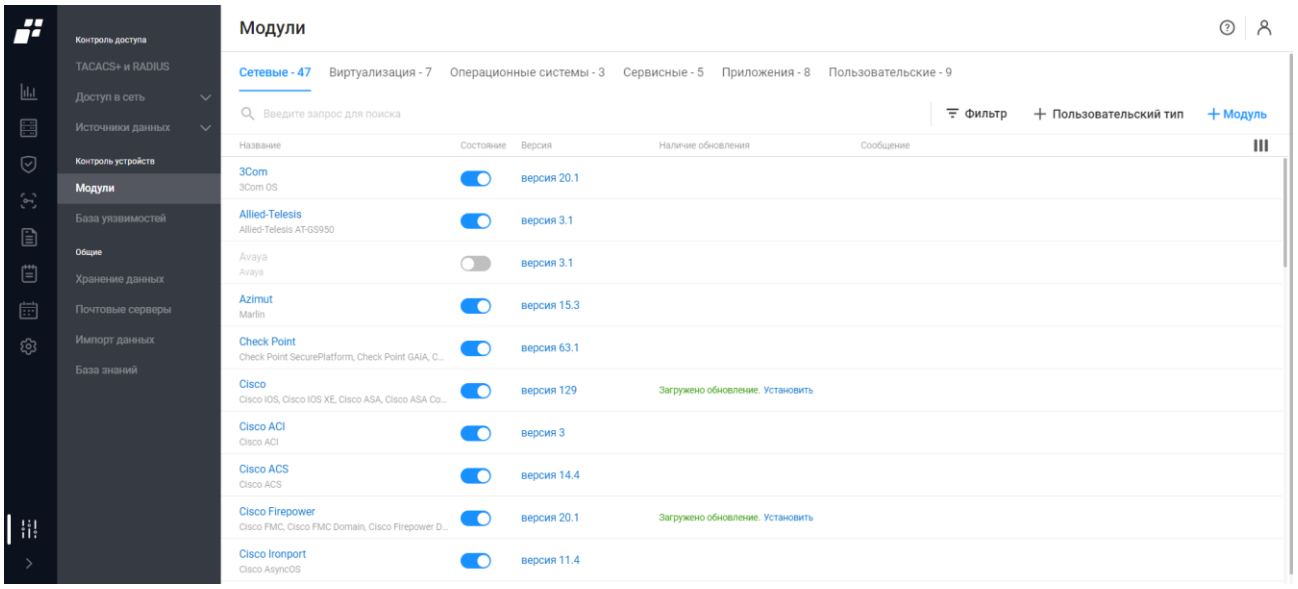


Рисунок 148 – Подраздел «Модули». Вкладка «Сетевые»

Для каждой записи списка отображаются следующие данные[10]:

— название модуля – доступна сортировка по имени модуля в алфавитном порядке;
— состояние модуля (подключен/отключен);
— версия модуля;
— наличие обновления;
— краткое сообщение.

Над списком доступны:

— поле поиска (Введите запрос для поиска);
— кнопка «Модуль» (+ Модуль);
— кнопка добавления пользовательского типа сетевого устройства (+ Пользовательский тип);
— кнопка «Фильтр» (Фильтр);
— кнопка «Колонки» ( ).

Состав и описание вкладок «Виртуализация», «Операционные системы»,

[10] Для пользовательских модулей отображаются только название и состояние

«Сервисные», «Приложения», «Пользовательские» подраздела «Модули» аналогичен составу вкладки «Сетевые».

11.3.2 Добавление модуля

Для добавления нового модуля администратору необходимо:

1) В заголовке любой вкладки подраздела «Модули» нажать кнопку «Модуль» (+ Модуль).
2) Выбрать в открывшемся стандартном окне используемой ОС файл добавляемого модуля и нажать кнопку «Открыть».
3) Подтвердить загрузку файла, нажав в открывшемся окне «Загрузка модуля» (рис. 149) кнопку «Загрузить».

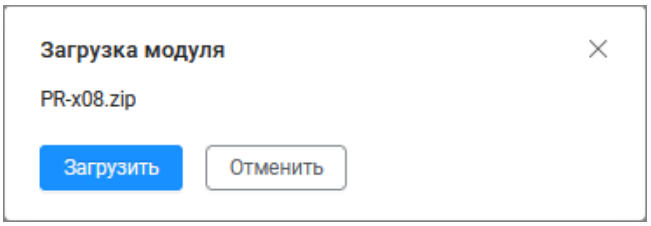


Рисунок 149 – Окно «Загрузка модуля»

Размер загружаемого файла не должен превышать 300 Мбайт.

После завершения загрузки во вкладке подраздела «Модули», соответствующей типу загруженного модуля, добавится строка добавленного модуля.

11.3.3 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» (+ Пользовательский тип). Откроется страница «Создание пользовательского типа сетевого устройства» (рис. 150)

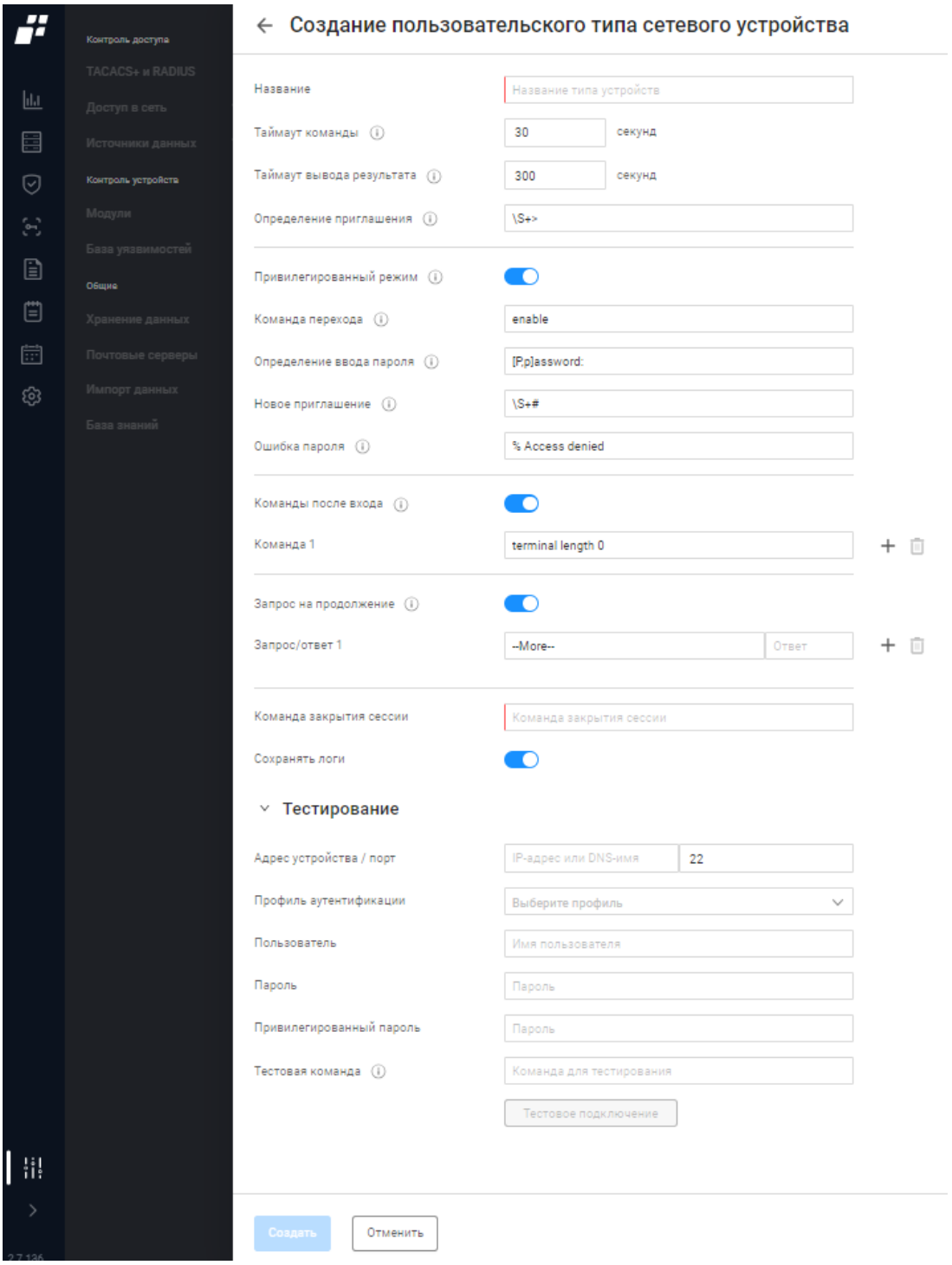


Рисунок 150 – Страница «Создание пользовательского типа сетевого устройства»

Таблица 48 – Состав и описание полей страницы «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	Описание
Поле «Таймаут команды»	Время ожидания ответа при выполнении команд на устройстве (секунд)
Поле «Таймаут вывода результата»	Время ожидания вывода результата при запросе 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: — «Активен» ( ) – включает привилегированный режим и дополнительные поля настройки режима; — «Неактивен» ( ) – выключает привилегированный режим и дополнительные поля настройки режима. По умолчанию переключатель установлен в положение «Включен» и поля для ввода параметров работы в привилегированном режиме (см. ниже) 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: — «Активен» ( ) – включает отображение блока полей дополнительного набора команд; — «Неактивен» ( ) – выключает отображение блока полей дополнительного набора команд. По умолчанию переключатель установлен в положение «Включен» и в окне отображается блок полей для добавления дополнительных команд (см. ниже)

Поле	Описание
Блок полей для добавления дополнительных команд Поле	По умолчанию содержи поле «Команда 1» для ввода первой дополнительной команды для настройки устройства. Параметры ввода текста: от 1 до 250 любых символов. При необходимости добавления следующей команды нужно нажать кнопку « + », при необходимости удалить лишнюю – нажать кнопку « 🗑 »
Поле «Запрос на продолжение»	Переключатель: — «Активен» ( ) – включает отображение полей с запросами на продолжение; — «Неактивен» ( ) – выключает отображение полей с запросами на продолжение. По умолчанию переключатель установлен в положение «Включен» и в окне отображается блок полей для добавления дополнительных запросов/ответов (см. ниже)
Блок полей для добавления дополнительных запросов/ответов	По умолчанию содержи поле ««Запрос/ответ 1» для ввода первой пары 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 При необходимости добавления следующей пары запрос/ответ нужно нажать кнопку « + », при необходимости удалить лишнюю – нажать кнопку « 🗑 »
Поле «Команда закрытия сессии»	Текстовое поле ввода команды. Параметры ввода текста: от 1 до 255 любых символов
Поле «Сохранять логи»	Переключатель: — «Активен» ( ) – включает сохранение логов сессии; — «Неактивен» ( ) – выключает сохранение логов сессии
Группа полей «Тестирование»	
Поле «Адрес устройства / порт»	Для ввода IP-адреса или доменного имени устройства и порта подключения
Поле «Профиль аутентификации»	Раскрывающийся список созданных профилей аутентификации в комплексе. Профиль аутентификации содержит в себе имя учетной записи (логин) и пароль,

Поле	Описание
	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 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
Кнопка «Тестовое подключение»	По нажатию кнопки выполняется проверка подключения и выполнения заданной команды
Элементы управления	
Создать	При нажатии кнопки выполняется сохранение внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу без сохранения внесенных данных

11.3.4 Настройка сетевого модуля

Для настройки сетевого модуля необходимо нажать на название-ссылку настраиваемого модуля. Откроется окно настройки (рис. 151):

- включить переключатель «Разрешить сохранение логов»;
- нажать кнопку «Сохранить».

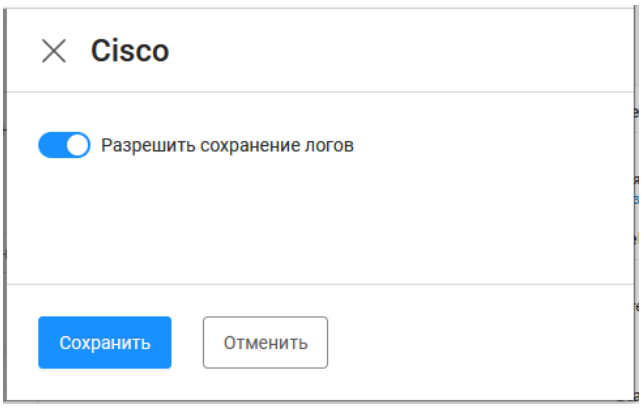


Рисунок 151 – Пример окна настройки модуля Cisco

11.4 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 их обнаружения (рис. 152).

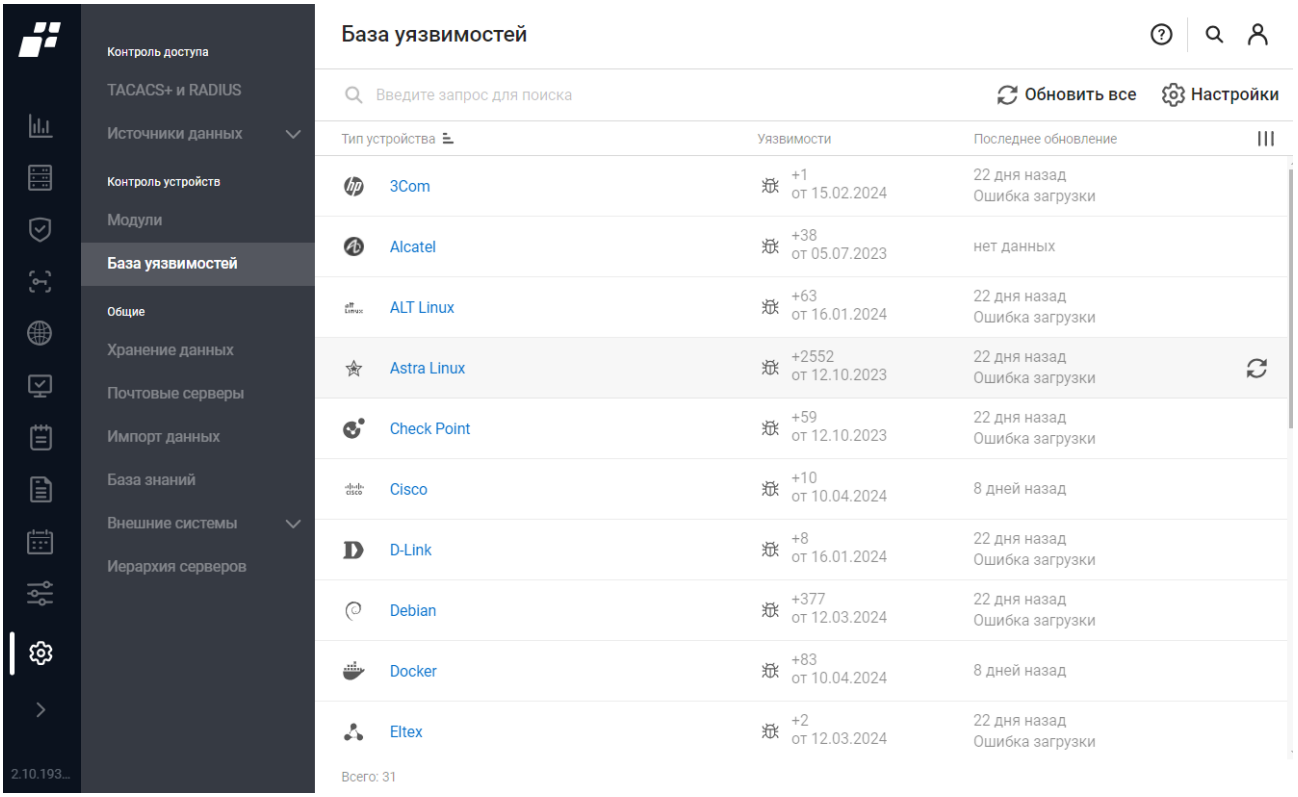


Рисунок 152 – Подраздел «База уязвимостей»

На странице список типов устройств с перечнем данных по уязвимостям реализован в виде таблицы.

Для каждой записи списка отображаются следующие данные:

- тип устройства;
- количество выявленных уязвимостей;
- время последнего обновления БДУ.

Над списком располагаются:

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

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

устрйоства.

11.4.1 Настройка базы уязвимостей

Для выполнения настройки базы уязвимостей пользователю необходимо:

1) Нажать кнопку «Настройки» (Настройки).
2) Откроется окно «Настройка сервера обновлений» (рис. 153). Заполнить поля необходимыми параметрами и нажать кнопку «Сохранить». Состав и описание полей окна приведены в таблице 49.
3) Введенные значения будут сохранены в БД ПК «Efros DO», будет запущен процесс обновления конфигурационного файла сервиса.

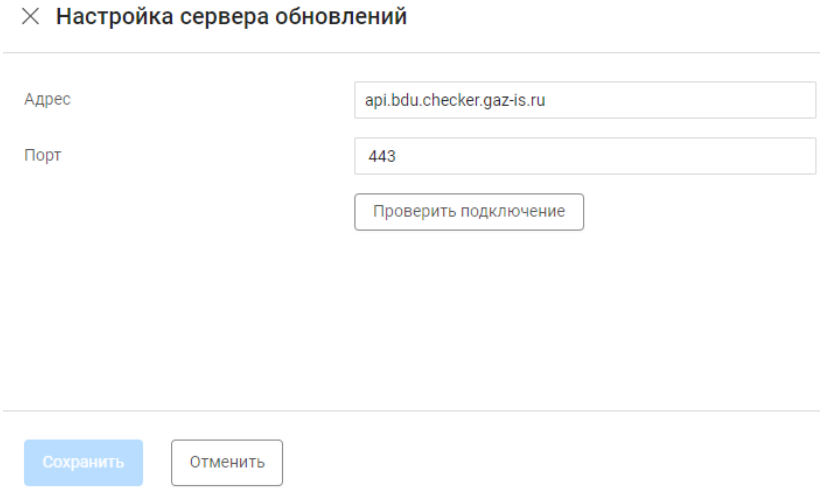


Рисунок 153 – Окно «Настройка сервера обновлений»

Таблица 49 – Состав и описание полей окна «Настройка сервера обновлений»

Поле	Описание
Поле «Адрес»	Поле для ввода 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 подключение»	В случае корректно установленных параметров рядом с кнопкой «Проверить подключение» появится надпись *«Успешно»* и ссылка на лог операций
Элементы управления	
Сохранить	При нажатии кнопки выполняется сохранение внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу без сохранения внесенных данных

11.5 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».

Подраздел «Хранение данных» (рис. 154) позволяет пользователю устанавливать сроки и объем хранения данных по устройствам, событиям и потокам данных для предотвращения переполнения БД комплекса. Состав и описание полей страницы приведены в таблице 50. Временные параметры могут быть заданы в интервале от 1 до 1825 дней.

