

Программный комплекс централизованного
управления контролем доступа к сетевым
устройствам «Efros ACS»

Руководство пользователя

Аннотация

Данный документ представляет собой руководство пользователей с административными правами для работы с программным комплексом (ПК) централизованного управления контролем доступа к сетевым устройствам (далее – ПК «Efros ACS»). Руководство содержит сведения, необходимые пользователям для настройки доступа пользователей ПК «Efros ACS» к сетевым ресурсам и функциям ПК «Efros ACS», а также контроля работы ПК «Efros ACS» с использованием веб-интерфейса ПК «Efros ACS».

Руководство пользователя содержит следующие разделы:

- раздел 1, в котором указаны общие сведения о назначении ПК «Efros ACS» и выполняемых им функциях;
- раздел 2, в котором указан состав аппаратных и программных средств, необходимых для работы ПК «Efros ACS»;
- раздел 3, в котором указана последовательность действий пользователя, обеспечивающих запуск, выполнение функций и завершение работы ПК «Efros ACS»;
- раздел 4, в котором приведен перечень сообщений пользователям о возможных ошибках в работе ПК «Efros ACS», выдаваемых в ходе выполнения функций ПК «Efros ACS», и соответствующие действия пользователя.

Для настройки работы ПК «Efros ACS» 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).

При изучении и работе с ПК «Efros ACS» необходимо дополнительно руководствоваться:

- 1) Эксплуатационной документацией на используемые программные и программно-технические средства ПК «Efros ACS».
- 2) Эксплуатационной документацией на подключенное к ПК «Efros ACS» АСО



Важная информация

Указания, требующие особого внимания.



Дополнительная информация

Указания, позволяющие упростить работу с подсистемой.

Содержание

1	Назначение ПК «Efros ACS»	6
1.1	Назначение	6
1.2	Выполняемые функции	6
1.3	Роли и аутентификация пользователей	8
2	Условия выполнения ПК «Efros ACS»	11
3	Выполнение ПК «Efros ACS»	13
3.1	Запуск веб-приложения ПК «Efros ACS»	13
3.1.1.	Запуск веб-приложения ПК «Efros ACS» и аутентификация пользователя	13
3.1.2.	Смена пароля	15
3.1.3.	Настройка аккаунта администратора ACS или RO	17
3.1.4.	Просмотр уведомлений администраторами ACS и RO	21
3.1.5.	Выбор настраиваемого сервера (при наличии подчиненных серверов)	23
3.2	Работа со списками сущностей ПК «Efros ACS». Общие сведения	24
3.2.1.	Выбор сортировки записей таблиц	28
3.2.2.	Поиск данных в таблицах списков сущностей	28
3.2.3.	Выбор периода внесения последних изменений в данные сущности	28
3.2.4.	Фильтрация данных в таблицах сущностей	30
3.2.5.	Настройка состава отображаемых столбцов в таблицах списков сущностей	31
3.2.6.	Удаление сущностей	32
3.3	Мониторинг текущего состояния ПК «Efros ACS»	33
3.4	Просмотр и настройка параметров работы ПК «Efros ACS»	35
3.4.1.	Общие сведения	35
3.4.2.	Ведение списков цифровых сертификатов	38
3.4.3.	Настройка служб протоколов TACACS+ и RADIUS	58
3.4.4.	Настройка интеграции с внешними системами	60
3.4.5.	Настройка доступа в сеть	71
3.4.6.	Настройка подключения к внешним источникам данных	80
3.4.7.	Выполнение общих настроек	95
3.4.8.	Управление подчиненными серверами	101
3.4.9.	Управление отказоустойчивостью	104

3.4.10. Лицензирование	108
3.5 Просмотр и ведение списка контролируемого АСО	108
3.5.1. Просмотр списка АСО.....	108
3.5.2. Фильтрация данных в таблице АСО.....	110
3.5.3. Ведение списка АСО.....	112
3.6 Просмотр и ведение списка групп АСО	120
3.6.1. Просмотр списка групп АСО.....	120
3.6.2. Ведение списка групп АСО.....	123
3.7 Просмотр и ведение списка клиентского оборудования	130
3.7.1. Просмотр списка клиентского оборудования	130
3.7.2. Ведение списка КО	132
3.8 Просмотр и ведение списка групп КО	135
3.9 Просмотр и ведение списков пользователей и администраторов, групп пользователей.....	137
3.9.1. Просмотр списков пользователей и администраторов	138
3.9.2. Просмотр списка групп пользователей и данных групп пользователей	143
3.9.3. Фильтрация данных в таблицах пользователей и администраторов	147
3.9.4. Ведение списка пользователей	149
3.9.5. Ведение списка групп пользователей	166
3.10 Настройка политик доступа	175
3.10.1. Наборы политик	176
3.10.2. Ведение списка профилей оборудования.....	188
3.10.3. Ведение списка профилей авторизации	196
3.10.4. Загружаемые ACL	201
3.10.5. Наборы команд.....	207
3.10.6. Конструктор условий.....	214
3.11 Просмотр и выгрузка журналов событий ПК «Efros ACS».....	221
3.11.1. Общие сведения	221
3.11.2. Просмотр журнала событий «TACACS+».....	222
3.11.3. Просмотр журнала событий «RADIUS».....	226
3.11.4. Просмотр журнала событий «Система»	231
3.11.5. Экспорт журналов в файлы формата CSV и XLSX	232