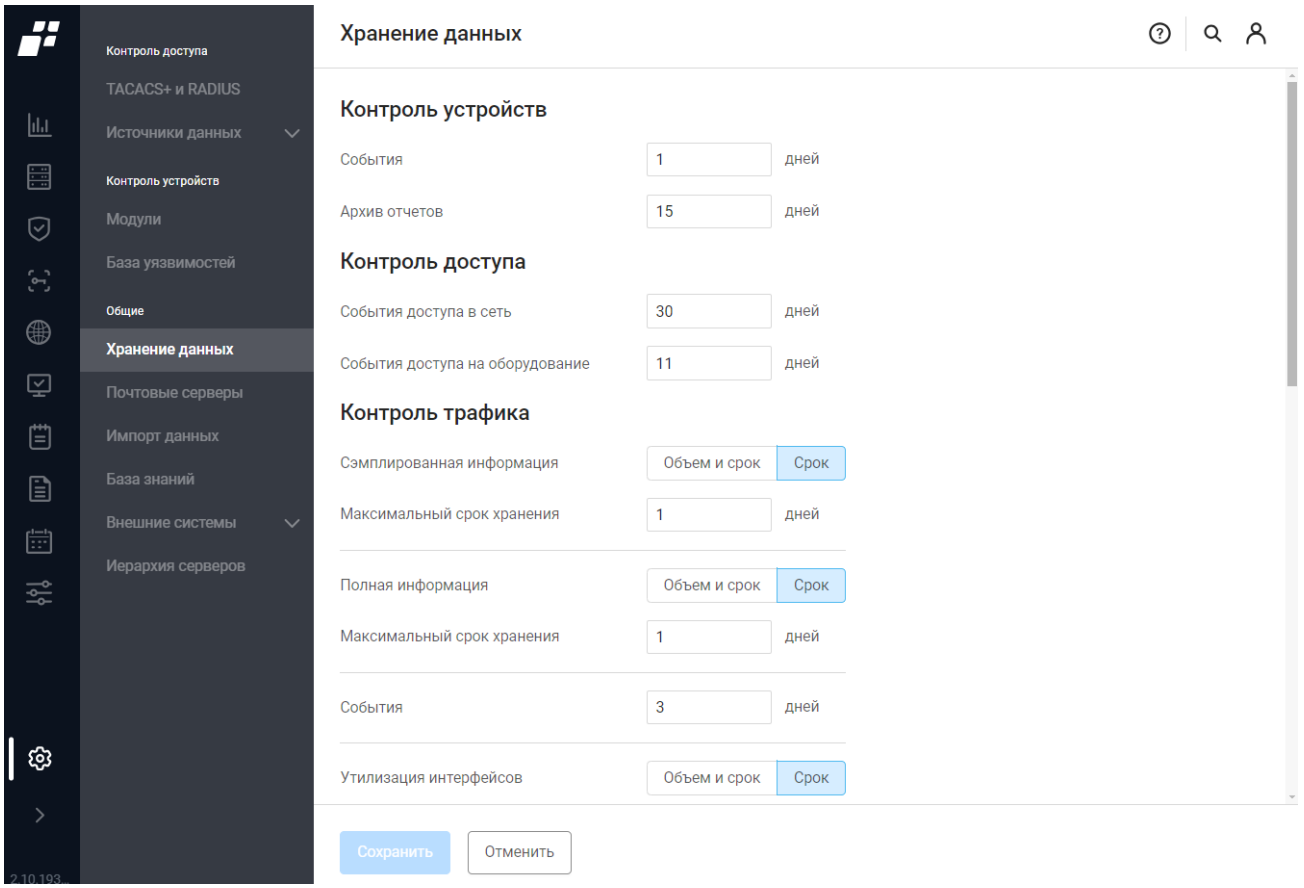


Рисунок 154 – Подраздел «Хранение данных»

Таблица 50 – Состав и описание полей подраздела «Хранение данных»

Поле	Описание
Группа полей «Контроль устройств»	
Поле «События»	Поле для ввода количества дней хранения записей событий раздела «Клонтроль устройств». Значение по умолчанию: 30
Поле «Архив отчетов»	Поле для ввода количества дней хранения отчетов устройств раздела «Клонтроль устройств» в архиве. Значение по

Поле	Описание
	умолчанию: 15
Группа полей «Контроль доступа»	
Поле «События доступа в сеть»	Поле для ввода количества дней хранения записей событий доступа в сеть. Значение по умолчанию: 30
Поле «События доступа на оборудование»	Поле для ввода количества дней хранения записей событий доступа на оборудование. Значение по умолчанию: 11
Группа полей «Контроль трафика»	
Поле «Сэмплированная информация»	Переключатель с двумя положениями: — *«Объем и срок» – архив сэмплированной информации может достигать определенного объема и хранится определенное время; — «Срок» – архив хранится определенное время. *При выборе варианта «Объем и срок» появляется поле «Максимальный объем» в МБ (значение по умолчанию: 50000)
Поле «Максимальный срок хранения»	Поле для ввода максимального срока хранения сэмплированной информации в днях. Значение по умолчанию: 1
Поле «Полная информация»	Переключатель с двумя положениями: — *«Объем и срок» – архив полной информации может достигать определенного объема и хранится определенное время; — «Срок» – архив хранится определенное время. *При выборе варианта «Объем и срок» появляется поле «Максимальный объем» в МБ (значение по умолчанию: 50000)
Поле «Максимальный срок хранения»	Поле для ввода максимального срока хранения полной информации в днях. Значение по умолчанию: 1
Поле «События»	Указывается максимальный срок хранения событий потоеов данных в днях. Значение по умолчанию: 3
Поле «Утилизация интерфейсов»	Переключатель с двумя вариантами: — *«Объем и срок» – архив информации по триннерам утилизации интерфейсов может достигать определенного объема и хранится определенное время; — «Срок» – архив хранится определенное время. *При выборе варианта «Объем и срок» появляется поле

Поле	Описание
	«Максимальный объем» в МБ (значение по умолчанию: 50000)
Поле «Максимальный срок хранения»	Поле для ввода максимального срока хранения информации об интерфейсах в днях. Значение по умолчанию: 15
Группа полей «Общее»	
Поле «События по объектам сети»	Переключатель с двумя вариантами: — *«Объем и срок» – архив событий по объектам сети может достигать определенного объема и хранится определенное время; — «Срок» – архив хранится определенное время. *При выборе варианта «Объем и срок» появляется поле «Максимальный объем» в МБ (значение по умолчанию: 50000)
Поле «Максимальный срок хранения»	Поле для ввода максимального срока хранения событий по объекту сети в днях. Значение по умолчанию: 15
Поле «Системные события»	Поле для ввода количества дней хранения отчета по системным событиям. Значение по умолчанию: 6
Поле «Аудит действий пользователя»	Переключатель с двумя вариантами: — *«Объем и срок» – архив аудита действий пользователей может достигать определенного объема и хранится определенное время; — «Срок» – архив хранится определенное время. *При выборе варианта «Объем и срок» появляется поле «Максимальный объем» в МБ (значение по умолчанию: 50000)
Поле «Максимальный срок хранения»	Поле для ввода максимального срока хранения аудита действий пользователя в днях. Значение по умолчанию: 15
Поле «Срабатывания планировщика»	Поле для ввода количества дней хранения отчета событий планировщика. Значение по умолчанию: 15
Группа полей «База знаний»	
Поле «Общие данные базы знаний»	Поле для ввода количества дней хранения данных базы знаний. Значение по умолчанию: 15
Поле «Данные профилирования»	Поле для ввода количества дней хранения данных от источников профилирования. Значение по умолчанию: 15
Поле «Данные от сканеров	Переключатель с двумя вариантами: — *«Объем и срок» – архив данных от сканеров

Поле	Описание
уязвимостей»	уязвимостей может достигать определенного объема и хранится определенное время; — «Срок» – архив хранится определенное время. *При выборе варианта «Объем и срок» появляется поле «Объем (Количество)» сканирований (значение по умолчанию: 10)
Поле «Максимальный срок хранения»	Поле для ввода максимального срока хранения данных от каждого сканера уязвимостей в разделе «Планировщик» в днях. Значение по умолчанию: 15
Группа полей «Агенты»	
Поле «События по агентам»	Переключатель с двумя вариантами: — *«Объем и срок» – архив данных от агентов может достигать определенного объема и хранится определенное время; — «Срок» – архив хранится определенное время. *При выборе варианта «Объем и срок» появляется поле «Максимальный объем» в МБ (значение по умолчанию: 50000)
Поле «Максимальный срок хранения»	Поле для ввода максимального срока хранения данных от каждого агента в днях. Значение по умолчанию: 15
Элементы управления	
Сохранить	При нажатии кнопки выполняется сохранение внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу без сохранения внесенных данных

11.6 Почтовые серверы

Отображаемые данные и доступная функциональность подраздела «Почтовые серверы» зависят от наличия хотя бы одной из лицензий.

Подраздел «Почтовые серверы» (рис. 155) позволяет пользователю настраивать параметры почтовых серверов для отправки сообщений. Состав и описание полей страницы подраздела приведены в таблице 51.

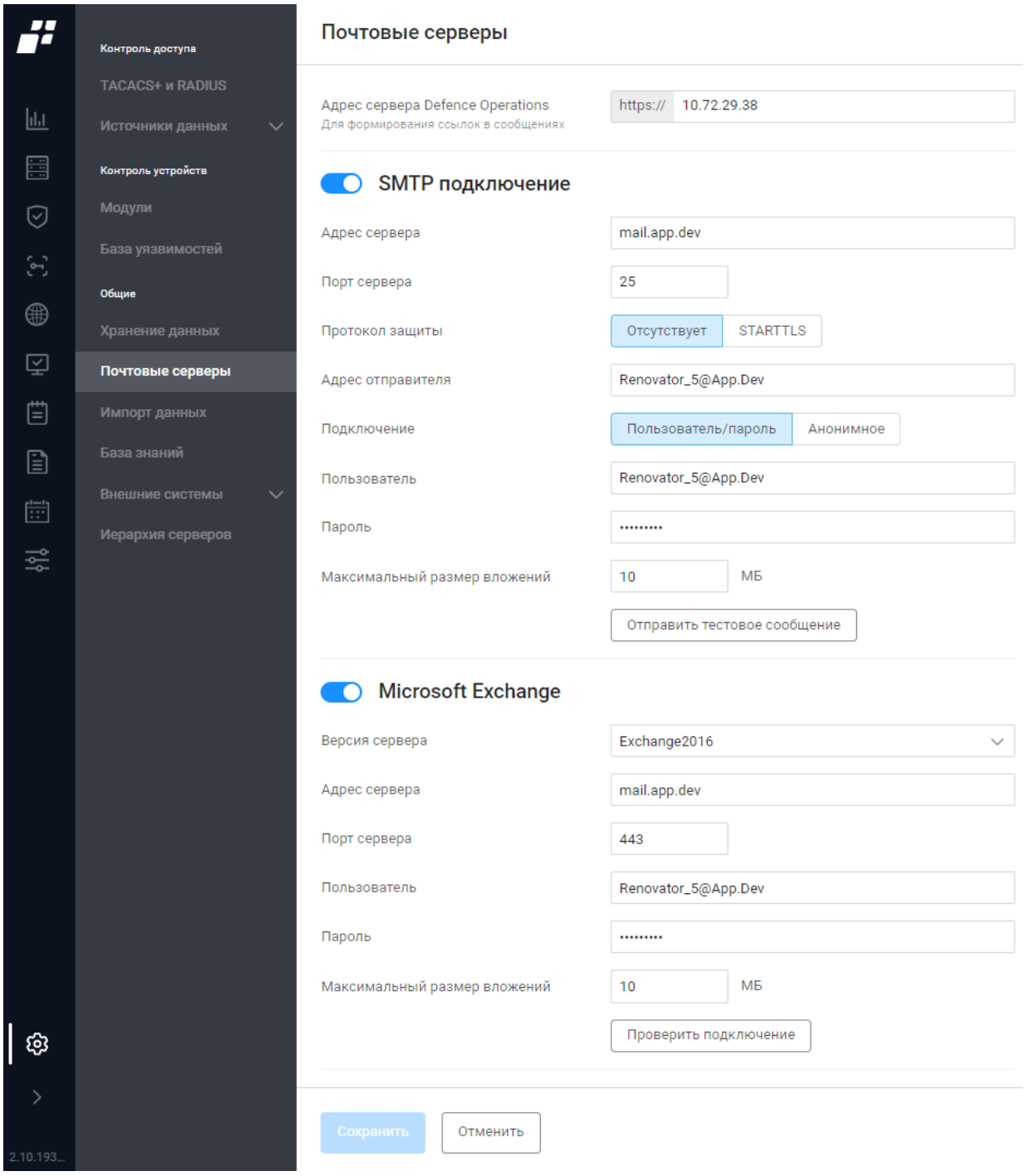


Рисунок 155 – Подраздел «Почтовые серверы»

Таблица 51 – 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 блока настройки SMTP подключения

Поле	Описание
Поле «Адрес сервера»	Адрес почтового сервера
Поле «Порт сервера»	Порт выбранного выше почтового сервера
Протокол защиты	Переключатель для включения/отключения протокола STARTTLS: — «Отсутствует»; — «STARTTLS»
Поле «Fingerprint ключа сервера»	Переключатель для включения/отключения сбора информации об удаленном сервере. Поле отображается, если выше выбран протокол STARTTLS
Поле «Адрес отправителя»	Почта отправителя сообщения
Поле «Подключение»	Переключатель для выбора типа подключения: — «Пользователь/пароль»; — «Анонимное»
Поле «Пользователь»	Логин пользователя. Если поле не заполнено, то в качестве пользователя используется адрес отправителя. Поле отображается, если выбран тип подключения «Пользователь/пароль»
Поле «Пароль»	Пароль отправителя сообщения. Поле отображается, если выбран тип подключения «Пользователь/пароль»
Поле «Максимальный размер вложений»	Максимальный суммарный размер вложений, прикрепленных к сообщению
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 блока настройки Microsoft Exchange
Поле «Версия сервера»	Окно с раскрывающимся списком для выбора версии сервера Exchange
Поле «Адрес сервера»	Адрес выбранной выше версии сервера
Поле «Порт сервера»	Порт выбранного выше сервера
Поле «Пользователь»	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	

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

11.7 Импорт данных

Отображаемые данные и доступная функциональность в подразделе «Импорт данных» зависят от наличия хотя бы одной лицензии на функциональные модули.

Подраздел «Импорт данных» (рис. 156) позволяет пользователю импортировать необходимые данные, исключая их ввод вручную.

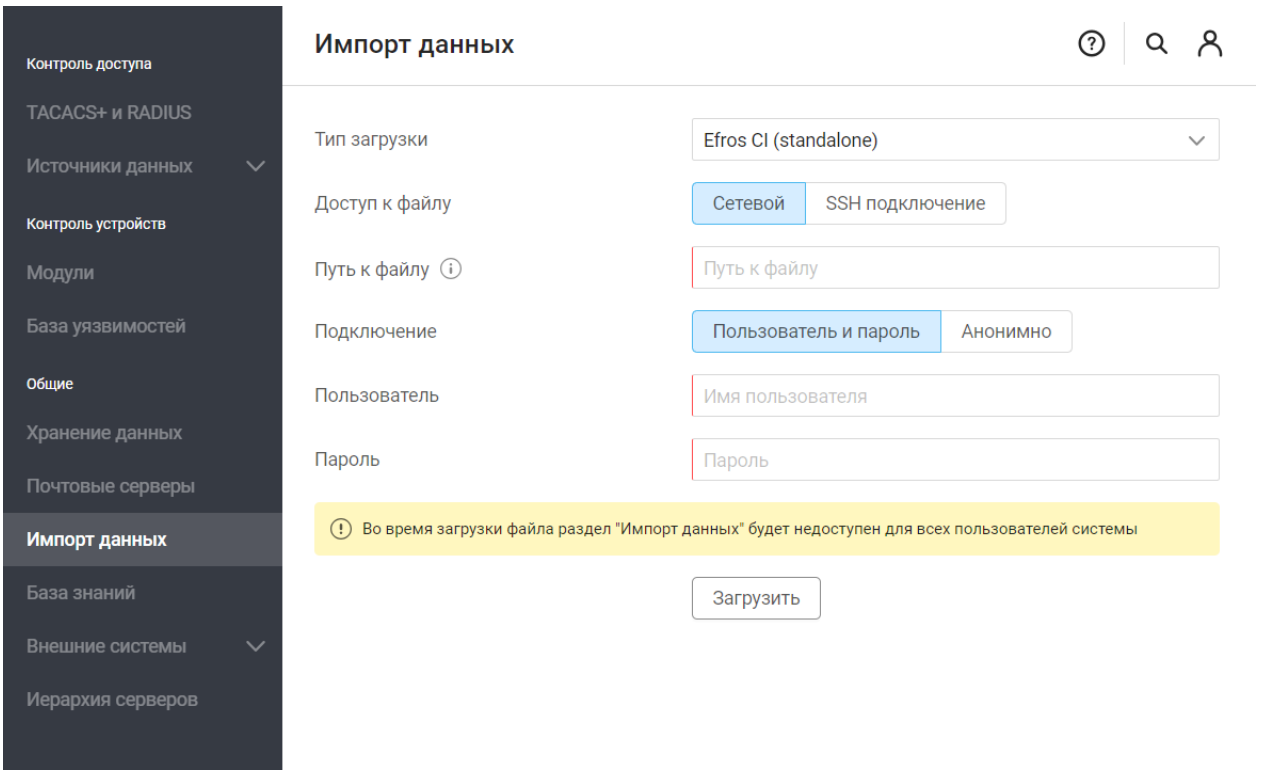


Рисунок 156 – Подраздел «Импорт данных»

Для импорта доступны следующие типы загрузок:

- «Efros CI (standalone)»;
- «Efros ACS (standalone)»;
- «Сетевые устройства»;
- «Сетевые пользователи»;
- «Разрешенные MAC-адреса»;
- «Конечные точки».

При наличии лицензии на функциональный модуль «Efros NAC» доступны все типы загрузки.

Тип загрузки «Efros CI (standalone)» доступен при наличии хотя бы одной лицензии на функциональные модули.

Состав и описание полей страницы при выборе типа загрузки «Efros CI (standalone)» приведены в таблице 52.

Таблица 52 – Состав и описание полей подраздела «Импорт данных» при выборе типа загрузки «Efros CI (standalone)»

Поле	Описание
Поле «Тип загрузки»	Раскрывающийся список с выбором типа загружаемых данных. Выбрано значение «Efros CI (standalone)». Загружаемый файл формируется с помощью инструмента экспорта из ПК «Efros Config Inspector» (ПК «Efros CI»)
Поле «Доступ к файлу»	Переключатель: — «Сетевой»; — «SSH подключение». При изменении значения в поле изменяется набор дополнительных полей
Дополнительные поля для доступа «Сетевой»	
Поле «Путь к файлу»	Текстовое поле для ввода пути к файлу, из которого забираются данные «Efros CI (standalone)» в формате .db Формат ввода: [адрес_хоста]/[путь_к_файлу]/[имя_файла].db Сетевая папка должна быть доступна с ПК «Efros DO»
Поле «Подключение»	Переключатель: — «Пользователь и пароль» – необходимо указать в полях ниже пользователя и пароль для доступа к папке; — «Анонимно»
Поле «Пользователь»	Логин пользователя для доступа к папке
Поле «Пароль»	Пароль пользователя для доступа к папке
Дополнительные поля для доступа «SSH подключение»	
Поле «Адрес сервера»	Текстовое поле для ввода адреса сервера.

Поле	Описание
	Для нестандартного порта ssh можно ввести данные в формате: [Адрес сервера]:[порт]
Поле «Пользователь»	Логин пользователя для доступа к папке
Поле «Пароль»	Пароль пользователя для доступа к папке
Поле «Путь к файлу»	Текстовое поле для ввода пути к файлу, из которого забираются данные «Efros CI (standalone)» в формате .db Формат ввода: [адрес_хоста]/[путь_к_файлу]/[имя_файла].db
Элементы управления	
Кнопка «Загрузить»	При нажатии кнопки выполняется загрузка файла. Во время загрузки файла раздел «Импорт данных» будет недоступен для всех пользователей системы

Состав и описание полей страницы при выборе типа загрузки «Efros ACS (standalone)» приведены в таблице 53.

Таблица 53 – Состав и описание полей подраздела «Импорт данных» при выборе типа загрузки «Efros ACS (standalone)»

Поле	Описание
Поле «Тип загрузки»	Раскрывающийся список с выбором типа загружаемых данных. Выбрано значение «Efros ACS (standalone)». Для использования типа загрузки «Efros ACS (standalone)» необходимо предварительно добавить в систему: — серверные сертификаты, присутствующие в «Efros ACS (standalone)» (см. п. 10.3); — загружаемые ACL (подробнее см. документ «Руководство пользователя. Часть 2. Контроль устройств».
Поле «Файл с данными»	Поле для загрузки архива, полученного из консоли экспорта данных ПК «Efros ACS». Формат файла: .zip. Загружаемый файл формируется с помощью инструмента экспорта из ПК «Efros ACS».
Поле «Инструмент	При нажатии кнопки выполняется скачивание инструмента

Поле	Описание
экспорта из Efros ACS»	экспорта из ПК «Efros ACS». Инструмент экспорта из ПК «Efros ACS» скачивается в виде архива формата .zip, в котором содержится утилита экспорта из ПК «Efros ACS» в формате .exe

Состав и описание полей страницы при выборе другого типа загрузки – «Сетевые устройства», «Сетевые пользователи», «Разрешенные MAC-адреса» или «Конечные точки» (далее – тип загрузки с разделителем данных) приведены в таблице 54.

Таблица 54 – Состав и описание полей подраздела «Импорт данных» при выборе типа загрузки с разделителем данных

Поле	Описание
Поле «Тип загрузки»	Раскрывающийся список с выбором типа загружаемых данных. Выбрано одно из значений: «Сетевые устройства», «Сетевые пользователи», «Разрешенные MAC-адреса» или «Конечные точки»
Поле «Разделитель данных»	Поле для выбора разделителя полей, который будет применен для загружаемого файла формата .csv или шаблона. Переключатель: — «Точка с запятой»; — «Запятая»; — «Табуляция»; — *«Другой». *При выборе значения «Другой» в дополнительно отобразившемся поле «Пользовательский разделитель» необходимо указать разделитель данных. Доступные для ввода значения ограничены следующим набором символов: aA-zZ, 0-9, символы !#$%&'()*+, -./:;<=>?@[\]^_{|}~
Поле «Файл с данными»	Поле выбора файла заполненного шаблона с необходимыми данными. Формат файла: .csv (кодировка UTF-8). Максимальный размер файла: 50 Мб. Загружаемый файл должен соответствовать выбранному типу загрузки. Разделитель полей в файле должен соответствовать значению, выбранному в поле «Разделитель данных».
Поле «Шаблон»	При нажатии кнопки выполняется скачивание файла шаблона

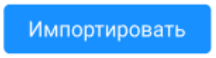
Поле	Описание
	в формате .csv для заполнения необходимыми данными Шаблон содержит строку заголовков, которая определяет формат полей. В качестве разделителя будет использоваться значение, выбранное в поле «Разделитель данных». При загрузке данных из файла строка заголовков не должна редактироваться и должна использоваться как есть

11.7.1 Экспорт и импорт данных «Efros CI (standalone)»

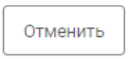
Для экспорта данных из «Efros CI (standalone)» и последующего импорта в ПК «Efros DO» пользователю необходимо выполнить следующие шаги:

1) Экспортировать данные из ПК «Efros CI» с помощью утилиты (подробное описание работы с утилитой приведено в документе «Инструкция по экспорту данных из ПК «Efros CI» для ПК «Efros DO»).
2) В подразделе «Импорт данных» в поле «Путь к файлу» ввести путь к файлу базы данных для загрузки.
3) Нажать кнопку «Загрузить». Начнется процесс загрузки файла. Все поля при этом будут заблокированы. Раздел «Импорт данных» будет недоступен для всех пользователей системы.

   После успешной загрузки отобразится сообщение «Загрузка завершена» (рис. 157). На странице пользователь может выполнить следующие действия:

   — импортировать данные в раздел «Контроль устройств», нажав кнопку «Импортировать» (

);

   — отметить процесс импорта, нажав кнопку «Отменить» (

).
4) Нажать кнопку «Импортировать». Начнется процесс импорта. Все данные из раздела «Контроль устройств» будут заменены. Во время импорта сервис «Контроль устройств» будет недоступен. Все поля при этом будут заблокированы.
5) После успешного импорта отобразится сообщение «Импорт завершен». Просмотр журнала операций доступен по нажатию кнопки «Лог операций».