3.12	Отчеты ПК «Efros ACS»	233
3.12.1.	Шаблоны отчетов	233
3.12.2.	Список сформированных отчетов.....	245
3.13	Завершение работы ПК «Efros ACS».....	248
4	Сообщения пользователю	249
4.1	При запуске ПК «Efros ACS».....	249
4.2	При выполнении функции по фильтрации данных журнала событий	249
4.3	Перечень возможных сообщений пользователю при создании/редактировании записей списков ПК «Efros ACS»	250
	Перечень сокращений	251

1 Назначение ПК «Efros ACS»

1.1 Назначение

ПК «Efros ACS» является специализированным программным комплексом, который обеспечивает возможность централизованной сетевой идентификации администраторов и управления доступом на сетевых устройствах, у которых на клиентском уровне поддерживаются протоколы TACACS+ и (или) RADIUS.

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

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

1.2 Выполняемые функции

 Доступ к функциям ПК «Efros ACS» пользователи получают только после активации лицензии на комплекс и в объеме, предусмотренном лицензией (подробнее см. п.3.4.9)!

В ПК «Efros ACS» реализованы следующие функциональные возможности:

- управление доступом к сетевым устройствам, поддерживающим на клиентском уровне протоколы TACACS+ и (или) RADIUS;
- централизованное управление учетными данными и настройками ПК «Efros ACS»;
- поддержка двухуровневой иерархии серверов;
- управление отказоустойчивостью;
- поддержка внешнего источника учетных записей (LDAP-сервер или Active Directory Services (AD DS));
- ведение журнала системных событий;
- авторизация сетевых устройств (Endpoints) по MAC-адресам;
- авторизация устройств с использованием расширяемого протокола аутентификации EAP;
- гибкая конфигурация службы выполнения команд на АСО;
- регистрация фактов доступа к АСО;

- поддержка ролевой модели администраторов комплекса;
- объединение в группы учетных записей пользователей АСО;
- объединение в группы сетевых устройств;
- экспорт журналов событий в ПК «Ankey SIEM»;
- экспорт журналов в файловую систему в виде CSV или XLSX;
- получение списка сетевых устройств из ПК «Efros Config Inspector» (ПК «Efros CI»)¹;
- импорт пользователей АСО и списка сетевых устройств из ПО «Cisco ACS»;
- контроль состояния комплекса и работоспособности основных служб.

Единый пользовательский веб-интерфейс ПК «Efros ACS» предоставляет доступ пользователям с административными правами к следующим функциональным возможностям:

- 1) Управление учетными записями:
 - администраторов ПК «Efros ACS»;
 - сетевых пользователей;
 - групп сетевых пользователей.
- 2) Управление инфраструктурой:
 - сетевыми устройствами (АСО и клиентским оборудованием);
 - группами сетевых устройств.
- 3) Управление правилами доступа к сетевому оборудованию.
- 4) Управление настройками ПК.
- 5) Просмотр журналов событий.
- 6) Настройка и просмотр отчетов.

Управление настройками ПК «Efros ACS» включает:

- ведение списка корневых, серверных, клиентских сертификатов, создание запросов на сертификаты, создание шаблонов клиентских сертификатов;
- настройку подключения к сервисам протоколов TACACS+ и RADIUS;
- настройку интеграции с внешними системами: ПК «Efros CI», ПК «Ankey SIEM» и ПО «Cisco ACS»;
- настройку доступа ПК «Efros ACS» в сеть;

¹ поддерживается работа с ПК «Efros Config Inspector» версии 4.5 до 4.7

- настройку подключения к внешним источникам данных (серверам LDAP, AD DS);
- настройку подчиненных серверов;
- настройку отказоустойчивости (создание кластеров);
- настройку парольной политики;
- активацию/сброс лицензии.