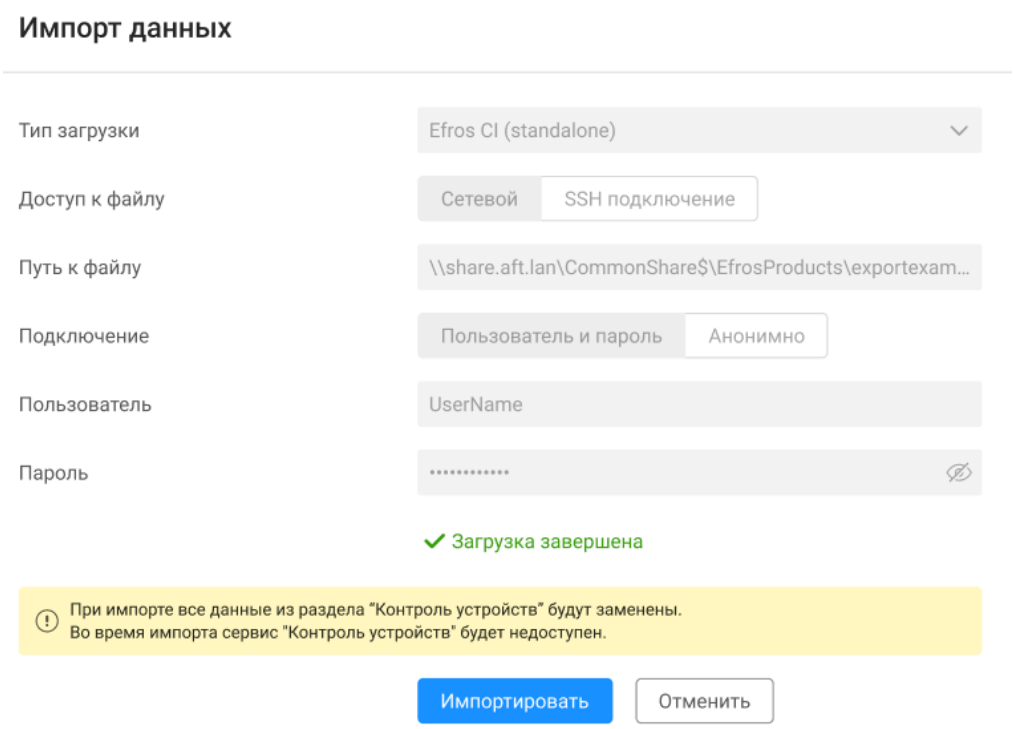


Рисунок 157 – Страница успешной загрузки файла базы данных

11.7.2 Экспорт и импорт данных «Efros ACS (standalone)»

Для экспорта данных из «Efros ACS (standalone)» и последующего импорта в ПК «Efros DO» пользователю необходимо выполнить следующие шаги:

1) Выбрать тип загрузки «Efros ACS (standalone)».
2) Скачать инструмент экспорта из ПК «Efros ACS» на локальную ЭВМ.
3) Распаковать архив формата .zip.
4) Экспортировать данные из ПК «Efros ACS» с помощью скачанного исполняемого файла формата .exe (подробное описание работы с утилитой приведено в документе «Инструкция по экспорту данных из ПК «Efros ACS» для ПК «Efros DO»).
5) В подразделе «Импорт данных» в поле «Файл с данными» выбрать архив для загрузки, полученный с помощью утилиты экспорта данных ПК «Efros ACS».
6) Ввести пароль для загружаемого архива, ранее заданный в командной строке утилиты экспорта данных ПК «Efros ACS».
7) Откроется страница «Импорт данных (EFROS ACS)» с информацией о сертификатах (рис. 158). На странице приведены типы объектов и их количество. При нажатии на кнопку объекта откроется окно с параметрами загружаемых объектов. В случае наличия одинаковых объектов выводится предупреждающее

сообщение о наличии дубликатов, которые не будут загружаться. На странице импорта данных пользователь может выполнить следующие действия:

— подтвердить загрузку приведенных сертификатов и перейти к следующему шагу импорта, нажав кнопку «Загрузить» (Загрузить);
— отметить процесс импорта, нажав кнопку «Отменить» (Отменить);
— перейти к следующему шагу, не загружая приведенные сертификаты, нажав кнопку «Пропустить» (Пропустить).

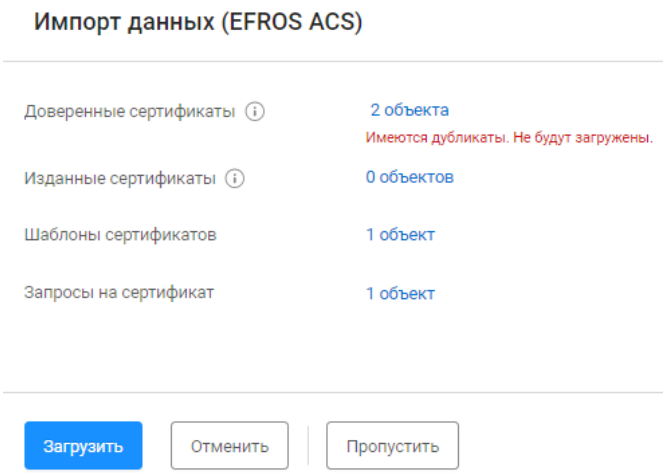


Рисунок 158 – Страница «Импорта данных (EFROS ACS)» с информацией о сертификатах

8) При продолжении импорта данных откроется страница «Импорт данных (EFROS ACS)» с информацией об объектах и пользователях сети (рис. 159).

Некоторые данные не допускаются к импорту в текущем формате, для них требуется ввод данных вручную для создания новых связей между объектами. Для этого необходимо нажать кнопку объекта с предупреждающим сообщением «Требуется ввод данных» и заполнить необходимые поля.

9) После ввода всех необходимых данных кнопка «Загрузить» (Загрузить) становится активной, при нажатии на кнопку начнется процесс импорта данных.

10) После завершения импорта будет выведено сообщение с количеством импортированных объектов.

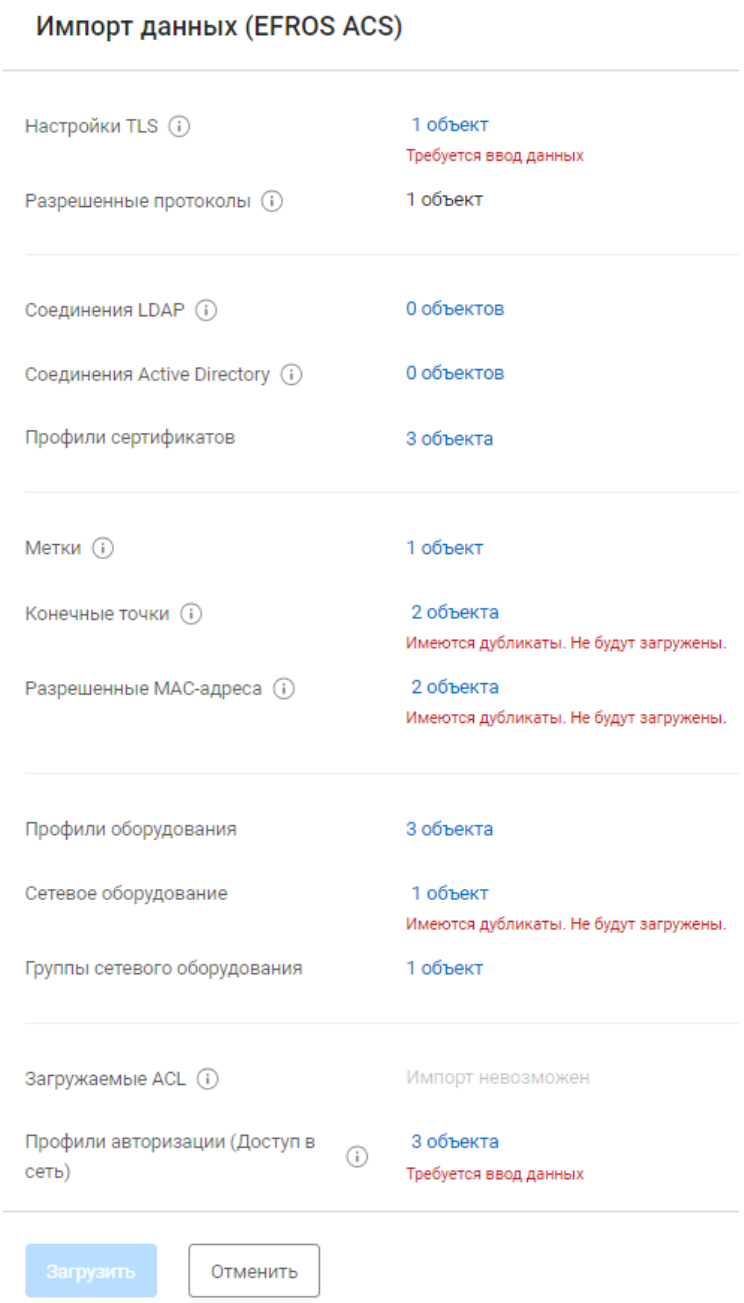


Рисунок 159 – Страница «Импорта данных (EFROS ACS)» с информацией об объектах и пользователях сети

11.7.3 Импорт данных типа загрузки с разделителем данных

Для импорта данных при выборе типа загрузки с разделителем данных пользователю необходимо выполнить следующие шаги:

1) Выбрать тип загрузки данных, например «Сетевые устройства» (рис. 160). Последующие шаги аналогичны для других типов загрузок.

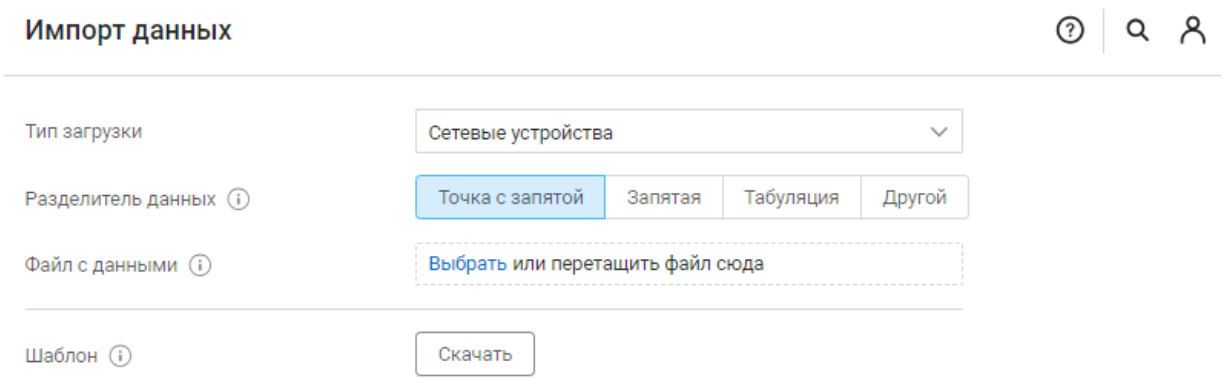


Рисунок 160 – Выбор типа загрузки

2) Выбрать разделитель данных.
3) Скачать шаблон на локальную ЭВМ.
4) Открыть шаблон, скачанный из ПК «Efros DO».
5) Открыть файл формата .csv с данными, которые необходимо добавить, в текстовом редакторе.
6) Добавить в начале файла пустую строку и указать в ней параметр: sep=,
7) Сохранить файл после редактирования.
8) Открыть сохраненный файл .csv в табличном виде с помощью программы для работы с таблицами, например, OpenOffice или любой другой подобной программы. Убедиться, что файл открылся в табличном виде.
9) Заполнить шаблон данными из подготовленного файла формата .csv, для этого поочередно скопировать данные из колонок файла в шаблон. Названия колонок в шаблоне и в файле соответствуют друг другу.

При копировании данных из колонок с IP-адресами необходимо заменить символ «#» на «;».

10) Загрузить откорректированный шаблон в ПК «Efros DO».

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.

11) Откроется страница со списком импортируемых данных в виде таблицы (рис. 161). Состав и описание полей страницы приведены в таблице 55.

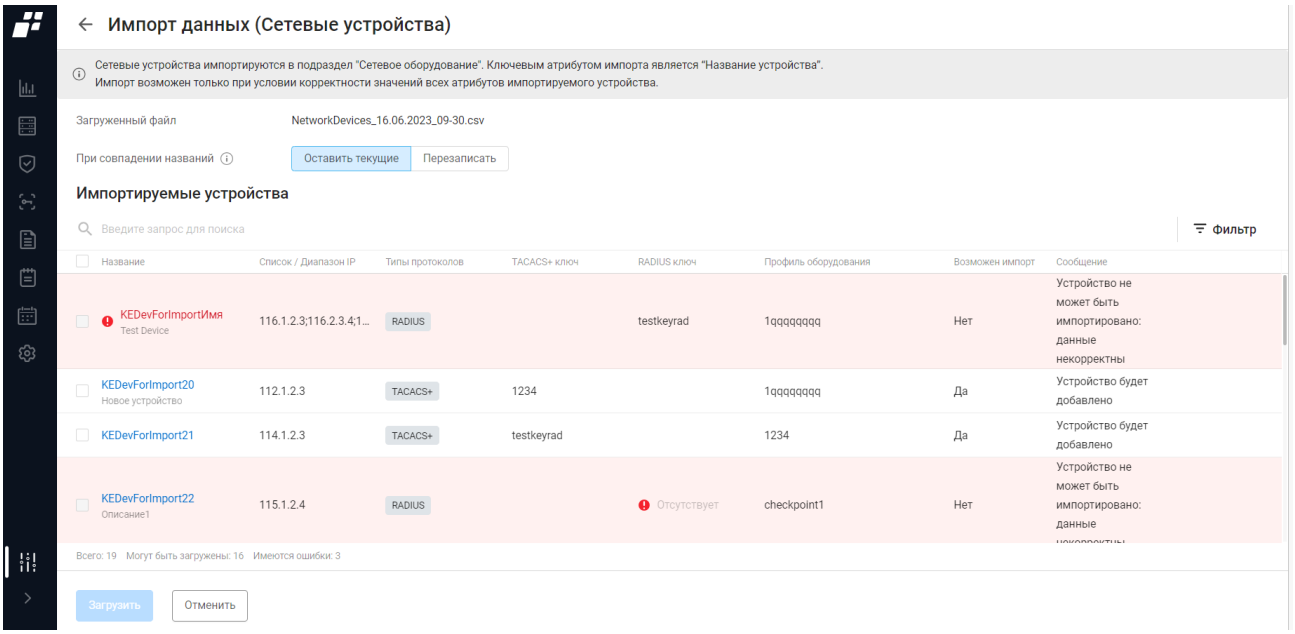


Рисунок 161 – Страница «Импорта данных (Сетевые устройства)»

Строки устройств, требующие корректировки, подсвечены красным.

Таблица 55 – 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 добавлены только новые сетевые устройства; — «Перезаписать» – данные существующих сетевых устройств будут заменены данными из файла импорта

Поле	Описание
Поле «Импортируемые устройства»	Сетевые устройства с данными по каждому устройству
Элементы управления	
Загрузить	При нажатии кнопки выполняется загрузка данных
Отменить	При нажатии кнопки выполняется переход на страницу без сохранения внесенных данных

12) Необходимо выполнить корректировку данных у объектов.

13) 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).

14) Нажать кнопку «Загрузить».

11.8 База знаний

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

Подраздел «База знаний» (рис. 162) позволяет настраивать источники сканирования, которые осуществляют систематический сбор сведений о сетевых ресурсах путем пассивного и активного сканирования сети с помощью протоколов и утилит. Состав и описание полей страницы приведены в таблице 56.

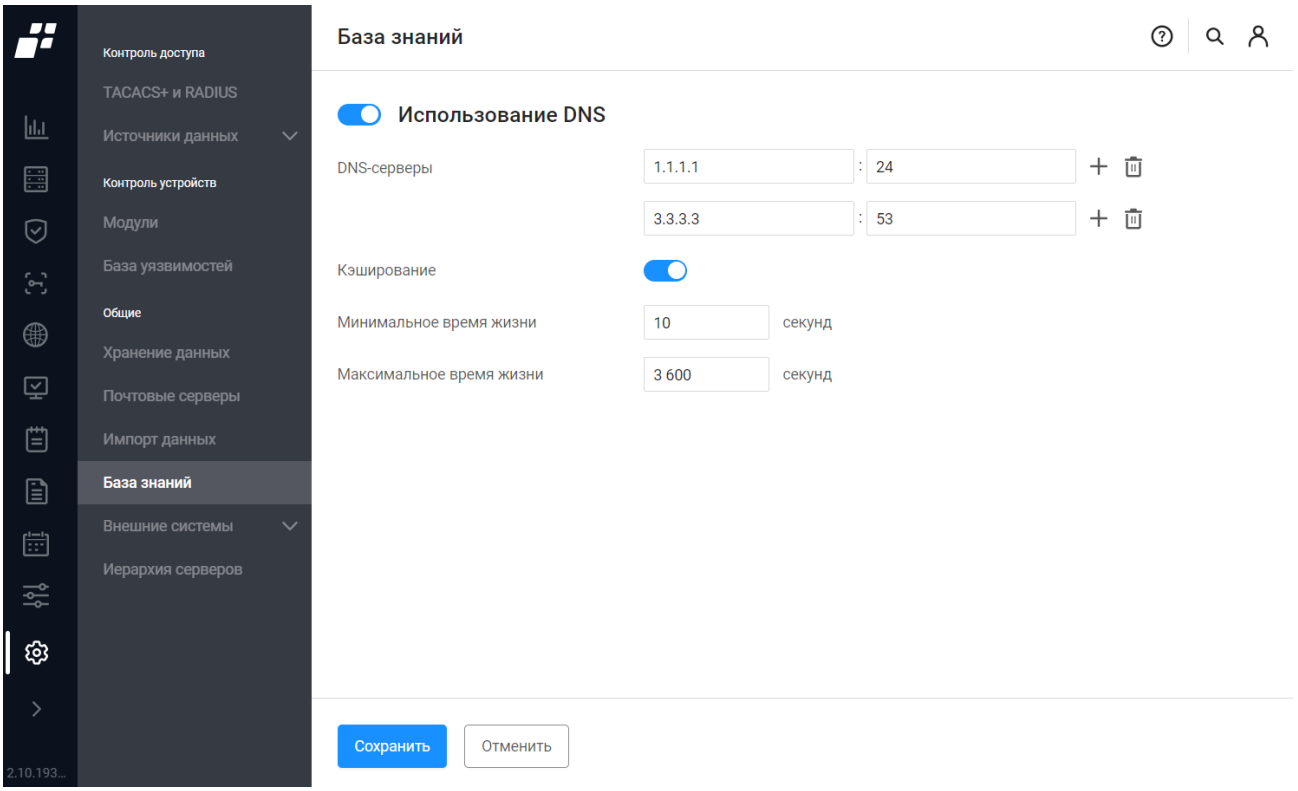


Рисунок 162 – Подраздел «База знаний»

Таблица 56 – Состав и описание полей подраздела «База знаний»

Поле	Описание
Группа полей «Использование DNS»	
Поле «Использование DNS»	Переключатель для включения использования DNS. При включении появляются дополнительные поля для добавления DNS-серверов (см. ниже)
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. Для добавления DNS-сервера – нажать кнопку «+», при необходимости удалить – нажать кнопку «🗑»
Поле «Кэширование»	Переключатель для включения использования кэширования. При включении появляются дополнительные поля для настройки кэширования (см. ниже)
Поле «Минимальное время жизни»	Поле для ввода минимального количества секунд хранения кэша
Поле «Максимальное время жизни»	Поле для ввода минимального количества секунд хранения кэша
Элементы управления	

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

11.9 Внешние системы

Отображаемые данные и доступная функциональность в подразделе «Внешние системы» зависят от наличия хотя бы одной лицензии на функциональные модули.

Подраздел «Внешние системы» позволяет настраивать следующие сервисы:

- внешние серверы RADIUS, которые осуществляют подключение к внешним системам аутентификации;
- внешние системы аутентификации, которые предназначены для включения возможности назначать для пользователя прохождение двухфакторной аутентификации при авторизации в ПК «Efros DO». Для пользователей можно настроить следующие методы прохождения второго этапа аутентификации:
  - «Программная генерация TOTP» – для аутентификации используется одноразовый код Time-based One-Time Password, сгенерированный программой;
  - «Одноразовый код по E-mail или SMS» – для аутентификации используется одноразовый код, сгенерированный и отправленный внешней системой аутентификации пользователю по E-mail или SMS.
- SMS-провайдеры, которые позволяют управлять списком внешних сервисов отправки сообщений или совершения звонков для проверки номера телефона, задаваемого пользователем при самостоятельной регистрации на гостевом портале.

11.9.1 Серверы RADIUS

Вкладка «Внешние серверы RADIUS» позволяет управлять списком внешних серверов RADIUS, на которые будут отправлены запросы на доступ (рис. 163).

Для каждой записи списка отображаются следующие данные:

- название сервера – доступна сортировка по имени сервера в алфавитном порядке. Является ссылкой для перехода в окно редактирования параметров сервера;
- адрес и порт для подключения к серверу;
- дата последнего изменения.