Статус текущего состояния ПК «Efros ACS» и состояние служб протоколов отображаются в веб-интерфейсе и включают следующие разделы:

- «Общая информация» – содержит данные об использовании аппаратных ресурсов, сетевых настройках, состоянии базы данных;
- «Пользователи и устройства» – содержит данные об общем количестве и состоянии пользователей, количестве сетевых устройств и групп;
- «Состояние служб и модулей» – отображает информацию о статусе служб ПК «Efros ACS»;
- «Журнал аварийных сигналов» – отображает события из журнала «Система» с уровнями «Предупреждения» и «Ошибки».

В ПК «Efros ACS» реализована поддержка протоколов для аутентификации, авторизации и учета (AAA) действий пользователя на сетевых устройствах.

Управление доступом к сетевым устройствам определяется следующими параметрами:

- поддержкой сетевыми устройствами протоколов TACACS+ и/или RADIUS;
- добавлением сетевого устройства в ПК «Efros ACS» с указанием типа протокола TACACS+ и/или RADIUS и разделяемого ключа;
- созданием правила доступа путем сопоставления пользователю сетевого устройства и назначения пользователю списка доступных для выполнения на устройстве команд.

Применение настроек доступа производится сразу после изменения параметров пользователя и устройства. Аналогичное поведение применяется для групп пользователей и групп устройств.

1.3 Роли и аутентификация пользователей

Пользователями ПК «Efros ACS» являются:

- 1) Администраторы ПК «Efros ACS».
- 2) Сетевые пользователи:
 - администраторы АСО;

- пользователи, использующие рабочие станции и другое клиентское оборудование, подключенное к сети, контролируемой ПК «Efros ACS».

Администраторы ПК «Efros ACS» имеют доступ к веб-приложению ПК «Efros ACS». Предусмотрено разделение доступа администраторов ПК «Efros ACS» к функциональным возможностям ПК «Efros ACS» на три уровня:

- полный доступ – с правом внесения изменений в параметры работы ПК «Efros ACS»;
- только чтение – с правом просмотра параметров работы ПК «Efros ACS», без возможности внесения изменений;
- инициализации клиентских сертификатов – с правом доступа только к странице инициализации клиентских сертификатов сетевых пользователей ПК «Efros ACS».

Для разделения доступа администраторов ПК «Efros ACS» в ПК «Efros ACS» используются роли:

- 1) «ACS Администратор» – пользователи с полным доступом, имеют доступ к функциям:
 - управление настройками ПК «Efros ACS»;
 - мониторинг текущего состояния ПК «Efros ACS»;
 - ведение списка контролируемого АСО (устройств и групп устройств);
 - ведение списка контролируемого клиентского оборудования (конечных точек сети и их групп);
 - ведение списка пользователей (всех ролей) и групп пользователей;
 - настройка политик доступа пользователей к АСО;
 - управление экспортом и импортом данных.
- 2) «RO Администратор» – пользователи с правом просмотра указанных в пункте 1 данных (без возможности внесения изменений, доступно только ведение списка шаблонов отчетов).
- 3) «SER Администратор» – пользователи с правом инициализации клиентских сертификатов. Имеют доступ только к одной странице веб-приложения для инициализации клиентских сертификатов, не имеют доступа к другим функциональным возможностям ПК «Efros ACS» ни с правом редактирования, ни с правом просмотра.

Для администраторов АСО в ПК «Efros ACS» используется роль «Пользователь». Внесенный в список пользователей ПК «Efros ACS» администратор АСО, которому

назначена роль «Пользователь», не имеет доступа к приложению ПК «Efros ACS», но имеет доступ к назначенным ему в ПК «Efros ACS» сетевым устройствам.

Администраторы ПК «Efros ACS» и администраторы АСО аутентифицируются в ПК «Efros ACS» с помощью учетного имени пользователя (логина) и пароля их учетной записи в ПК «Efros ACS».

В зависимости от типа сетевого устройства и используемого им протокола, устройства аутентифицируются:

- АСО – по IP-адресу их учетной записи в ПК «Efros ACS»;
- клиентское оборудование: по MAC-адресу их учетной записи в ПК «Efros ACS» или, при использовании технологии EAP (протокол 802.1x), по учетной записи устройства во внешней системе: через LDAP, один из контроллеров домена, через сетевых пользователей (тип аутентификации настраивается при выборе источника данных в правилах аутентификации наборов политик (см. п. 3.10)).

 Пользователям с административными ролями «ACS Администратор» (далее – администратор ACS), «RO Администратор» (далее – администратор RO) и «CER Администратор» (далее – администратор CER) не могут быть назначены доступные устройства. Если пользователь должен иметь доступ к приложению ПК «Efros ACS» и к устройствам, то для такого пользователя должны быть созданы две учетные записи в ПК «Efros ACS» с ролями соответственно «ACS Администратор»/«RO Администратор»/«CER Администратор» и «Пользователь».

2 Условия выполнения ПК «Efros ACS»

Минимальный состав технических средств, который должна иметь электронно-вычислительная машина (ЭВМ)², для установки ПК «Efros ACS» (далее – сервер ПК):

- требования к производительности рассчитываются на основе данных, приведенных в таблице 1;
- сетевой адаптер: 1 Гбит Integrated Ethernet Card;
- минимальное разрешение экрана видеодисплея ЭВМ должно составлять 1280 x 1024 пикселей.

Таблица 1 – Рекомендуемые требования к производительности ЭВМ для установки сервера ПК

Размер контролируемой сети сервером ПК	Аппаратные требования				
	CPU	RAM	ROM ¹⁾	Рекомендованный объем дискового пространства ²⁾ для хранения данных на срок до	
				90 дней ³⁾ , Гбайт	180 дней ⁴⁾ , Гбайт
До 150 ОЗ	от 2 Ghz CPU, Cores: 4	16 GB	SAS 10K и выше	Не менее 150	Не менее 250
До 300 ОЗ	от 2 Ghz CPU, Cores: 4	16 GB	SAS 10K и выше	Не менее 250	Не менее 450
До 500 ОЗ	от 2 Ghz CPU, Cores: 8	16 GB	SAS 15K и выше	Не менее 450	Не менее 600
До 1000 ОЗ	от 2 Ghz CPU, Cores: 12	32 GB	SSD	Не менее 600	Не менее 1200
От 1000 ОЗ	Рассчитывается индивидуально. Необходимо обращение в техподдержку				
1) Для повышения отказоустойчивости функционирования решения в составе аппаратной платформы рекомендуется выделить системный раздел, рекомендуемый объем системного раздела не менее 200 Гбайт					
2) Для снижения вероятности потери данных рекомендуется организация RAID-массива в конфигурации RAID1 + 1 диск Hot Spare					
3) Объем дискового пространства рекомендован для хранения данных не менее 90 дней при указанной емкости контролируемой сети					
4) Объем дискового пространства рекомендован для хранения данных не менее 180 дней при указанной емкости контролируемой сети. При необходимости хранения больше чем 180 дней, рекомендуется использовать регулярную выгрузку на сторонние носители					

² Под ЭВМ понимается электронно-вычислительная машина, совместимая с архитектурой Intel x86 (x86_64)

Для функционирования используемых протоколов необходимо наличие следующих открытых портов:

- для TACACS+ – порт 49/TCP;
- для RADIUS – порты 1812/UDP, 1813/UDP;
- для создания кластеров (функция отказоустойчивости) – порты 5405/UDP, 2224/TCP, 3121/TCP;
- для веб-интерфейса – порт 443/TCP;
- для двухуровневой иерархии серверов – порт 8081/TCP;
- для взаимодействия со службой контейнеризации – 2376/TCP.

Данные ПК «Efros ACS» должны храниться во внешней СУБД. В качестве внешней СУБД поддерживаются PostgreSQL 10.2 и выше, и «Защищенная система управления базами данных «Jatoba». Допускается установка СУБД локально на сервере ПК «Efros ACS». В случае обеспечения отказоустойчивости, СУБД должна размещаться на отдельном сервере относительно программного комплекса.

Установка серверной части ПК «Efros ACS» должна осуществляться на компьютеры, функционирующие под управлением операционной системы Astra Linux Special Edition, сертификат соответствия № 2557 (выдан ФСТЭК России 27 января 2012 г.).

Прикладное ПО, используемое в установке серверной части ПК «Efros ACS» – Docker-compose 1.28.2.

Веб-интерфейс программного комплекса должен поддерживать работу с браузерами, которые работают на основе проекта с открытым кодом Chromium, а также с браузером Mozilla Firefox начиная с версии 99.0.1 и выше.