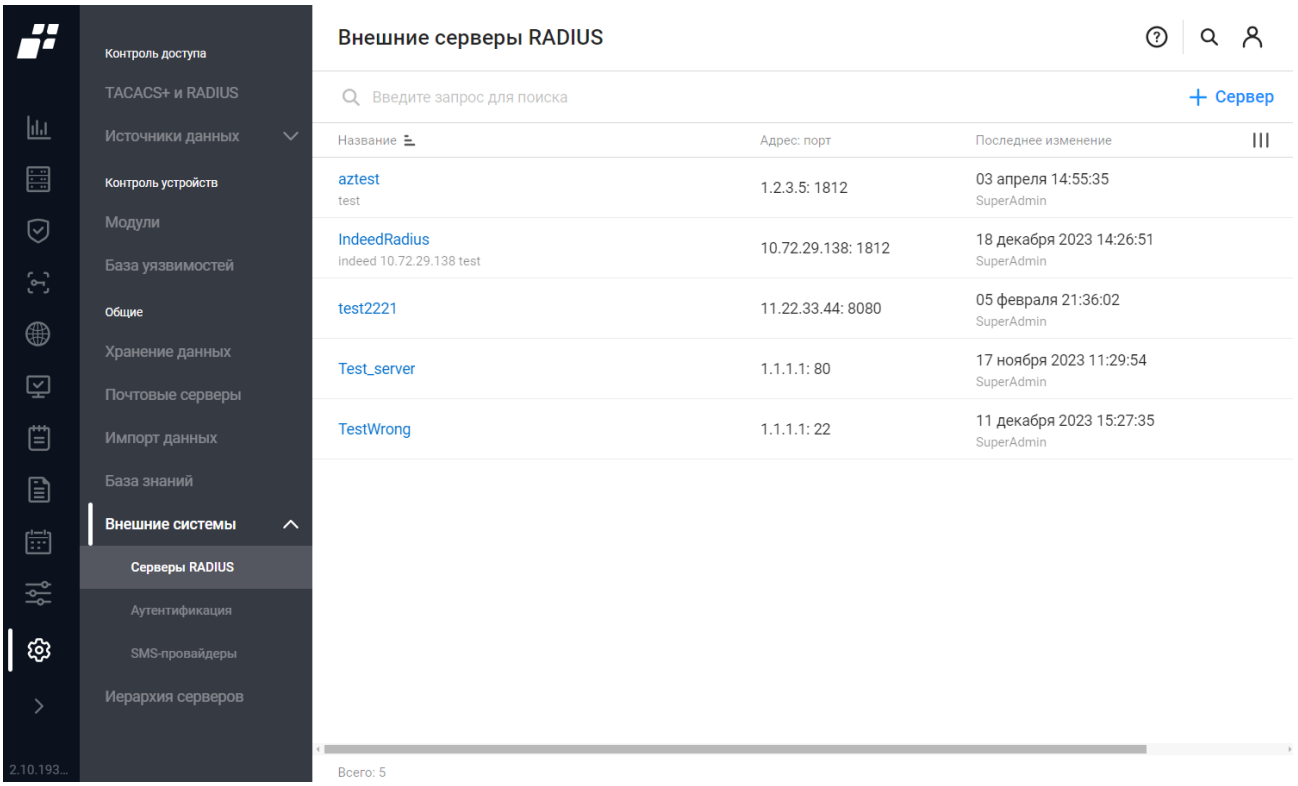


Рисунок 163 – Вкладка «Внешние серверы RADIUS»

Над списком доступны следующие функции:

— поле поиска (Введите запрос для поиска);

— кнопка «Добавить сервер» (+ Сервер);

— кнопка «Колонки» ( ).

При наведении курсора на строку сервера в правой части строки появляется кнопка «Удалить» ( ).

11.9.1.1 Добавление сервера RADIUS

Для добавления внешнего сервера RADIUS администратору необходимо:

1) Выбрать раздел «Настройки», далее подраздел «Внешние системы» и открыть вкладку «Серверы RADIUS» (см. рис. 163).

2) Нажать кнопку «Добавить сервер» (+ Сервер). Откроется страница создания внешнего сервера RADIUS (рис. 164). Необходимо заполнить поля требуемыми параметрами и нажать кнопку «Создать». Состав и описание полей страницы приведены в таблице 57.

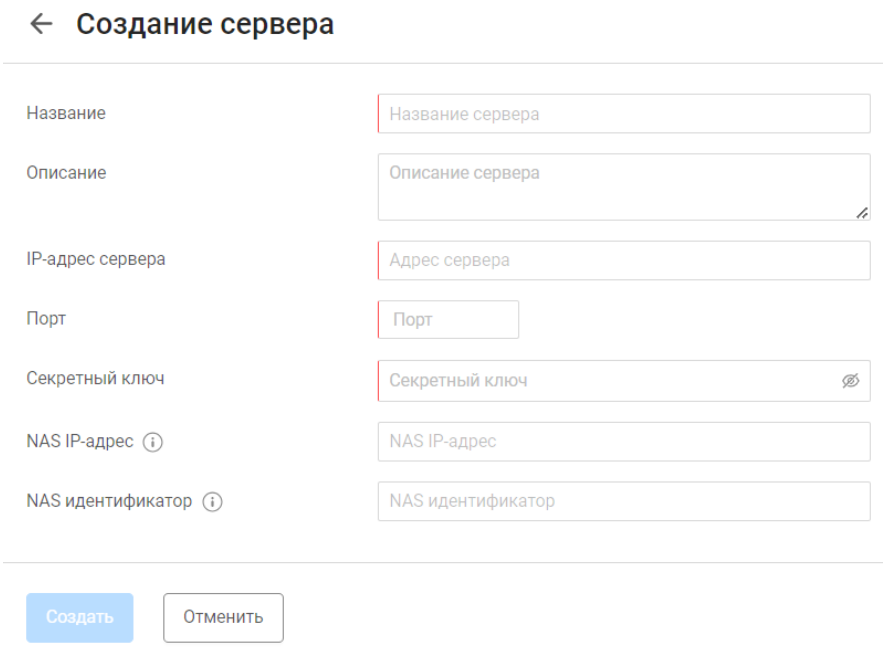


Рисунок 164 – Страница создания внешнего сервера RADIUS

Таблица 57 – Состав и описание полей страницы создания внешнего сервера RADIUS

Поле	Описание
Поле «Название»	Текстовое поле для ввода названия внешнего сервера RADIUS. Параметры ввода текста: от 1 до 50 символов. Допустимые символы: буквы латинского алфавита, цифры, «_», «–»
Поле «Описание»	Текстовое поле для ввода описания внешнего сервера RADIUS. Параметры ввода текста: от 1 до 250 любых символов
Поле «IP-адрес сервера»	Текстовое поле для ввода IP-адреса сервера
Поле «Порт»	Числовое поле для ввода номера порта для подключения к серверу. Допустимые значения: от 1 до 65535
Поле «Секретный ключ»	Текстовое поле для ввода секретного ключа, используемого для шифрования данных в пакетах RADIUS, передаваемых между клиентом RADIUS и сервером RADIUS во время сеансов аутентификации. Параметры ввода текста: от 1 до 128 любых символов
Поле «NAS IP-адрес»	Текстовое поле для ввода IP-адреса сервера сетевого доступа (Network Access Server), от имени которого посылается запрос RADIUS серверу. Передается RADIUS клиентом серверу как один из атрибутов в запросе
Поле «NAS-	Текстовое поле для ввода идентификатора сервера (NAS-

Поле	Описание
идентификатор»	Identifier), отправляющего запрос. Параметры ввода текста: от 1 до 250 символов. Допустимые символы: буквы латинского алфавита, цифры, спец. символы
Элементы управления	
Создать	При нажатии кнопки выполняется сохранение внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу без сохранения внесенных данных

11.9.2 Внешние системы аутентификации

Вкладка «Внешние системы аутентификации» позволяет управлять списком внешних систем аутентификации, которым может быть перенаправлен запрос на проверку прохождения второго этапа аутентификации (рис. 165).

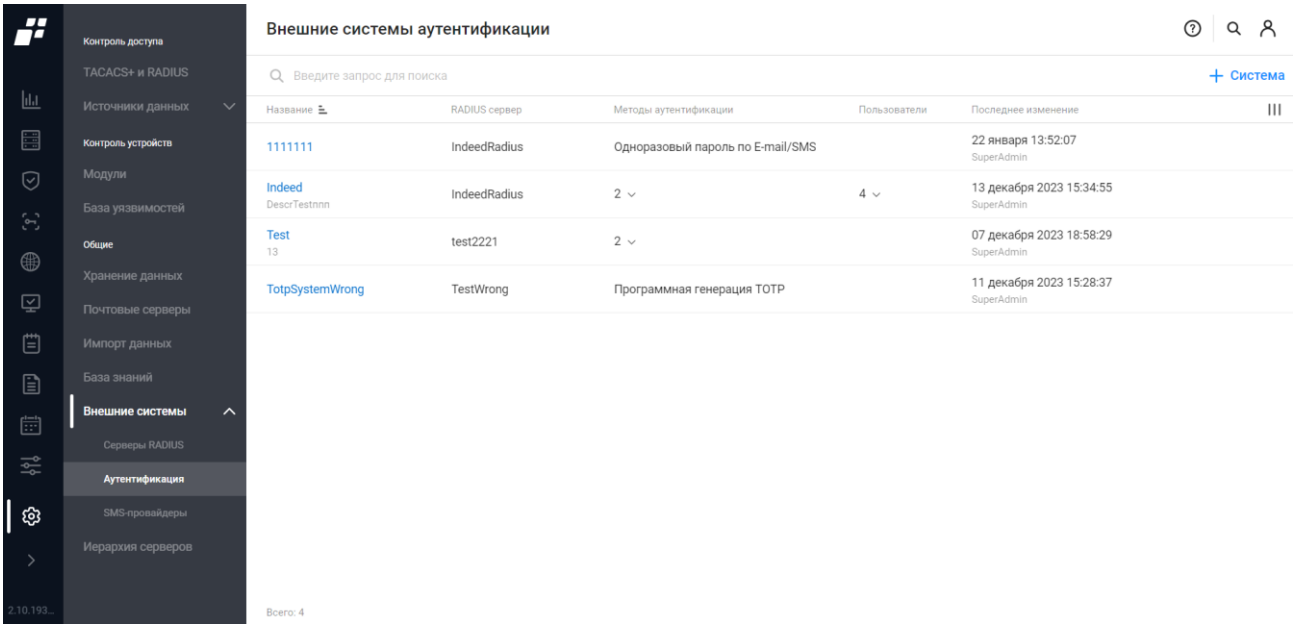


Рисунок 165 – Вкладка «Внешние системы аутентификации»

Для каждой записи списка отображаются следующие данные:

- название внешней системы аутентификации – доступна сортировка по имени системы в алфавитном порядке. Является ссылкой для перехода в окно редактирования параметров системы;
- название RADIUS сервера, на который отправляется запрос на доступ;
- метод аутентификации;
- пользователь или количество пользователей, для которых включена двухфакторная аутентификация. Количество является раскрывающимся списком пользователей;

— дата последнего изменения и пользователь изменивший настройки.

Над списком доступны следующие функции:

— поле поиска (Введите запрос для поиска);

— кнопка «Добавить систему» (+ Система);

— кнопка «Колонки» ( ).

При наведении курсора на строку системы в правой части строки появляется кнопка «Удалить» ( ).

11.9.2.1 Добавление внешней системы аутентификации

Для добавления внешней системы аутентификации администратору необходимо:

1) Выбрать раздел «Настройки», далее подраздел «Внешние системы» и вкладку «Аутентификация» (см. рис. 165).

2) Нажать кнопку «Добавить систему» (+ Система). Откроется страница создания системы внешней аутентификации (рис. 166). Необходимо заполнить поля требуемыми параметрами и нажать кнопку «Создать». Состав и описание полей страницы приведены в таблице 58.

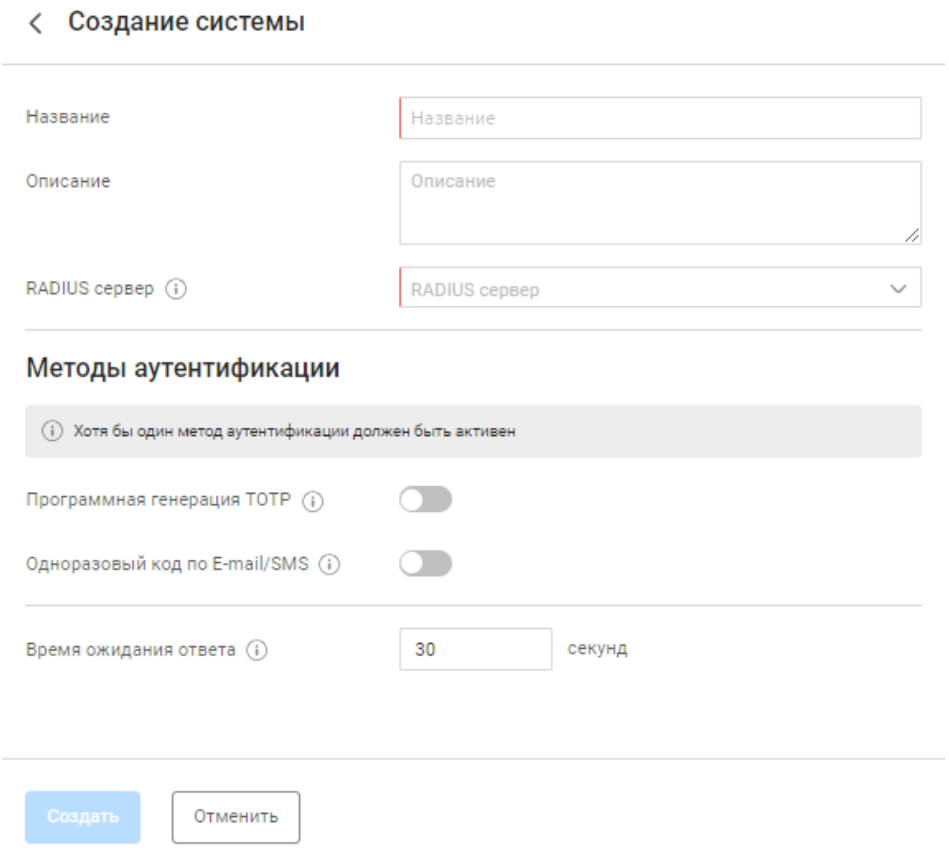


Рисунок 166 – Страница создания внешней системы аутентификации

Таблица 58 – Состав и описание полей страницы создания внешней системы аутентификации

Поле	Описание
Поле «Название»	Текстовое поле для ввода названия внешней системы аутентификации. Параметры ввода текста: от 1 до 50 символов. Допустимые символы: буквы латинского алфавита, цифры, «_», «–»
Поле «Описание»	Текстовое поле для ввода описания внешней системы аутентификации. Параметры ввода текста: от 1 до 250 любых символов
Поле «RADIUS сервер»	Поле для выбора в раскрывающемся списке требуемого сервера RADIUS
Группа полей «Методы аутентификации»	
Поле «Программная генерация TOTP»	Переключатель с двумя положениями: — «Активен» ( ) – включение аутентификации с использованием одноразового кода (Time-based One-Time Password), сгенерированного программой; — «Неактивен» ( ) – отключение аутентификации с использованием одноразового кода (Time-based One-Time Password), сгенерированного программой
Поле «Одноразовый код по E-mail/SMS»	Переключатель с двумя положениями: — «Активен» ( ) – включение аутентификации с использованием одноразового кода отправленного на E-mail или SMS; — «Неактивен» ( ) – отключение аутентификации с использованием одноразового кода отправленного на E-mail или SMS. При включении пуреключателя становится доступным поле ввода интервала повторной отправки кода (см ниже).
Поле «Повторная отправка кода через»	Числовое поле для ввода интервала времени (в секундах), ожидания получения кода, по истечении которого можно совершить повторную отправку кода. Допустимые значения: от 30 до 120. Значение по умолчанию: 30
Поле «Время ожидания ответа»	Числовое поле для ввода интервала времени (в секундах) ожидания ответа, по истечении которого осуществляется блокировка веб-интерфейса с необходимостью повторной авторизации. Допустимые значения: от 30 до 600.

Поле	Описание
	Значение по умолчанию: 60
Элементы управления	
Создать	При нажатии кнопки выполняется сохранение внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу без сохранения внесенных данных

После создания системы внешней аутентификации можно включить возможность применения двухфакторной аутентификации пользователей на вкладке «Настройки безопасности» раздела «Пользователи» (см. п. 10.1.3).

11.9.3 SMS-провайдеры

Вкладка «SMS-провайдеры» позволяет управлять списком внешних сервисов отправки сообщений или совершения звонков для проверки номера телефона, задаваемого пользователем при самостоятельной регистрации на гостевом портале (рис. 167).

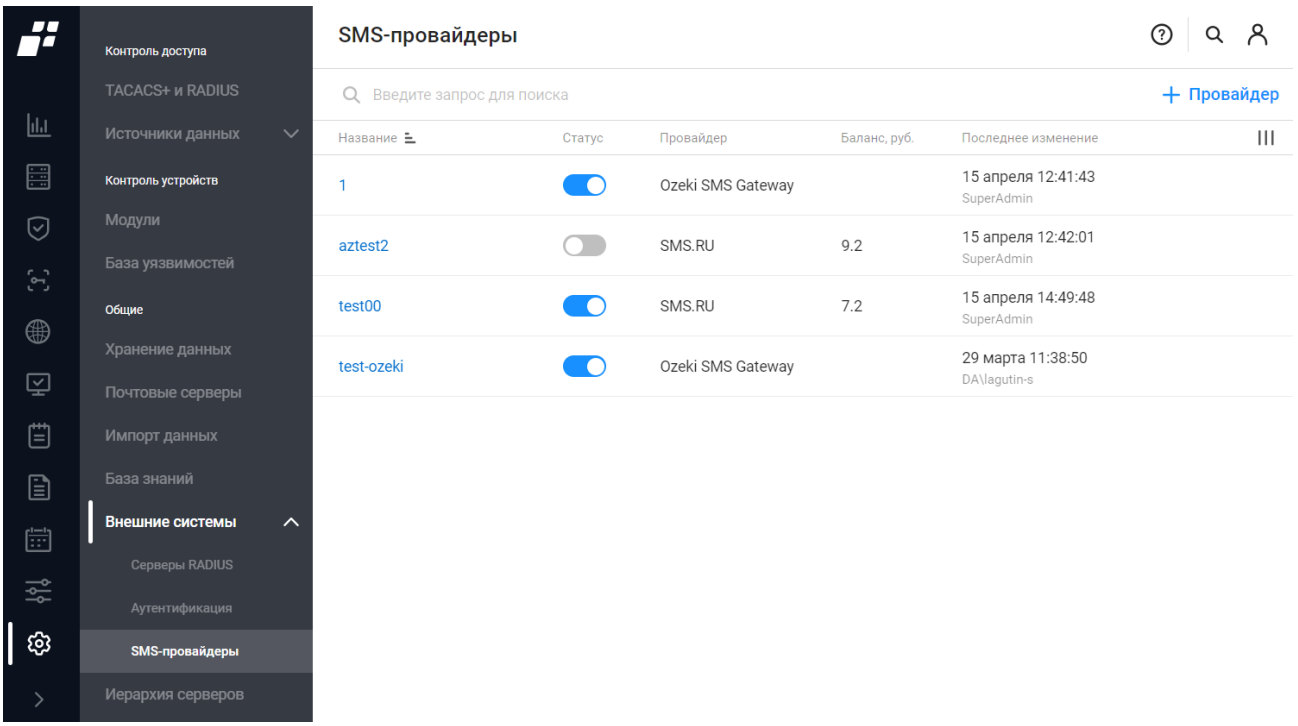


Рисунок 167 – Вкладка «SMS-провайдеры»

Для каждой записи списка отображаются следующие данные:

- название и описание SMS-провайдера – доступна сортировка по имени провайдеров в алфавитном порядке. Является ссылкой для перехода в окно редактирования параметров провайдера;
- статус. Переключатель, отображает состояние (активен или неактивен);
- название провайдера, на который отправляется запрос для доступа;

— баланс на счету номера телефона, в рублях (отображаются для провайдера «SMS.RU»);
— дата последнего изменения и пользователь изменившего настройки.

Над списком доступны следующие функции:

— поле поиска (Введите запрос для поиска);
— кнопка «Добавить систему» (Провайдер);
— кнопка «Колонки» ( ).

При наведении курсора на строку провайдера в правой части строки появляются кнопки:

— «Обновить» ( ) для обновления баланса на счету провайдера;
— «Удалить» ( ).

11.9.3.1 Добавление провайдера

Для добавления провайдера администратору необходимо:

1) Выбрать раздел «Настройки», далее подраздел «Внешние системы» и вкладку «SMS-провайдеры» (см. рис. 167).
2) Нажать кнопку «Провайдер» (Провайдер). Откроется страница создания провайдера (рис. 168). Необходимо заполнить поля требуемыми параметрами и нажать кнопку «Создать». Состав и описание полей страницы приведены в таблице 59.

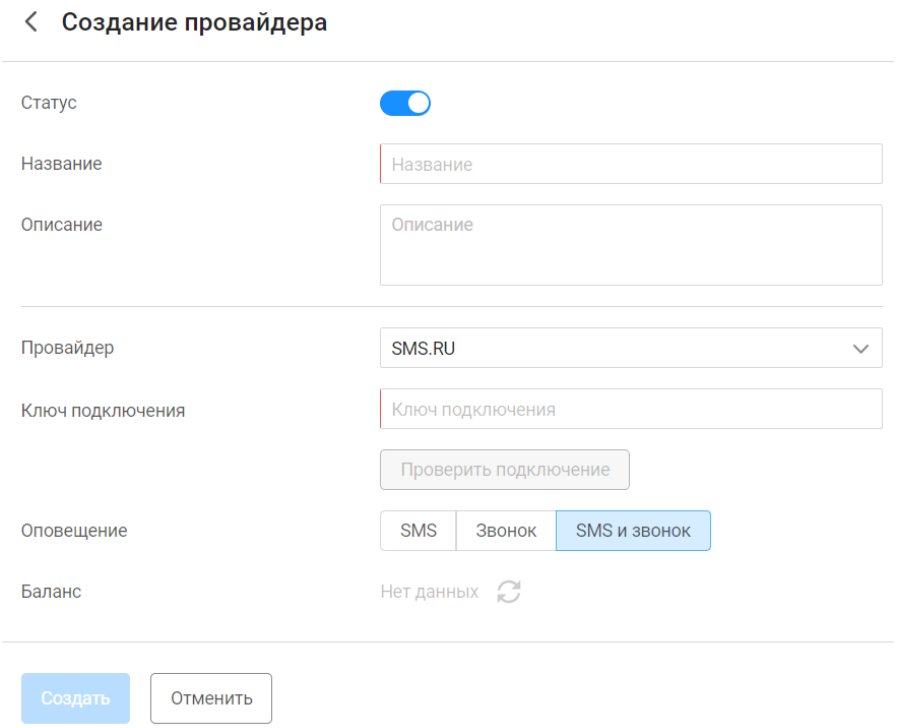


Рисунок 168 – Страница создания провайдера

Таблица 59 – Состав и описание полей страницы создания провайдера

Поле	Описание
Поле «Статус»	Переключатель: — «Активен» ( ); — «Неактивен» ( )
Поле «Название»	Текстовое поле для ввода названия SMS-провайдера. Параметры ввода текста: от 1 до 50 символов. Допустимые символы: буквы латинского алфавита, цифры, «_», «–»
Поле «Описание»	Текстовое поле для ввода описания SMS-провайдера. Параметры ввода текста: от 1 до 250 любых символов
Поле «Провайдер»	Поле для выбора в раскрывающемся списке требуемого провайдера: — «SMS.RU»; — «Ozeki SMS Gateway». Дополнительные поля (см. ниже) зависят от выбранного провайдера
Группа полей для провайдера «SMS.RU»	
Поле «Ключ подключения»	Текстовое поле для ввода уникального программного ключа (api_id), полученного при регистрации у провайдера «SMS.RU». Регистрация пользователя у провайдера «SMS.RU» производится на сайте: https://sms.ru/
Кнопка «Проверить подключение»	При нажатии кнопки выполняется проверка подключения номера телефона
Поле «Оповещение»	Переключатель: — «SMS»; — «Звонок»
Поле «Баланс»	Поле для просмотра текущего баланса на счету номера телефона с регистрацией у провайдера «SMS.RU». Обновить данные можно с помощью кнопки обновления значения баланса ( )
Группа полей для провайдера «Ozeki SMS Gateway»	
Поле «Адрес провайдера»	Поле для выбора префикса (http:// или https://) и ввода адреса сервера для подключения к API провайдера «Ozeki SMS Gateway». Допустимо применение номера порта и пути до API. Пример: http://10.10.10.10:9501/api

Поле	Описание
	Предварительно необходимо произвести настройку SMS-шлюза «Ozeki SMS Gateway»
Поле «Логин»	Поле для ввода имени пользователя, под которым выполняется подключение к API провайдера «Ozeki SMS Gateway»
Поле «Пароль»	Поле для ввода пароля пользователя, под которым выполняется подключение к API провайдера «Ozeki SMS Gateway». При вводе символы пароля заменяются знаком «•». Для просмотра введенного значения необходимо нажать в поле ввода кнопку «Просмотреть» ( )
Поле «Телефон»	Поле для ввода номера телефона, на который будет отправлено тестовое SMS
Кнопка «Отправить тестовое SMS»	При нажатии кнопки выполняется отправка тестового SMS на указанный номер. Стоимость отправки тестового SMS определяется в соответствии с установленными тарифами провайдера
Элементы управления	
Создать	При нажатии кнопки выполняется сохранение внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу без сохранения внесенных данных

11.10 Иерархия серверов

Подраздел «Иерархия серверов» предназначен для управления иерархией серверов ПК «Efros DO» и предоставляет пользователю с соответствующей привилегией возможность построения иерархии серверов ПК: добавления подчиненных серверов и настройки доступа пользователей к ним (рис. 169).

Иерархия серверов ПК «Efros DO» обеспечивает следующую функциональность:

- управление (добавление, редактирование, удаление, включение/отключение) списком основных ПК «Efros DO», входящих в иерархию;
- получение данных о подчиненных серверах, подключенных к основным серверам;
- получение сведений о доступности и последней активности подчиненных серверов;

— разграничение доступа и прав пользователей основного сервера к подчиненным серверам.

Страница содержит вкладки:

— «Подчиненные»;
— «Вышестоящие»;
— «Токены подключения».

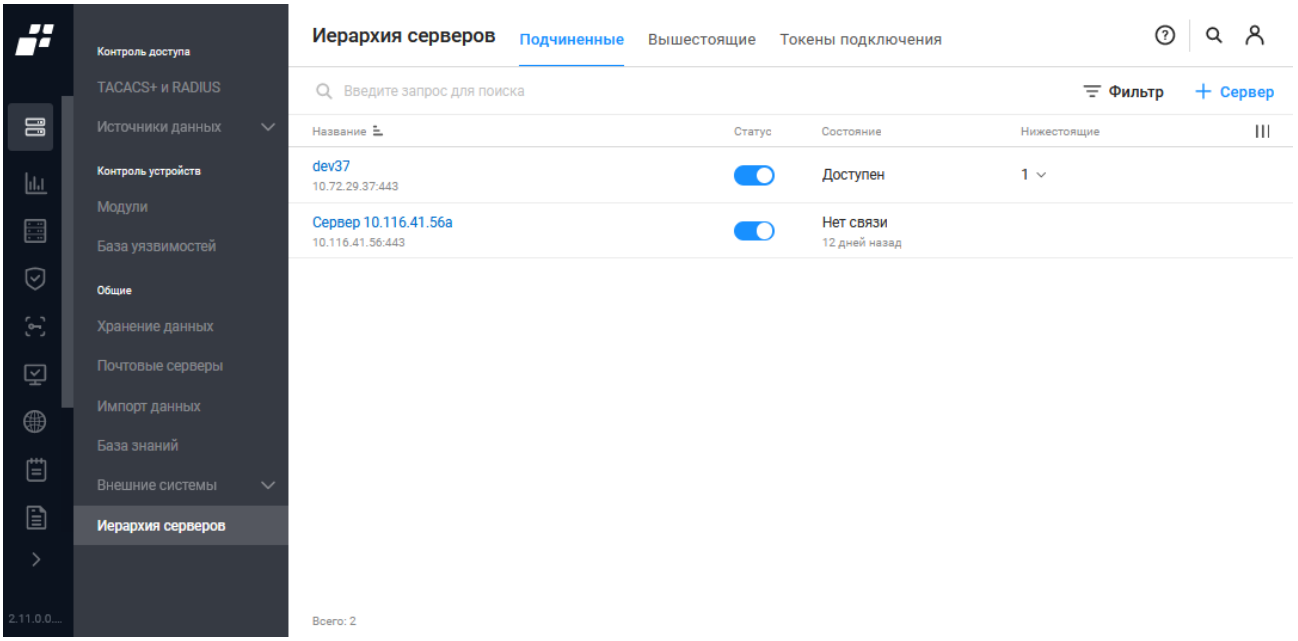


Рисунок 169 – Подраздел «Иерархия серверов»

11.10.1 Вкладка «Подчиненные»

На вкладке «Подчиненные» можно добавить сервер только на один уровень ниже. Для добавления следующих уровней необходимо переключиться на подчиненный сервер, зайти в раздел «Настройки» → «Общие» → «Иерархия серверов» и добавить новый уровень вложенности, который автоматически отобразится на основном сервере.

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

— название – название подчиненного сервера. Является ссылкой, при переходе по которой открывается окно для редактирования данных сервера;
— статус сервера. Переключатель:
  - « » – сервер активен;
  - « » – сервера неактивен. При отключении сервера он и подключенные к нему нижестоящие серверы становятся недоступными для пользователей вышестоящих серверов;

— состояние сервера:
  - «Доступен»;
  - «Недоступен»;
  - «Нет связи»;

— количество нижестоящих серверов у подчиненного сервера.

Над списком серверов располагаются:

— поле поиска (Введите запрос для поиска);

— кнопка «Фильтр» (Фильтр);

— кнопка «Сервер» (+ Сервер);

— кнопка «Колонки» ( ).

При выборе строки с необходимым сервером в правом углу строки появляется кнопка «Удалить» ( ). В нижней части страницы отображается информация об общем количестве починенных серверов.

11.10.1.1 Добавление подчиненного сервера

Для добавления подчиненного сервера пользователю необходимо:

1) Выбрать раздел «Настройки», далее подраздел «Иерархия серверов», вкладка «Подчиненные».

2) Нажать кнопку «Сервер» (+ Сервер). Откроется страница создания внешнего сервера (рис. 170). Заполнить поля страницы необходимыми параметрами и нажать кнопку «Добавить». Состав и описание полей страницы приведены в таблице 60.

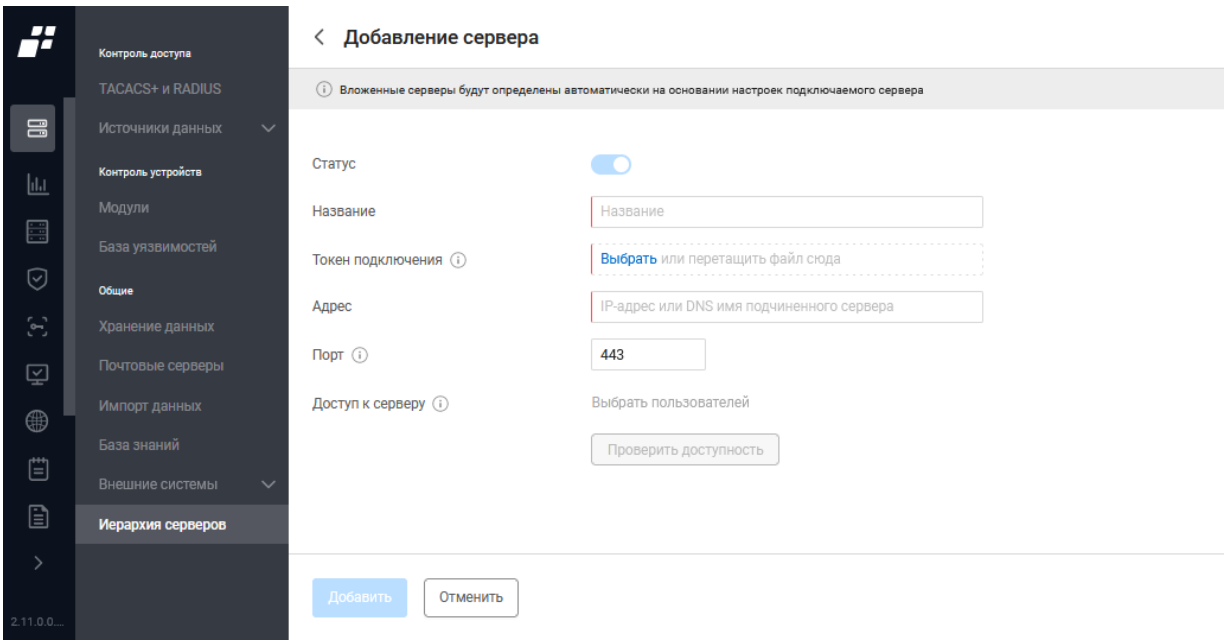


Рисунок 170 – Страница добавления подчиненного сервера

Таблица 60 – Состав и описание полей страницы добавления сервера

Поле	Описание
Поле «Статус»	Переключатель: — «Активен» ( ); — «Неактивен» ( ). Доступен для изменения только после создания сервера
Поле «Название»	Поле для ввода названия подчиненного сервера. Параметры ввода текста: от 1 до 50 символов. Допустимые символы: буквы латинского алфавита, цифры, «_», «–»
Поле «Токен подключения»	Поле для выбора токена, созданного на добавляемом сервере в разделе «Настройки» → «Общие» → «Иерархия серверов» → вкладка «Токены». Содержит ссылку для загрузки токена с локального ПК. Токен одноразовый и доступен для использования только в статусе «Действителен» и для того сервера, на котором он выпускался.
Поле «Адрес»	IP-адрес или DNS подчиненного сервера. Поле автоматически заполняется после заполнения поля «Токен». При необходимости поле доступно для редактирования
Поле «Порт»	Поле для ввода номера порта для подключения к серверу. По умолчанию номер порта для HTTPS 443 Допустимые значения: от 1 до 65535
Поле «Доступ к серверу»	Поле для выбора пользователей, которым назначен доступ к серверу. Поле доступно для редактирования после создания сервера
Элементы управления	
Проверить подключение	Кнопка для проверки доступности сервера
Добавить	При нажатии кнопки выполняется сохранение внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу без сохранения внесенных данных

11.10.2 Вкладка «Вышестоящие»

Вкладка «Вышестоящие» содержит список вышестоящих серверов (на один уровень выше), к которым текущий сервер подключен как нижестоящий (подчиненный).

Список вышестоящих сервероа доступен только для просмотра.

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

- сервер – адрес вышестоящего сервера;
- дата подключения – дата и время подключения текущего сервера к вышестоящему как подчиненного:
- последнее взаимодействие – дата и время последнего взаимодействия вышестоящего сервера с текущим сервером по иерархии, а также имя пользователя с вышестоящего сервера, который последним взаимодействовал с текущим подчиненным сервером

Над списком серверов располагаются:

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

11.10.3 Вкладка «Токены подключения»

На вкладке «Токены подключения» возможно создать и выгрузить на локальную ЭВМ токены подключения. Токены подключения необходимы для подключения текущего сервера в качестве подчиненного к вышестоящему серверу.

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

- название – название токена;
- дата создания токена и логин пользователя, создавшего токен;
- статус токена:
  - «Действителен»;
  - «Истек»;
  - «Использован».
- адрес вышестоящего сервера, к которому был подключен текущий сервер с использованием данного токена.

Над списком серверов располагаются:

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

При выборе строки с необходимым токеном в правом углу строки появляются кнопки:

- «Удалить» ( );
- «Экспорт» ( ). Экспорт доступен только для токенов со статусом «Действителен».

В нижней части страницы отображается информация об общем количестве токенов.

11.10.3.1 Создание токена

Для создания токена пользователю необходимо:

1) Выбрать раздел «Настройки», далее подраздел «Иерархия серверов», вкладка «Токены подключения».

2) Нажать кнопку «Токен» (+ Токен). Откроется страница создания токена (рис. 171). Заполнить поля страницы необходимыми параметрами и нажать кнопку «Создать». Состав и описание полей страницы приведены в таблице 61.

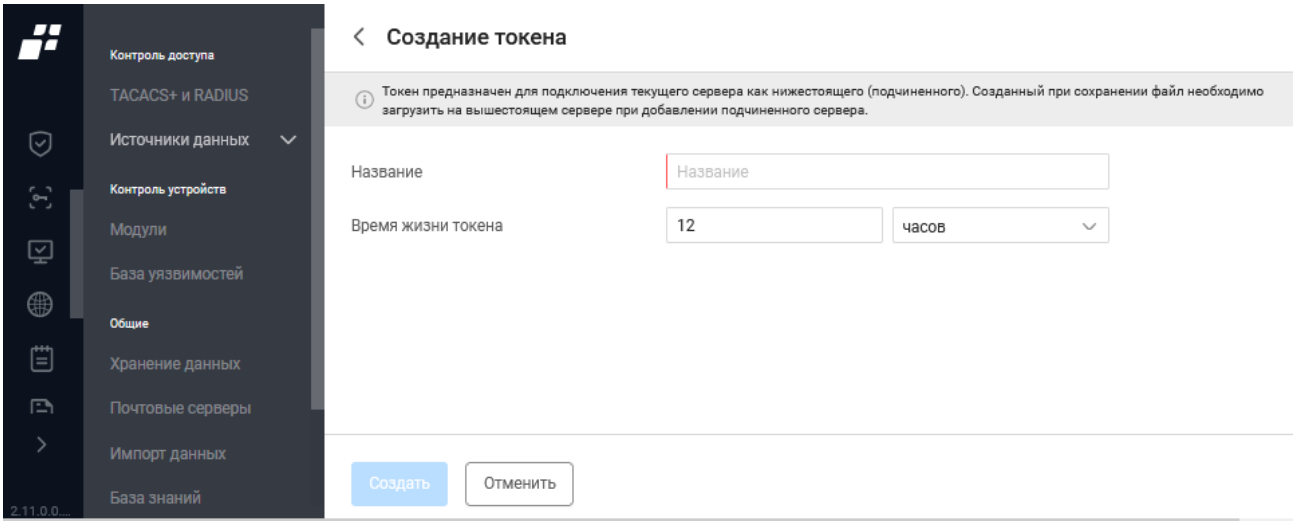


Рисунок 171 – Страница создания токена

Таблица 61 – Состав и описание полей страницы создания токена

Поле	Описание
Поле «Название»	Текстовое поле для ввода названия токена. Параметры ввода текста: от 1 до 50 символов. Допустимые символы: буквы латинского алфавита, цифры, «_», «–»
Поле «Время жизни токена»	Поле для ввода числового параметра в формате количества дней или часов
Элементы управления	
Создать	При нажатии кнопки выполняется сохранение внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу без сохранения внесенных данных

12 Сообщения об ошибках пользователю

12.1 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 осуществлена попытка входа под несуществующей записью;
- «Ваша сессия устарела, требуется повторный вход» – в случае, если бездействие пользователя длится больше времени, указанного в параметре «Блокировка пользователя, при неактивности»;
- «Пользователь заблокирован» – в случае, если осуществлена 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 комплекса. Во втором случае подождать указанное в параметре «Блокировка пользователя, при неактивности» время и повторить попытку аутентификации. В третьем случае необходимо обратиться к системному администратору комплекса.

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).

12.2 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 создании пользователя в поле «Пароль» указан 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.

12.3 Ошибки, связанные с лицензией на ПК «Efros DO»

Ошибки, связанные с лицензией на комплекс:

- «Ключ лицензии неверный» – ошибка во вводе ключа лицензии;
- «Ключ активации неверный» – ошибка во 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.

12.4 Ошибки, связанные с миграцией настроек хранения параметров почтовых серверов

В связи с миграцией настроек хранения параметров почтовых серверов, последние могут не проинициализироваться.

При возникновении ошибки пользователю рекомендуется обратиться к системному администратору комплекса.

Для устранения ошибки требуется воспользоваться следующим скриптом, запущенным в базе «Voltron»:

```
CREATE EXTENSION IF NOT EXISTS dblink;
insert into public.settings SELECT *
FROM dblink('hostaddr={IP-address} port={port_number} dbname=shedules
user={username} password={user_password}','SELECT name, type, value FROM
public.settings')
AS settings(name text, type text,value text);
```

В фигурных скобках указываются параметры конкретного сервера, заданные при импорте.

.

13 Завершение работы ПК «Efros DO»

Для завершения работы с веб-интерфейсом комплекса необходимо в заголовке текущей страницы нажать кнопку «Аккаунт» ( ), выбрать в раскрывшемся меню пункт «Выход» и закрыть вкладку используемого веб-браузера.

Приложение А
Примеры построенных маршрутов прохождения заявок

Примеры построенных в ПК «Efros DO» маршрутов прохождения заявок в сетевой структуре приведены на рисунках 172 и 173.