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

3 Выполнение ПК «Efros ACS»

3.1 Запуск веб-приложения ПК «Efros ACS»

3.1.1. Запуск веб-приложения ПК «Efros ACS» и аутентификация пользователя

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

- 1) Запустить веб-браузер.
- 2) Ввести в адресной строке открывшегося окна сетевой адрес приложения. Сетевой адрес приложения пользователю должен сообщить администратор ACS, обслуживающий ПК «Efros ACS».
- 3) Нажать клавишу клавиатуры ENTER. На экране монитора откроется страница авторизации пользователя, приведенная на рис. 1.

EFROS ACCESS CONTROL SERVER

Добро пожаловать
войдите, чтобы продолжить

Логин ?
domain\login

Пароль ?
Введите пароль

Войти

2021 © ООО «Газинформсервис»
Версия: 2.1.3.10 - 09.03.21 16:21



Рисунок 1 – Страница авторизации пользователя

- 4) Ввести в поле «Логин»:
 - для локального пользователя – имя учетной записи пользователя (далее – логин);
 - для доменного пользователя – данные доменной учетной записи в формате <доменное имя>\<логин>, где «доменное имя» – наименование сервера LDAP, с учетной записью которого связан пользователь ПК «Efros ACS».
- 5) Ввести в поле «Пароль» пароль пользователя.

6) Нажать кнопку «Войти».

При возникновении ошибки в ходе авторизации в верхней части страницы отобразится сообщение об ошибке. Полный перечень ошибок приведен в разделе 4.

В случае успешной авторизации:

- для администратора ACS или RO откроется страница раздела «Мониторинг» в соответствии с рис. 2;
- для администратора CER откроется страница «Инициализация сертификата» в соответствии с рис. 3.

В этом случае пользователю необходимо нажать кнопку «ОК» и либо завершить работу с ПК «Efros ACS», закрыв соответствующую вкладку веб-браузера, либо выполнить повторный запуск веб-интерфейса ПК «Efros ACS».

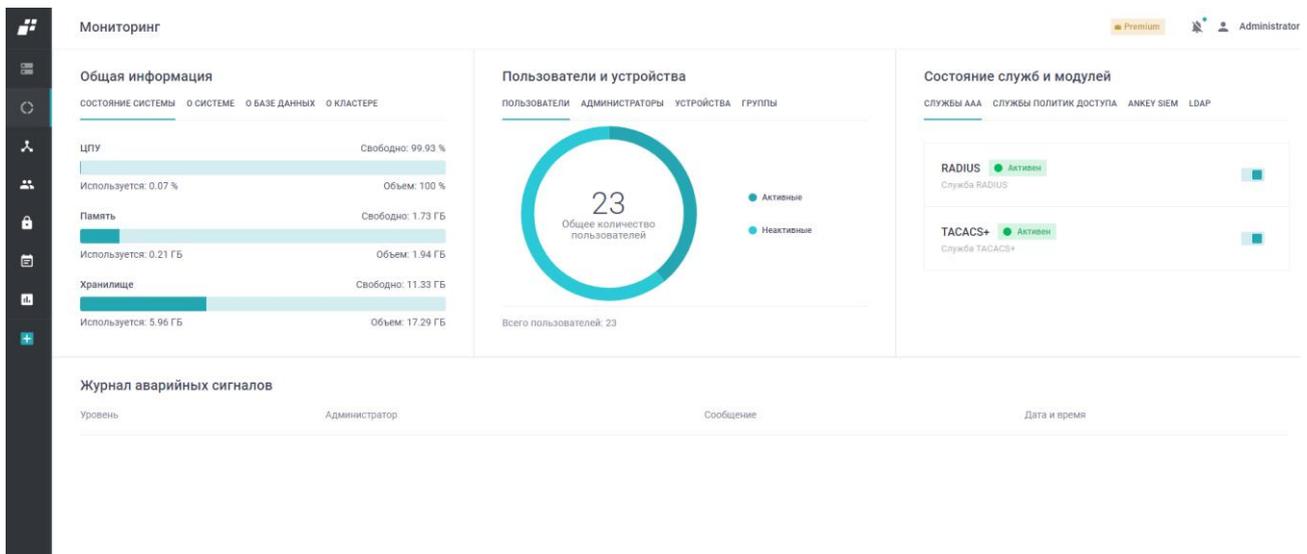


Рисунок 1 – Рисунок 2 – Страница «Мониторинг» после успешной авторизации администратора ACS или RO

The screenshot shows a web form titled "Инициализация сертификата" (Certificate Initialization). It contains four input fields and a button:

- общее имя (CN) ?**: A text input field with the placeholder "Введите общее имя" (Enter common name) and a red error message "Обязательное поле" (Required field). The character count is 0/50.
- Альтернативное имя (SAN) ?**: A dropdown menu with the placeholder "Выберите тип" (Select type) and a plus sign icon. The character count is 0/50.
- Шаблон ?**: A dropdown menu with the placeholder "Выберите шаблон" (Select template).
- Формат загрузки ?**: A dropdown menu with the placeholder "Выберите формат загрузки" (Select upload format).