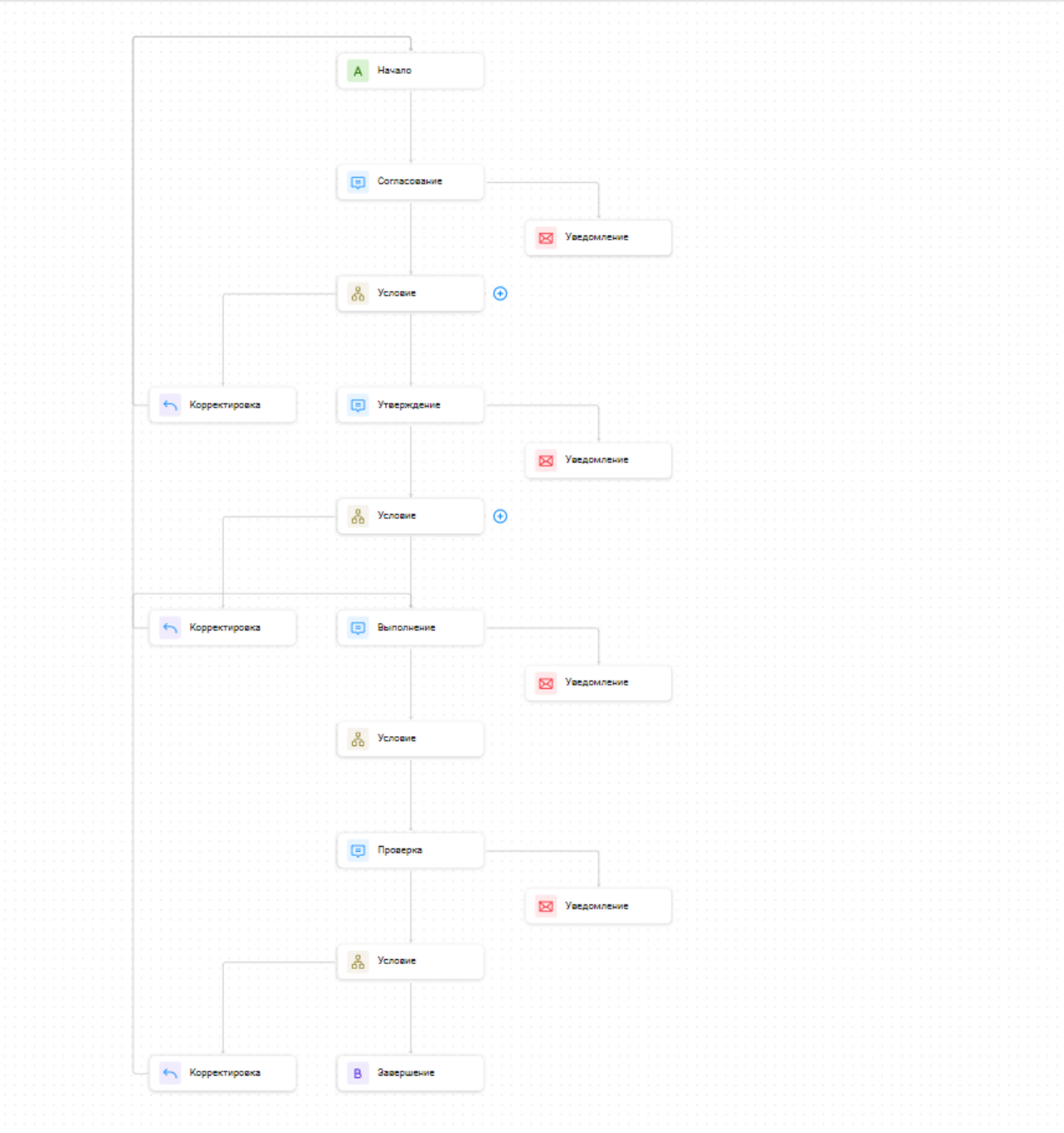


Рисунок 172 – Пример маршрута с большим количеством стадий

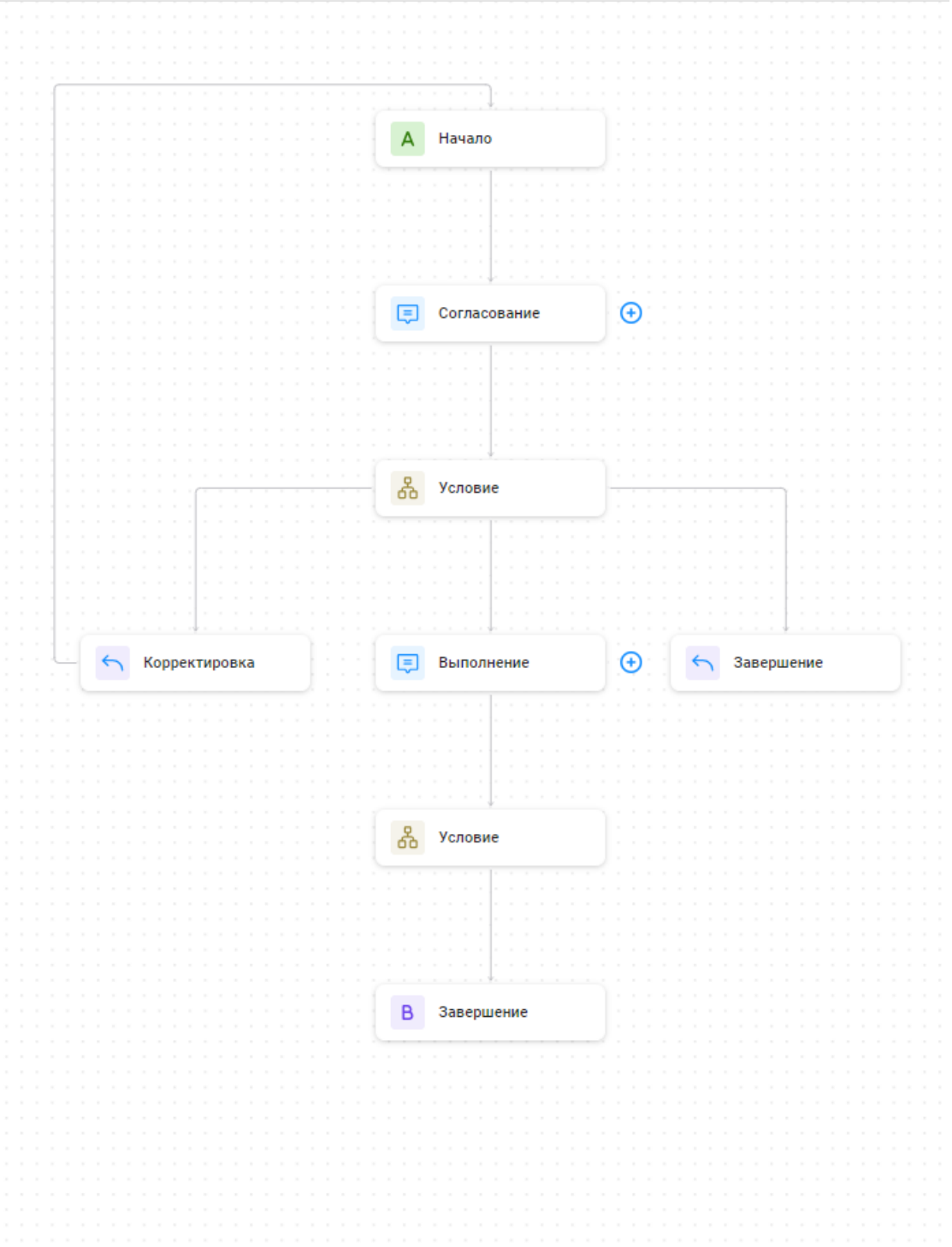


Рисунок 173 – Пример маршрута с малым количеством стадий

Приложение Б
Рекомендуемая последовательность работы с сертификатами

Б.1 Локальные сертификаты

Для настройки локальных сертификатов пользователю комплекса необходимо сделать следующие шаги:

1) Перейти в раздел «Администрирование», подраздел «Сертификаты», вкладка «Доверенные» (рис. 174).

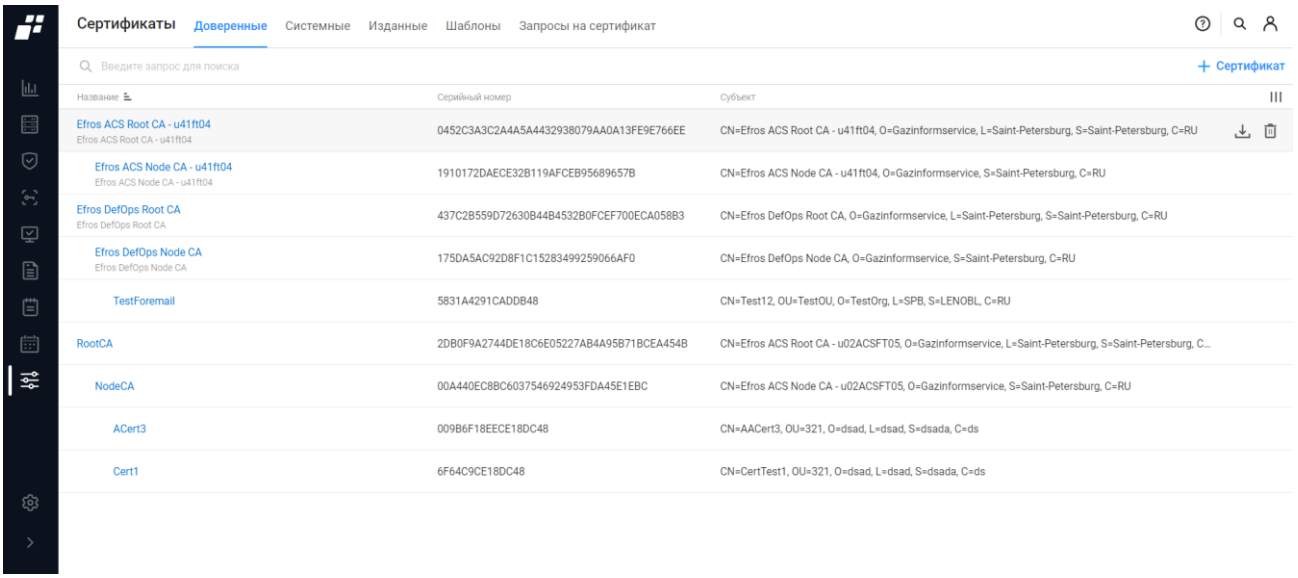


Рисунок 174 – Подраздел «Сертификаты», вкладка «Доверенные»

2) Скачать предустановленные корневой и промежуточный сертификаты («Efros DefOps Node CA» и «Efros DefOps Root CA»).
3) Установить корневой и промежуточный сертификаты на устройство.
4) Перейти на вкладку «Шаблоны» (рис. 175).

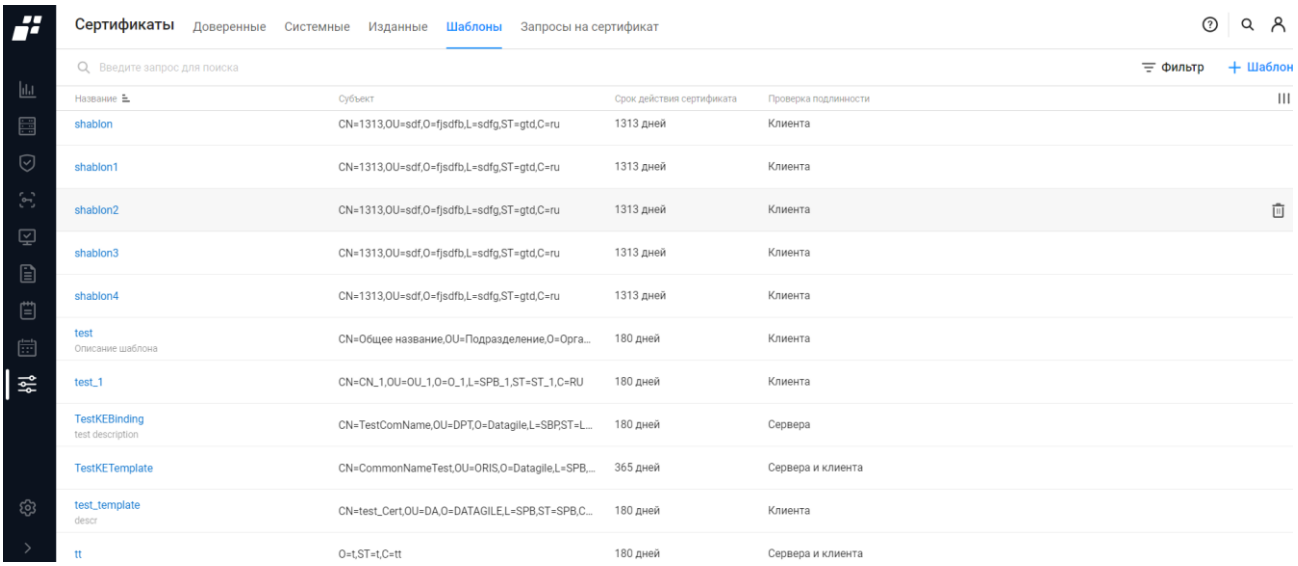


Рисунок 175 – Вкладка «Шаблоны»

5) Создать шаблон клиентского сертификата, заполнив поля необходимыми данными (рис. 176).

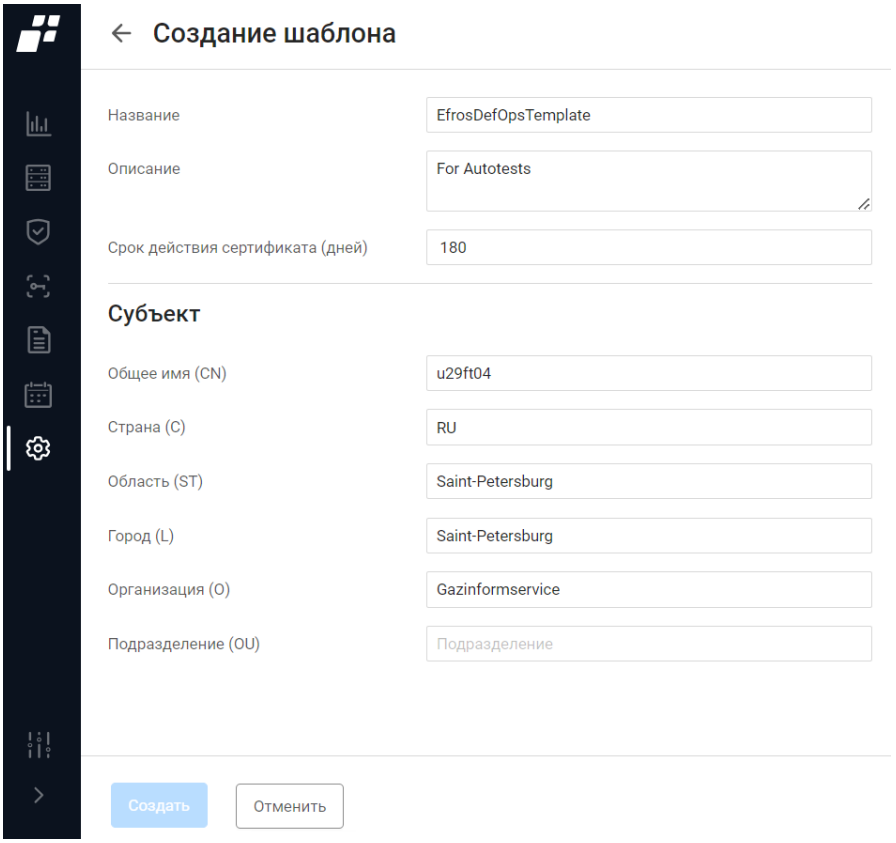


Рисунок 176 – Создание шаблона

6) Перейти на вкладку «Изданные» (рис. 177). Нажать кнопку « + Сертификат ».

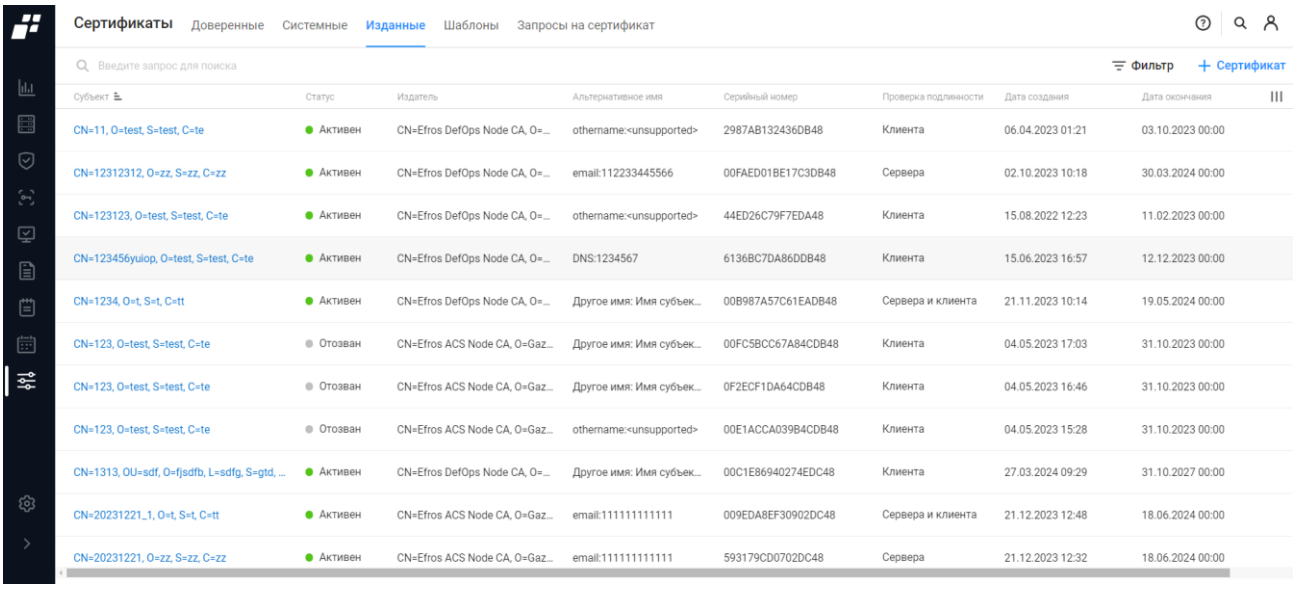


Рисунок 177 – Вкладка «Изданные»

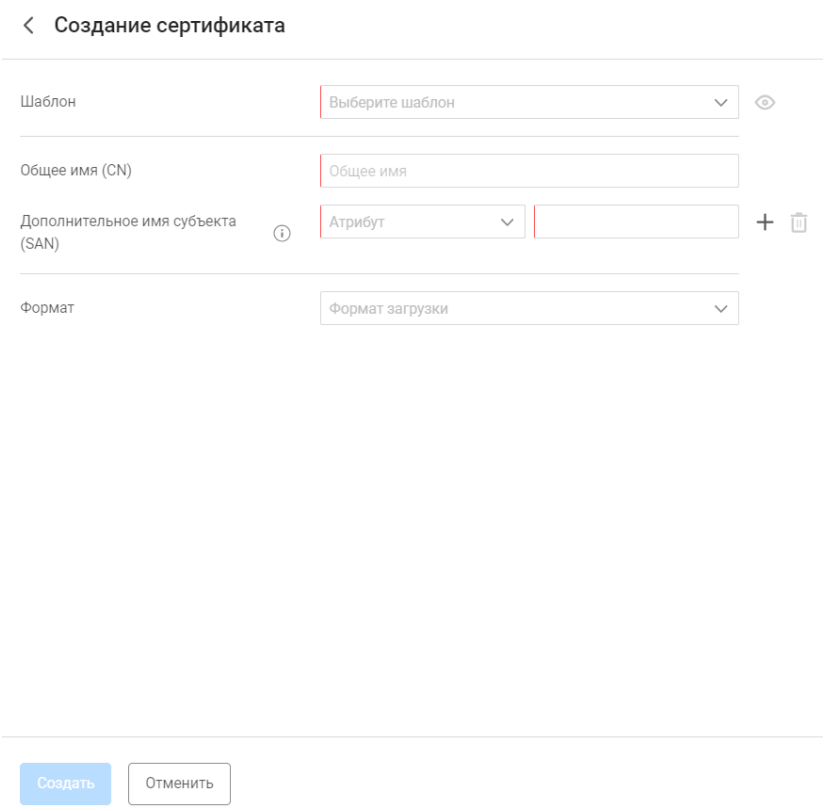


Рисунок 178 – Создание сертификата

7) Выбрать в поле «Шаблон» открывшегося окна «Создание сертификата» название требуемого шаблона.

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.

8) Указать дополнительное имя (одно или несколько) клиентской ЭВМ, для чего в поле «Дополнительное имя (SAN)»:
— выбрать в поле со списком тип дополнительного параметра: «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.
9) Выбрать формат сертификата.

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.

10) Для обеспечения взаимной аутентификации клиентских ЭВМ и сервера ПК «Efros DO» – выпустить клиентский сертификат.
11) Установить клиентский сертификат на устройство.

Использование шаблонов позволяет унифицировать и ускорить процесс выпуска сертификатов, поскольку параметры субъекта сертификата "Организация", "Подразделение", "Страна", "Город", "Область" могут быть одинаковыми для клиентских ЭВМ.

На рис. 179 представлена краткая схема по работе с локальными сертификатами.

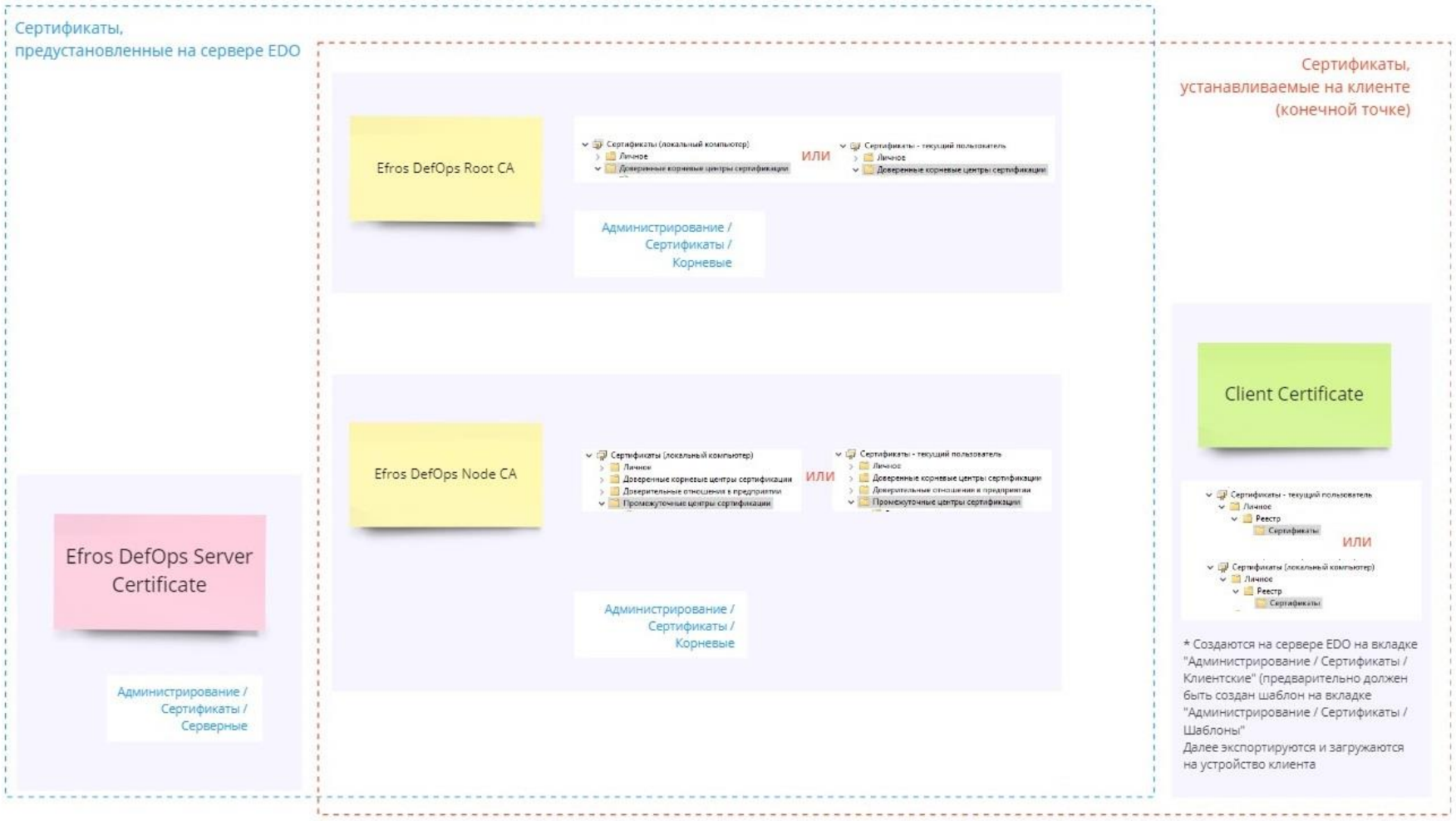


Рисунок 179 – Краткая схема по работе с локальными сертификатами[11]

[11] Расположение сертификатов на клиенте приведено для ОС Windows и зависит от особенностей реализации конкретного сценария доступа в сеть и используемой версии ОС. Рекомендуется руководствоваться документацией производителя ОС

Б.2 Сторонние сертификаты

Для настройки сторонних сертификатов пользователю комплекса необходимо сделать следующие шаги:

1) Перейти в раздел «Администрирование», подраздел «Сертификаты», вкладка «Корневые» (см. рис. 174).
2) Загрузить корневой сертификат, выданный сторонним Центром Сертификации (ЦС).
3) Перейти на вкладку «Системные» (рис. 180).

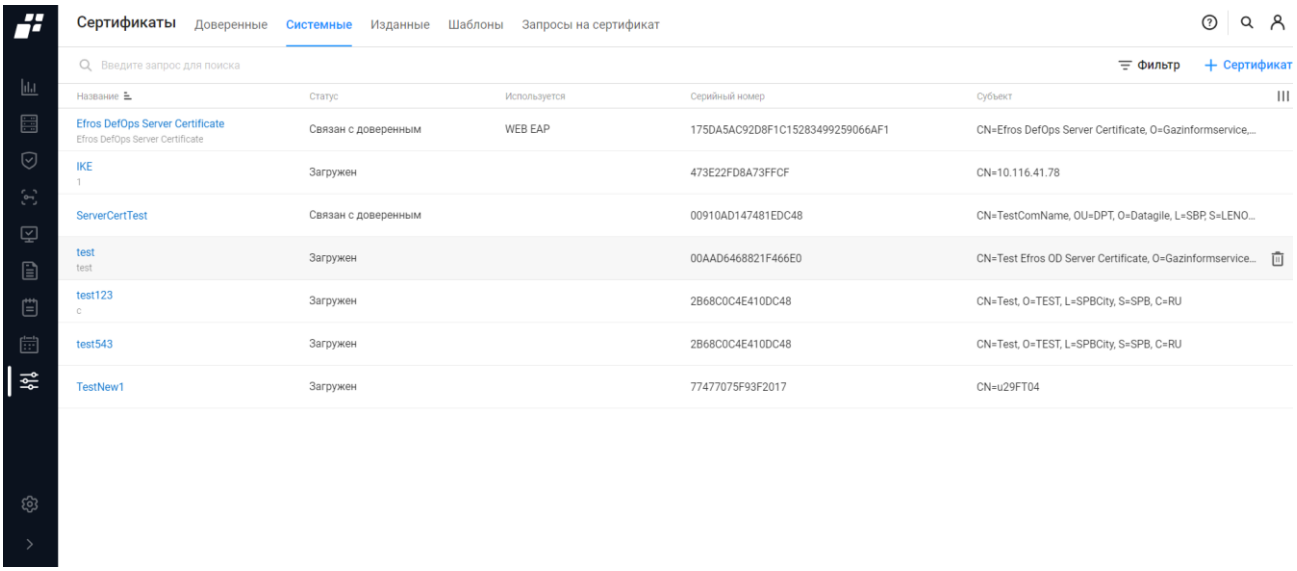


Рисунок 180 – Подраздел «Сертификаты», вкладка «Системные»

4) Загрузить системный сертификат, выданный сторонним ЦС.

При импорте системного сертификата автоматически определяется соответствующий ему доверенный сертификат. Если в БД комплекса не обнаружен соответствующий доверенный сертификат, то системный сертификат добавляется в список подраздела «Сертификаты» вкладка «Системные». Такой сертификат не доступен для выбора в настройках доступа в сеть (настройки TLS) в качестве системного сертификата, используемого при аутентификации устройств на сервере аутентификации. При этом соответствующий доверенный сертификат может быть добавлен в список сертификатов на вкладке «Доверенные» после добавления системного сертификата. В процессе добавления будет выполнена автоматическая привязка системного сертификата к добавленному доверенному, после чего системный сертификат будет доступен для выбора при настройке доступа в сеть в качестве системного сертификата, используемого при аутентификации устройств на сервере аутентификации.

Если необходимо создать новые доверенный/промежуточный и системный сертификаты, то:

1) Перейти на вкладку «Запросы на сертификат». Нажать кнопку «Запрос на сертификат» (рис. 181, 182).

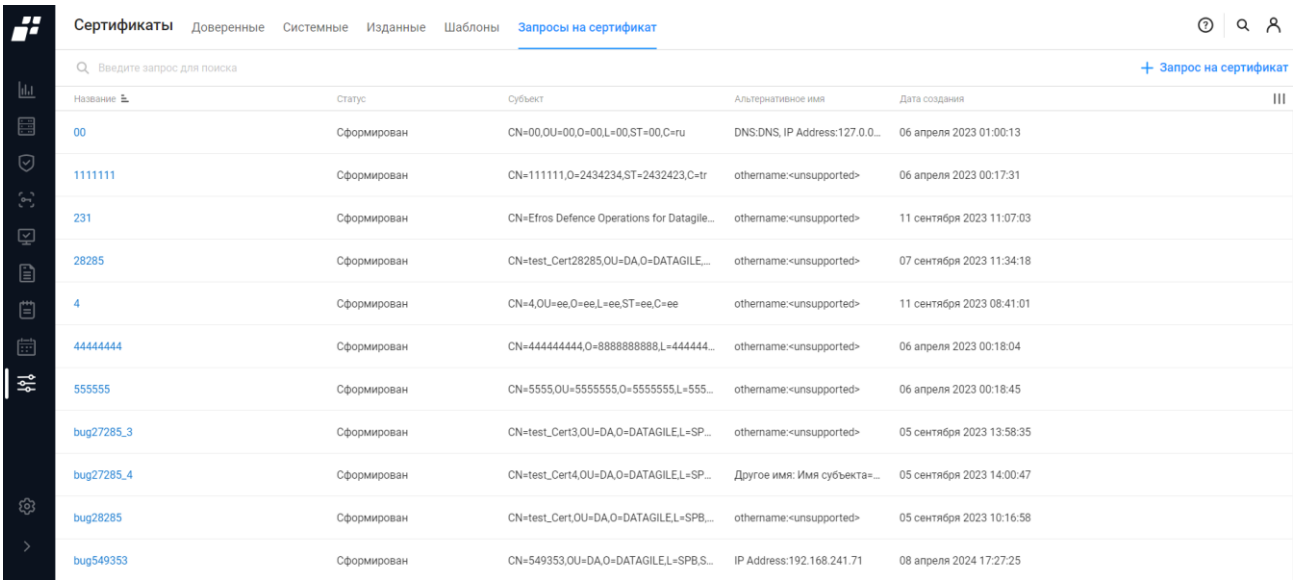


Рисунок 181 – Вкладка «Запросы на сертификат»

2) Создать запрос на сертификат (рис. 182).

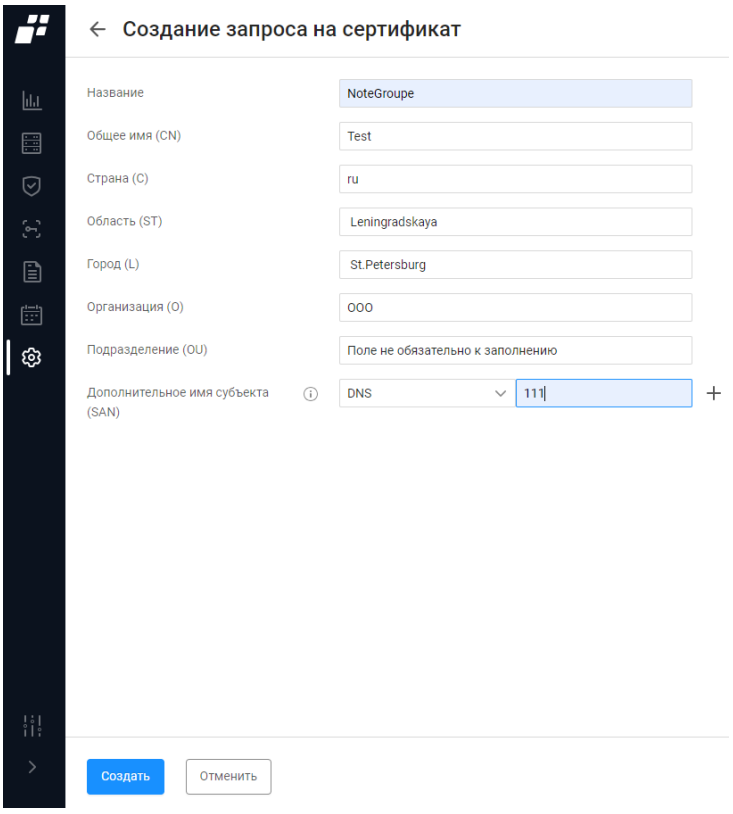


Рисунок 182 – Создание запроса на сертификат

3) Заполнить поля необходимыми данными.
4) Экспортировать сертификат в сторонний ЦС.
5) Получить от ЦС системный и доверенный сертификаты.
6) Загрузить системный и доверенный сертификаты в БД комплекса.
7) Привязать системный сертификат к запросу на сертификат. Доверенный сертификат автоматически свяжется с системным (рис. 183).

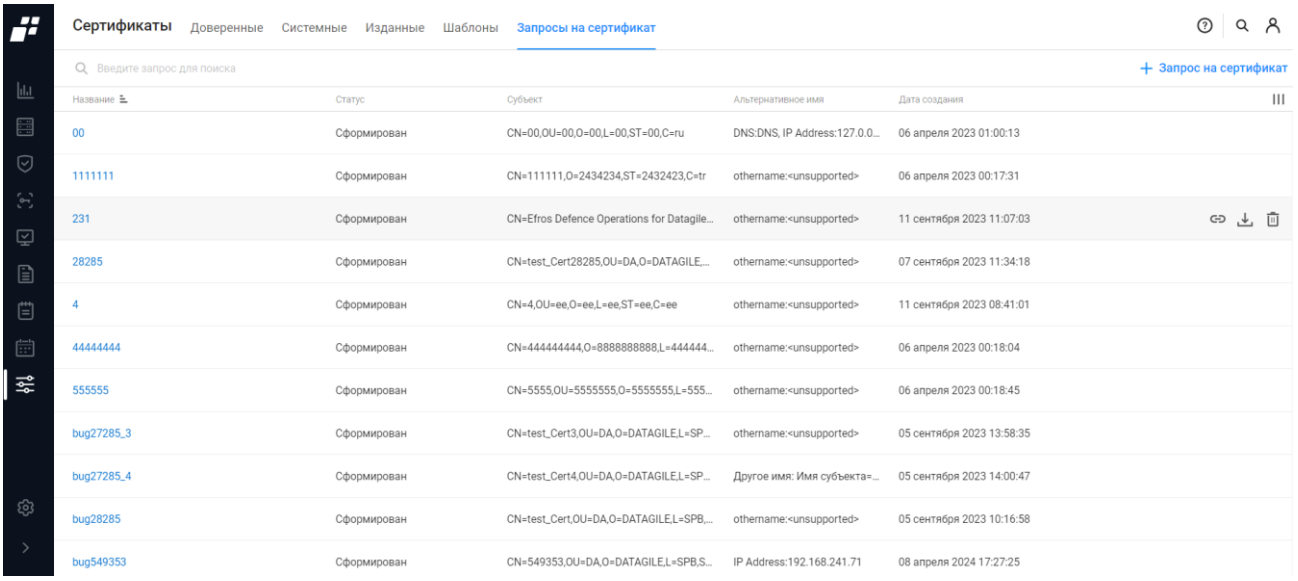


Рисунок 183 – Привязка запроса на серверный сертификат

При загрузке сторонних корневых и серверных сертификатов выдача локальных клиентских сертификатов, созданных в БД ПК «Efros DO», не требуется. Сторонние клиентские сертификаты контролируются сторонними корневым и серверным сертификатами.

Б.2.1 Генерация сертификата в FreeIPA

Б.2.1.1 Использование интерфейса командной строки

Действия по выпуску сертификата в FreeIPA можно выполнить с помощью интерфейса командной строки. Для выпуска сертификата необходимо сгенерировать запрос на сертификат.

Генерация запроса на сертификат осуществляется с помощью утилиты OpenSSL. Для генерации запроса необходимо сделать следующие шаги:

1) Подготовить конфигурационный файл с основными данными для сертификата:

```
$ cat san.conf
[ req ]
default_bits = 2048
```

```
distinguished_name = req_distinguished_name
req_extensions = req_ext
prompt = no
[ req_distinguished_name ]
countryName = RU
stateOrProvinceName = SPB
localityName = SPB
organizationName = Test ltd
commonName = prn.test.lan
[ req_ext ]
subjectAltName = @alt_names
[alt_names]
DNS.1 = prn.test.lan
IP.1 = 10.10.10.10
```

2) Выполнить генерацию пары закрытый/открытый ключ:

```
$ openssl genrsa -out private.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
..............................+++++
.....................................................+++++
e is 65537 (0x010001)
```

3) Сформировать запрос на сертификат на основе закрытого ключа и конфигурационного файла san.conf, подготовленного на первом шаге:

```
$ openssl req -out new-prn.csr -new -key private.key -config
san.conf
```

4) При необходимости просмотреть подготовленный запрос на выдачу сертификата:

```
$ openssl req -in new-prn.csr -noout -text
```

Пример сгенерированного запроса:

```
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: C = RU, ST = SPB, L = SPB, O = Test ltd, CN =
prn.test.lan
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:aa:74:42:60:bf:32:92:07:65:79:35:66:18:91:
                    7a:8b:89:f6:db:69:20:ea:9d:f1:a0:49:60:ed:88:
                    81:0a:3a:60:c3:ce:28:bb:e0:43:7e:2b:1e:e2:9e:
```

```
                    eb:82:7b:97:56:a7:18:d9:16:8d:30:0e:c9:09:8f:
                    c5:36:d3:ea:f6:e6:6a:c0:fa:76:9d:08:d2:f9:75:
                    3f:13:0c:82:39:18:86:02:8f:74:cc:e3:9a:9a:70:
                    c0:b2:df:0b:2a:78:52:6e:bc:ca:b4:58:6e:24:95:
                    79:0c:45:a0:20:93:45:dc:e5:1e:ff:f8:27:cc:54:
                    57:19:de:fb:38:e2:55:c3:90:cb:a9:02:d9:11:69:
                    79:f8:97:1a:36:a9:8c:c2:11:9a:ee:f9:7b:a2:3d:
                    64:ef:f8:3b:ce:44:27:eb:6a:69:a0:bf:fb:10:f1:
                    59:78:ef:25:b3:76:9e:4e:6d:34:5b:a6:ac:8c:bb:
                    fc:fc:0d:13:b9:9d:9c:45:a7:90:18:2e:0a:86:d3:
                    2c:1a:98:41:64:97:9a:b8:2c:03:6b:96:c6:df:43:
                    05:25:dd:e7:c0:e9:f9:30:20:a4:84:dc:bc:26:93:
                    68:62:af:ef:99:11:e9:41:3b:eb:ef:bc:77:f7:23:
                    9b:34:ee:f7:a1:18:61:04:43:7e:3c:ee:bb:c9:91:
                    aa:9f
                Exponent: 65537 (0x10001)
        Attributes:
        Requested Extensions:
            X509v3 Subject Alternative Name:
                DNS:prn.test.lan, IP Address:10.10.10.111
    Signature Algorithm: sha256WithRSAEncryption
         7f:27:8a:13:2e:ee:2b:5d:cf:2f:e8:8e:14:a7:58:57:9c:93:
         45:43:b7:2e:50:69:ef:dd:cd:14:3c:15:0b:85:79:7b:ac:51:
         07:06:11:5e:a3:63:15:27:8f:6c:7b:fd:5b:d8:99:40:7d:5d:
         3d:a4:d1:fa:df:d5:51:a3:ef:26:76:a2:7a:8e:5d:ee:65:a5:
         e0:d0:81:8f:a9:6b:77:46:66:b0:12:22:56:50:2b:f8:54:e0:
         d6:29:d7:e0:11:6f:8c:94:54:10:70:c4:36:d3:84:3a:82:0e:
         11:d2:e3:b4:3b:6d:7f:5b:b9:65:83:17:0d:f1:0e:81:5f:8f:
         40:5e:52:30:4b:cc:33:45:3b:c7:c1:bb:21:d5:83:60:e9:52:
         2c:d1:0a:ed:40:7f:79:66:31:64:17:e9:27:9e:af:12:73:86:
         28:19:6f:75:39:29:b7:82:46:72:84:e5:f3:c7:af:6a:d3:dc:
         d6:1d:73:b2:91:74:95:bd:e5:44:e5:b7:46:b9:39:1b:a0:20:
         85:9e:b1:f4:53:94:1d:3e:e7:3b:68:1b:24:ae:99:1b:d0:13:
         d2:f1:01:3c:b2:b8:c3:61:23:90:b9:93:3c:4f:73:7f:53:f3:
         3c:e1:6e:48:78:59:f7:bd:2c:5d:b8:71:95:66:3f:39:85:01:
         6b:b9:9e:81
```

Выпуск сертификата для сгенерированного запроса:

1) Если в домене FreeIPA еще не создана учетная запись для необходимого устройства, необходимо добавить записи в DNC для нового узла и добавить узел в базу домена FreeIPA. Для выполнения данных действий, требуется подключиться к серверу FreeIPA с учетной записью администратора домена и выполнить команды:

```
admin@freeipa1:$ ipa dnsrecord-add test.lan prn --a-rec 10.1.10.111
  Имя записи: prn
  A record: 10.10.10.111
```

```
admin@freeipa1:~$ ipa dnsrecord-add 10.10.10.in-addr.arpa. 111 --
ptr-rec prn.test.lan.
  Имя записи: 111
  PTR record: prn.test.lan.

admin@freeipa1:~$ ipa host-add prn.test.lan
---------------------------
Добавлен узел "prn.test.lan"
---------------------------
  Имя узла: prn.test.lan
  Имя учётной записи: host/prn.test.lan@TEST.LAN
  Псевдоним учётной записи: host/prn.test.lan@TEST.LAN
  Пароль: False
  Таблица ключей: False
  Managed by: prn.test.lan
```