At the bottom of the form is a button labeled "СГЕНЕРИРОВАТЬ" (GENERATE).

Рисунок 2 – Рисунок 3 – Страница «Инициализация сертификата» после успешной авторизации администратора CER

3.1.2. Смена пароля

После установки и настройки ПК «Efros ACS» в БД ПК «Efros ACS» автоматически создается учетная запись пользователя с ролью «ACS Администратор»: с логином «administrator» и паролем «\$Qwerty123456\$» (далее – предустановленный администратор ACS). Учетные записи других пользователей ПК «Efros ACS» создаются пользователем под учетной записью предустановленного администратора ACS и других администраторов ACS.

При первом запуске ПК «Efros ACS» для любого пользователя открывается окно смены пароля (рис. 4), в котором необходимо указать в качестве старого пароля значение «\$Qwerty123456\$» (для предустановленного администратора ACS) или пароль, присвоенный учетной записи пользователя при ее создании (пароль пользователю должен сообщить администратор ACS), дважды указать новый пароль и нажать кнопку «Изменить».

Изменение пароля

Текущий пароль

Новый пароль

Подтверждение пароля

Рисунок 3 – Рисунок 4 – Окно смены пароля

Будет выполнена автоматическая проверка соответствия пароля заданной в ПК «Efros ACS» сложности пароля, по умолчанию пароль должен:

- быть не менее 6 символов;
- содержать хотя бы одну цифру;
- содержать хотя бы одну латинскую букву верхнего регистра;
- содержать хотя бы одну латинскую букву нижнего регистра;
- не совпадать с предыдущими тремя паролями пользователя.

Допустимые символы в пароле: латинские буквы обоих регистров, цифры, не буквенно-цифровые символы (! @ # & () - _ [{ }] : ; ' , ? / * ~ \$ ^ + = < >).

При возникновении ошибки в ходе смены пароля в верхней части страницы авторизации отобразится соответствующее сообщение об ошибке.

После успешной смены пароля вновь откроется страница авторизации пользователя и администратору для доступа к веб-приложению ПК «Efros ACS» необходимо выполнить запуск ПК «Efros ACS» с новым паролем³.

Кроме того, если в ПК «Efros ACS» при настройке парольной политики заданы временные ограничения действия паролей, то по истечении времени действия пароля

³ После входа администратора с новым паролем откроется страница «Лицензирование» раздела «Настройки системы», необходимо выполнить активацию комплекса в соответствии с документом «ПК «Efros ACS». Руководство администратора»

при попытке авторизации любому администратору ПК также будет выведено окно смены пароля и пользователю необходимо выполнить аналогичные действия по смене пароля. Пароль при этом должен соответствовать текущим настройкам парольной политики ПК «Efros ACS».

Смена пароля может быть выполнена также пользователем в любой момент времени при работе с ПК «Efros ACS». Окно смены пароля открывается при нажатии кнопки «Изменить» на странице просмотра данных текущего пользователя (см. п. 3.1.3). Новый пароль должен соответствовать текущим настройкам парольной политики ПК «Efros ACS».

3.1.3. Настройка аккаунта администратора ACS или RO

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

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

1) Заголовок страницы, содержащий:

- логотип (пиктограмму) ПК «Efros ACS»;
- название страницы (название раздела приложения);
- пиктограмму с типом лицензии ПК «Efros ACS» (Premium или Standard);
- кнопку «Уведомления» (🔔), по нажатию которой раскрывается список уведомлений (подробнее см. п. 3.1.4);
- кнопку «Аккаунт» (<логин пользователя>), по нажатию которой открывается меню, содержащее (рис. 5):
 - а) логин текущего пользователя;
 - б) блок «Оформление» – для выбора цветового решения интерфейса приложения (тема), используемого текущим пользователем. Выбор осуществляется установкой переключателя. Выбранная тема применяется сразу без перезапуска приложения;