2) Для выпуска сертификата ввести команду `ipa cert-request`, предварительно скопировав на сервер FreeIPA файл, содержащий запрос на сертификат (в примере файл «new-prn.csr»):

```
admin@freeipa1:~$ ipa cert-request new-prn.csr
--principal=HOST/prn.test.lan --add

  Выдающий CA: ipa
  Сертификат:
MIIEnTCCAwWgAwIBAgIBDzANBgkqhkiG9w0BAQsFADAzMREwDwYDVQQKDAhURVNULkxB
TjEeMBwGA1UEAwwVQ2VydGlmaWNhdGUgQXV0aG9yaXR5MB4XDTIzMTEwNzEyNTMxOFoX
DTI1MTEwNzEyNTMxOFowKjERMA8GA1UECgwIVEVTVC5MQU4xFTATBgNVBAMMDHBybi50
ZXN0LmxhbjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKp0QmC/MpIHZXk1
ZhiReouJ9ttpIOqd8aBJYO2IgQo6YMPOKLvgQ34rHuKe64J7l1anGNkWjTAOyQmPxTbT
6vbmasD6dp0I0vl1PxMMgjkYhgKPdMzjmppwwLLfCyp4Um68yrRYbiSVeQxFoCCTRdzl
Hv/4J8xUVxne+zjiVcOQy6kC2RFpefiXGjapjMIRmu75e6I9ZO/4O85EJ+tqaaC/+xDx
WXjvJbN2nk5tNFumrIy7/PwNE7mdnEWnkBguCobTLBqYQWSXmrgsA2uWxt9DBSXd58Dp
+TAgpITcvCaTaGKv75kR6UE76++8d/cjmzTu96EYYQRDfjzuu8mRqp8CAwEAAaOCAUMw
ggE/MB8GA1UdIwQYMBaAFGv2Olcuv+n0lBD0M7dgZauC08i2MDoGCCsGAQUFBwEBBC4w
LDAqBggrBgEFBQcwAYYeaHR0cDovL2lwYS1jYS50ZXN0Lmxhbi9jYS9vY3NwMA4GA1Ud
DwEB/wQEAwIE8DAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwcwYDVR0fBGww
ajBooDCgLoYsaHR0cDovL2lwYS1jYS50ZXN0Lmxhbi9pcGEvY3JsL01hc3RlckNSTC5i
aW6iNKQyMDAxDjAMBgNVBAoMBWlwYWNhMR4wHAYDVQQDDBVDZXJ0aWZpY2F0ZSBBdXRo
b3JpdHkwHQYDVR0OBBYEFIfGrvoWGFV+nGhK2dNQ5U4CALLOMB0GA1UdEQQWMBSCDHBy
bi50ZXN0LmxhbocECnSrbzANBgkqhkiG9w0BAQsFAAOCAYEAGqowT0p+j+NR1A/SE8Xn
pbEdZoHs7uWzJjS333MMFst1bfKoFhmHGlUyXslvUufCBxZjfZNAX3BHELFRRfuX12M2
aOFhBsBPK41a1fZl26BgBce8KU4oE5FWA9kjX3/ACgombKqSxInIE7ijwsjYbN+zLfeU
H9ON63J6V/WrNO5GUjZ0pQjRXrcHV6spB8thuW0cwoXCzcdoywkQWQ/nz8qit9d1/DUe
/hh7TfHmDvJ/SmJJ6AFAY7Sgs0iGdaeiK0sbrxwxxQYoewuh9UxWDcjMuu5Fr+zPeii6
3A3FNzQ4e7bletKRBv3SpCS5wrkCXCdG4QBm4tGLFDz/lTY38LPNqxhz33iryQ6DEuzF
yz6lqBZLUXCfdgaY/d491Fm3dB4WuGmLXIzGTv+UiUOjRaWH6F4Vcjr89Q/sO38+4R44
1JAc2pSAV+P34v80yLiOexY/y77uyxdommqAuT7uk5zyeRXREom9Di7E5xk30NfqPfg1
o0zgVrBtjNy+oeJQ
```

```
  Субъект: CN=prn.test.lan,O=TEST.LAN
  DNS-имя субъекта: prn.test.lan
  Издатель: CN=Certificate Authority,O=TEST.LAN
  Недействителен до: Tue Nov 07 12:53:18 2023 UTC
  Недействителен после: Fri Nov 07 12:53:18 2025 UTC
  Серийный номер: 15
  Серийный номер (hex): 0xF
```

3) Для экспорта сертификата и сохранения его в файл необходимо:

— выполнить команду:

```
ipa cert-show <серийный_номер> --out=prn_cert.pem
```

— заменить <серийный_номер> на фактический номер, предоставленный на предыдущем шаге (в примере номер «15»):

```
admin@freeipa1:~$ ipa cert-show 15 --out prn_cer.pem
  Выдающий CA: ipa
  Сертификат:
MIIEnTCCAwWgAwIBAgIBDzANBgkqhkiG9w0BAQsFADAzMREwDwYDVQQKDAhURVNULkxB
TjEeMBwGA1UEAwwVQ2VydGlmaWNhdGUgQXV0aG9yaXR5MB4XDTIzMTEwNzEyNTMxOFoX
DTI1MTEwNzEyNTMxOFowKjERMA8GA1UECgwIVEVTVC5MQU4xFTATBgNVBAMMDHBybi50
ZXN0LmxhbjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKp0QmC/MpIHZXk1
ZhiReouJ9ttpIOqd8aBJYO2IgQo6YMPOKLvgQ34rHuKe64J7l1anGNkWjTAOyQmPxTbT
6vbmasD6dp0I0vl1PxMMgjkYhgKPdMzjmppwwLLfCyp4Um68yrRYbiSVeQxFoCCTRdzl
Hv/4J8xUVxne+zjiVcOQy6kC2RFpefiXGjapjMIRmu75e6I9ZO/4O85EJ+tqaaC/+xDx
WXjvJbN2nk5tNFumrIy7/PwNE7mdnEWnkBguCobTLBqYQWSXmrgsA2uWxt9DBSXd58Dp
+TAgpITcvCaTaGKv75kR6UE76++8d/cjmzTu96EYYQRDfjzuu8mRqp8CAwEAAaOCAUMw
ggE/MB8GA1UdIwQYMBaAFGv2Olcuv+n0lBD0M7dgZauC08i2MDoGCCsGAQUFBwEBBC4w
LDAqBggrBgEFBQcwAYYeaHR0cDovL2lwYS1jYS50ZXN0Lmxhbi9jYS9vY3NwMA4GA1Ud
DwEB/wQEAwIE8DAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwcwYDVR0fBGww
ajBooDCgLoYsaHR0cDovL2lwYS1jYS50ZXN0Lmxhbi9pcGEvY3JsL01hc3RlckNSTC5i
aW6iNKQyMDAxDjAMBgNVBAoMBWlwYWNhMR4wHAYDVQQDDBVDZXJ0aWZpY2F0ZSBBdXRo
b3JpdHkwHQYDVR0OBBYEFIfGrvoWGFV+nGhK2dNQ5U4CALLOMB0GA1UdEQQWMBSCDHBy
bi50ZXN0LmxhbocECnSrbzANBgkqhkiG9w0BAQsFAAOCAYEAGqowT0p+j+NR1A/SE8Xn
pbEdZoHs7uWzJjS333MMFst1bfKoFhmHGlUyXslvUufCBxZjfZNAX3BHELFRRfuX12M2
aOFhBsBPK41a1fZl26BgBce8KU4oE5FWA9kjX3/ACgombKqSxInIE7ijwsjYbN+zLfeU
H9ON63J6V/WrNO5GUjZ0pQjRXrcHV6spB8thuW0cwoXCzcdoywkQWQ/nz8qit9d1/DUe
/hh7TfHmDvJ/SmJJ6AFAY7Sgs0iGdaeiK0sbrxwxxQYoewuh9UxWDcjMuu5Fr+zPeii6
3A3FNzQ4e7bletKRBv3SpCS5wrkCXCdG4QBm4tGLFDz/lTY38LPNqxhz33iryQ6DEuzF
yz6lqBZLUXCfdgaY/d491Fm3dB4WuGmLXIzGTv+UiUOjRaWH6F4Vcjr89Q/sO38+4R44
1JAc2pSAV+P34v80yLiOexY/y77uyxdommqAuT7uk5zyeRXREom9Di7E5xk30NfqPfg1
o0zgVrBtjNy+oeJQ
  Субъект: CN=prn.test.lan,O=TEST.LAN
  DNS-имя субъекта: prn.test.lan
  Издатель: CN=Certificate Authority,O=TEST.LAN
  Недействителен до: Tue Nov 07 12:53:18 2023 UTC
  Недействителен после: Fri Nov 07 12:53:18 2025 UTC
```

```
  Серийный номер: 15
  Серийный номер (hex): 0xF
  Отозван: False
  Owner service: HOST/prn.test.lan@TEST.LAN

admin@freeipa1:~$ ls -l *.pem
-rw-r--r-- 1 admin admins 1659 ноя  7 17:34 prn_cer.pem
```

Б.2.1.2 Использование веб-интерфейса FreeIPA

Действия по выпуску сертификата можно выполнить в веб-интерфейсе FreeIPA сервера. Для этого необходимо сделать следующие шаги:

1) Создать новый узел. Поочередно выбрать разделы: «Идентификация → Узлы». Нажать кнопку «Добавить» (рис. 184).

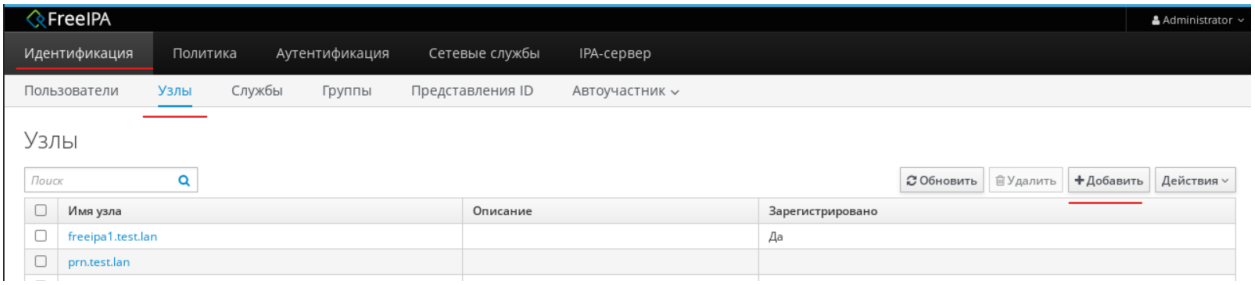


Рисунок 184 – Вкладка «Узлы» в FreeIPA

2) В появившимся окне ввести данные: «Имя узла», «Зона DNS», «IP-адрес».
3) Нажать кнопку «Добавить». Откроется окно «Добавить узел» (рис. 185).

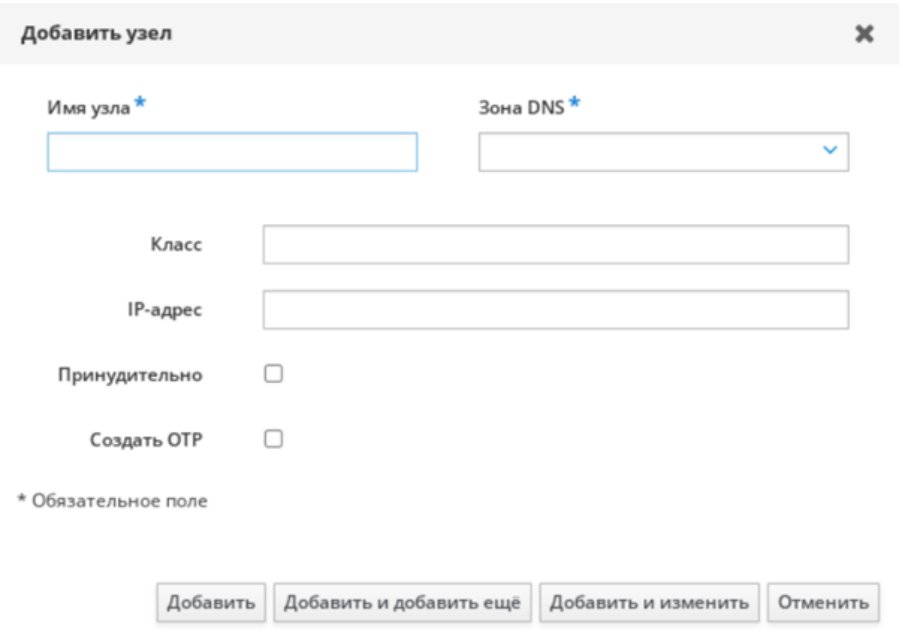


Рисунок 185 – Окно «Добавить узел»

4) Далее выполнить переход: «Аутентификация → Сертификаты → Сертификаты». Нажать кнопку «Выдать» (рис. 186).

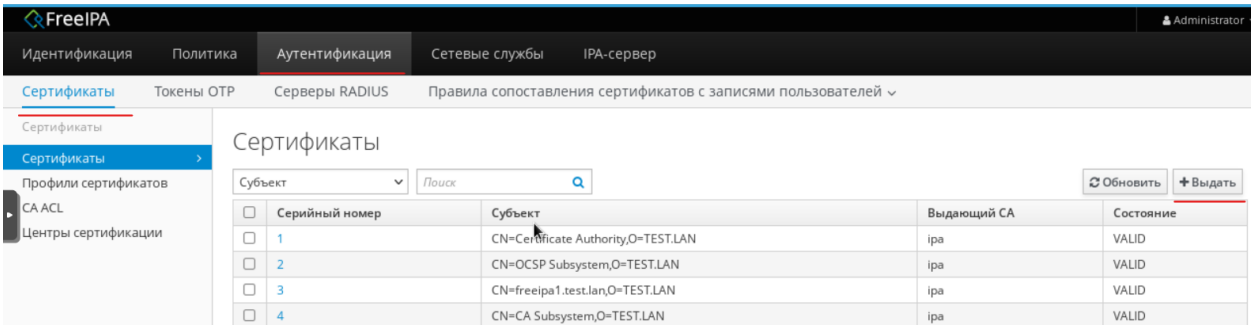


Рисунок 186 – Вкладка «Сертификаты»

5) В появившемся окне выдачи нового сертификата необходимо выполнить действия (рис. 187):

— в поле «Учетная запись» добавить данные в формате HOST/доменное имя хоста;
— установить флаг «Добавить учетную запись»;
— выбрать необходимые значения в поле «Центр сертификации (CA)»;
— выбрать необходимые значения в поле «Идентификатор профиля»;
— ввести заранее созданный зашифрованный запрос на сертификат в соответствующее поле;
— нажать кнопку «Выдать».

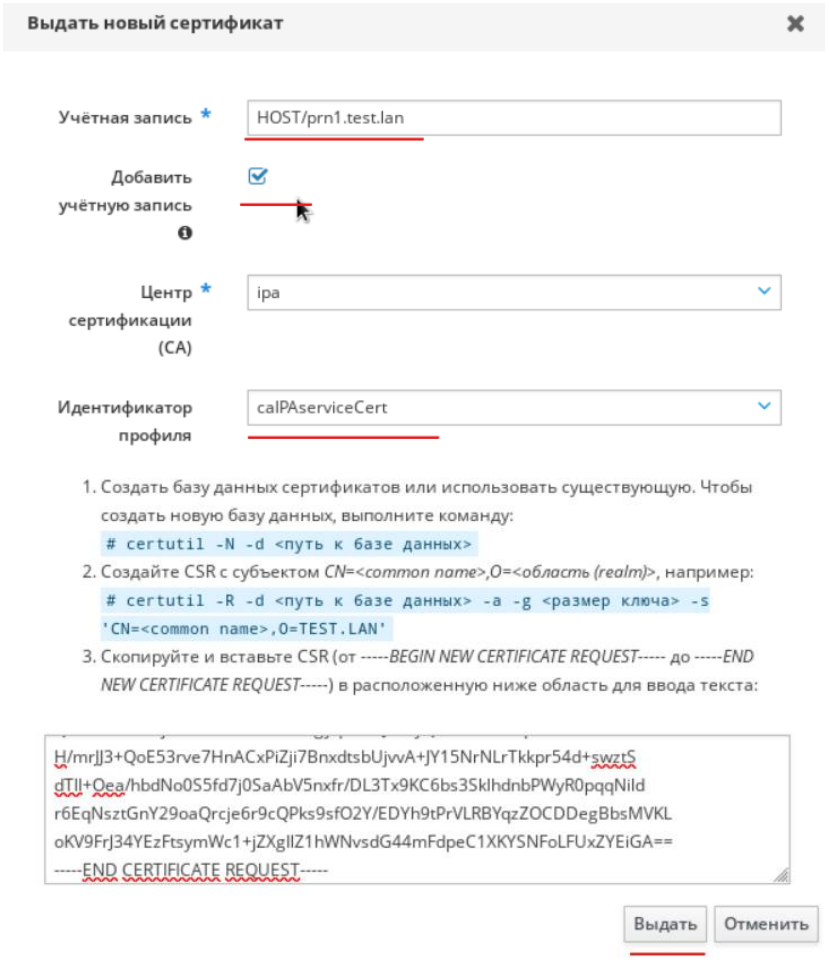


Рисунок 187 – Пример заполнения окна «Выдать новый сертификат»

6) В списке сертификатов появится новый сертификат (рис. 188).

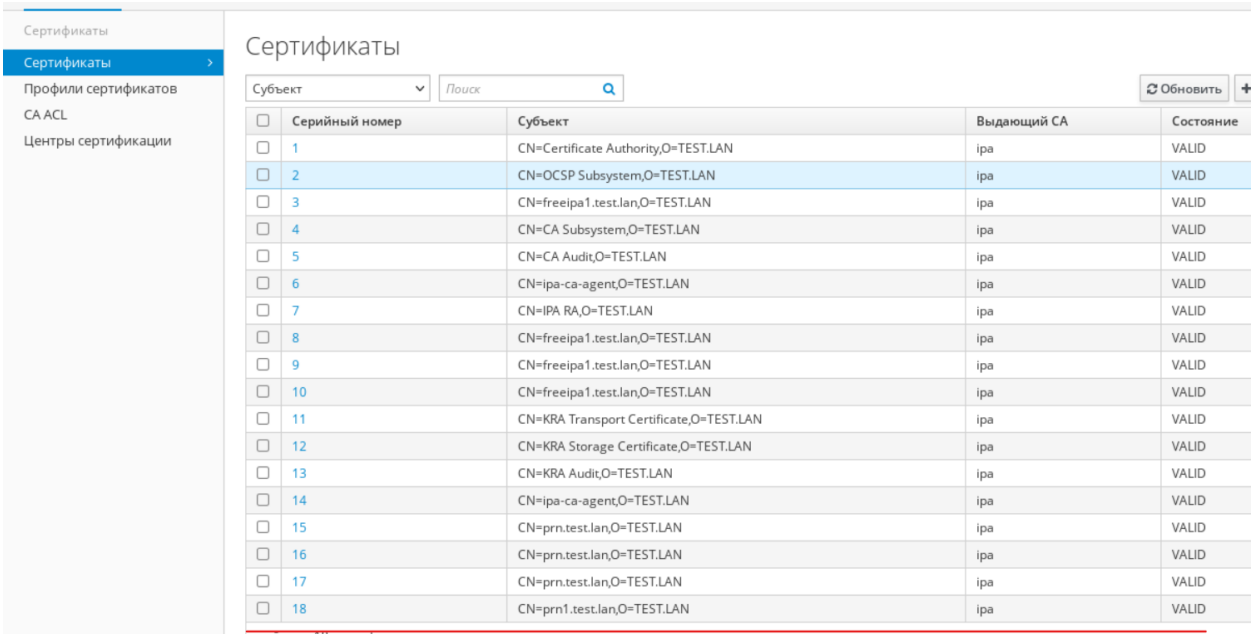


Рисунок 188 – Новый сертификат на вкладке «Сертификаты»

7) Для экспорта сертификата в виде файла необходимо выбрать сгенерированный сертификат, в открывшемся окне развернуть вкладку «Действия» и нажать кнопку «Загрузить» (рис. 189). В результате сертификат будет сохранен на ЭВМ.

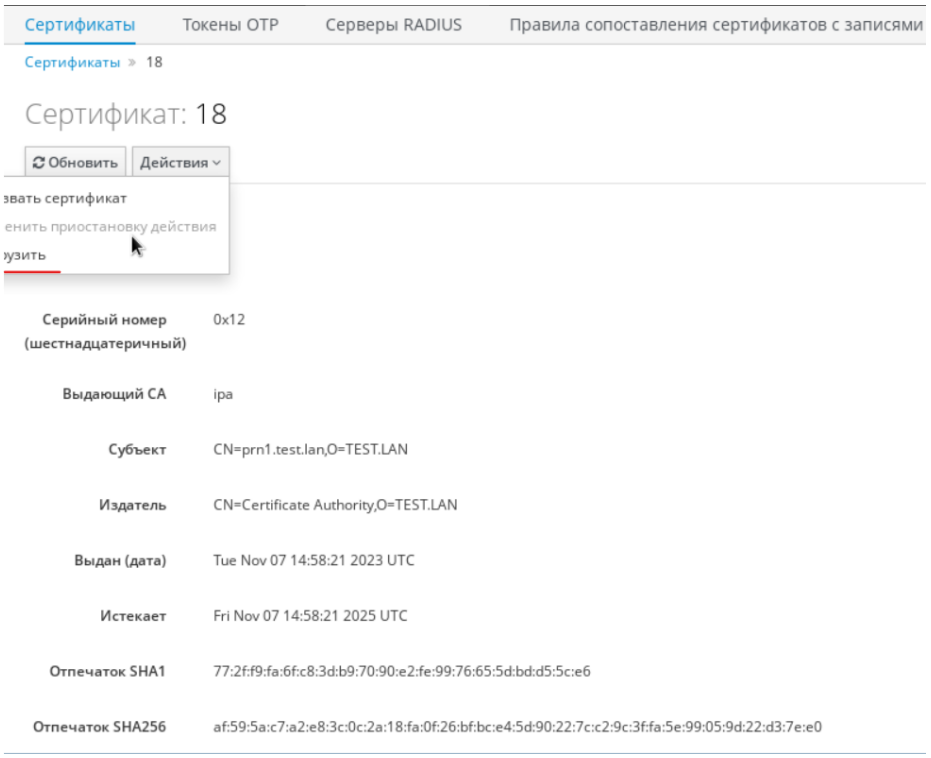


Рисунок 189 – Окно сгенерированного сертификата

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
CVSS	–	Common Vulnerability Scoring System
DES	–	Data Encryption Standard
DGA	–	Domain Generation Algorithm
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
IDS	–	Intrusion Detection System
IIS	–	Internet Information Services
IP	–	Internet Protocol
IPFIX	–	Internet Protocol Flow Information Export
IPS	–	Intrusion Prevention System
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
TOTP	–	Time-based One-Time Password
TTLS	–	Tunneled Transport Layer Security
UDP	–	User Datagram Protocol
UPN	–	User Principal Name
URI	–	Uniform Resource Identifier
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
ИБ	–	Информационная безопасность
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
ЭВМ	–	Электронно-вычислительная машина
ЦС	–	Центр Сертификации