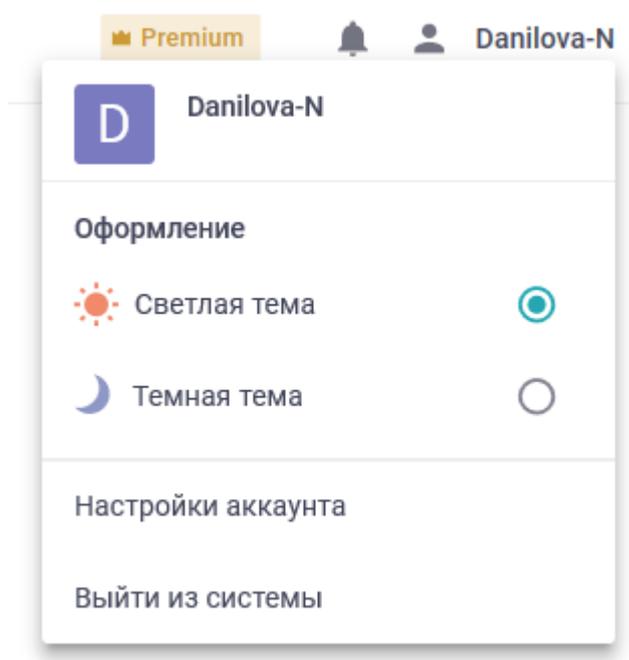


Рисунок 4 – Рисунок 5 – Меню «Аккаунт»

в) пункт «Настройки аккаунта», при выборе которого открывается страница (рис. 6) для просмотра данных текущего пользователя, используемой версии ПК «Efros ACS», для перехода в окно смены пароля пользователя, а также для настройки используемой пользователем темы, языка приложения и включения/отключения режима получения уведомлений. Выбор параметров настройки осуществляется установкой переключателя. Выбранные параметры применяются сразу без перезапуска приложения;

i По умолчанию в веб-приложении используется язык, выбранный в серверной части ПК. Смена используемого языка в веб-приложении не влияет на серверную часть.

г) пункт «Выйти из системы», при выборе которого завершается работа пользователя с приложением и открывается страница авторизации пользователя (см. рис. 1).

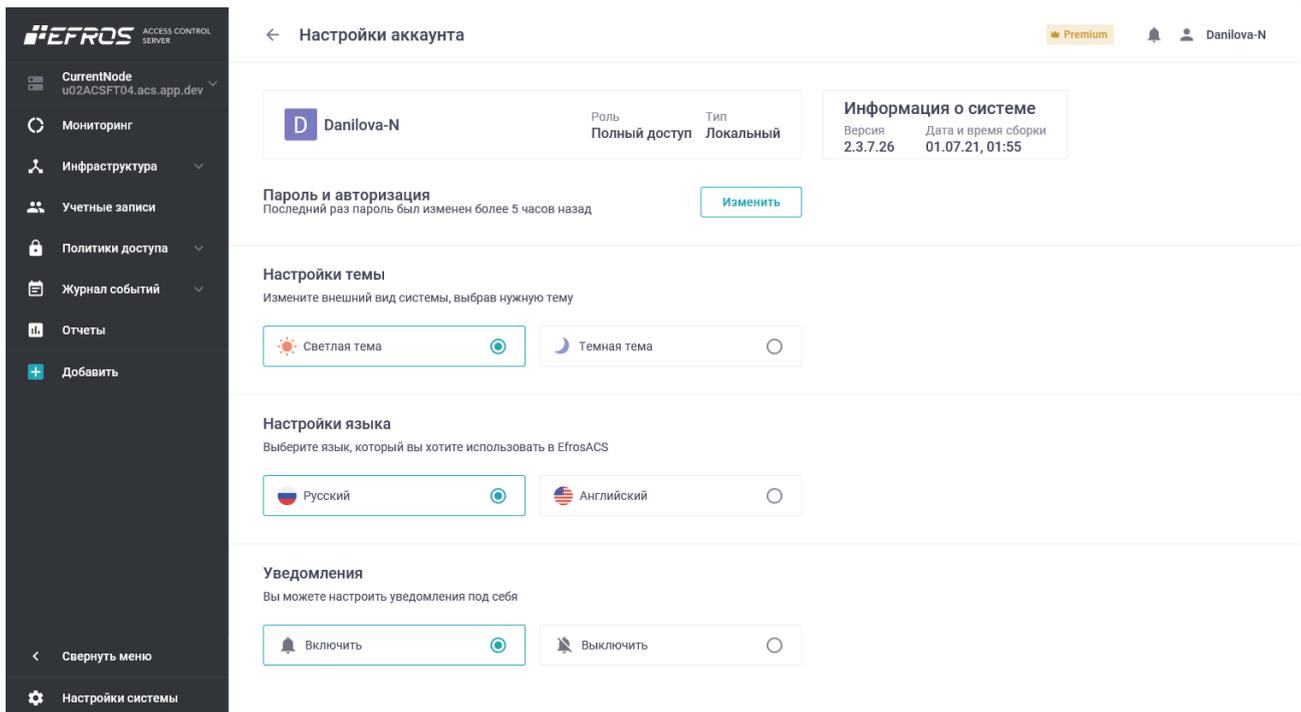


Рисунок 5 – Рисунок 6 – Страница просмотра данных текущего пользователя

2) Панель главного меню. Содержит:

- поле со списком доступных пользователю серверов (главный и все доступные подчиненные). Пользователь имеет возможность выбрать в списке требуемый сервер для перехода к просмотру или настройке параметров работы выбранного сервера (в зависимости от прав пользователя, назначенных ему на соответствующем сервере)⁴;
- ссылки на разделы: «Мониторинг», «Инфраструктура», «Учетные записи», «Политики доступа», «Журнал событий», «Отчеты»;
- ссылку «Добавить» (только для администраторов ACS), по нажатию которой раскрывается меню выбора категории «Инфраструктура», «Учетные записи» или «Политики доступа» и добавляемого элемента выбранной категории в соответствии с рис. 7;
- строку управления отображением панели главного меню. В развернутом состоянии панели строка имеет вид в соответствии с рис. 7, в свернутом – «>». Панель в развернутом состоянии содержит пиктограммы (иконки) и текст ссылок, в свернутом – только пиктограммы. Выбор пиктограммы

⁴ Настройка иерархии серверов и управление подчиненными серверами доступны только для лицензии ПК «Efros ACS» типа Premium

позволяет перейти на страницу соответствующего раздела или раскрыть меню выбора добавляемого элемента без разворачивания панели главного меню;

— ссылку на раздел «Настройки системы».

- 3) Рабочая область страницы – содержит блоки с данными выбранного раздела/подраздела приложения.

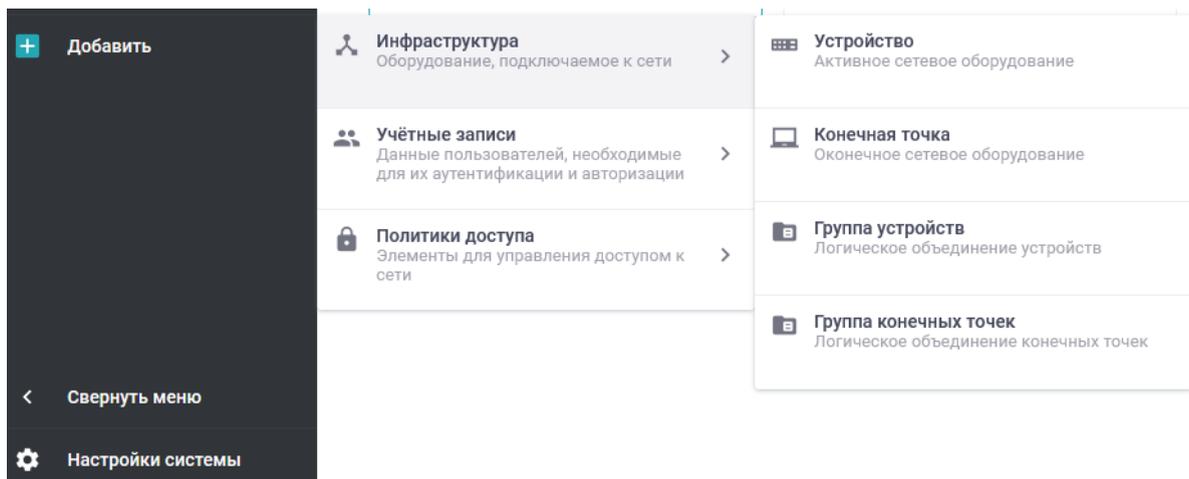


Рисунок 6 – Рисунок 7 – Меню выбора добавляемой сущности

Если в течение 30 минут пользователь будет неактивен в ПК «Efros ACS», то есть не будет взаимодействовать с веб-интерфейсом ПК «Efros ACS», то сессия пользователя будет заблокирована до его повторной авторизации, на экране откроется окно в соответствии с рис. 8.

В этом случае пользователю необходимо нажать кнопку «ОК» и либо завершить работу с ПК «Efros ACS», закрыв соответствующую вкладку веб-браузера, либо выполнить повторный запуск веб-интерфейса ПК «Efros ACS».

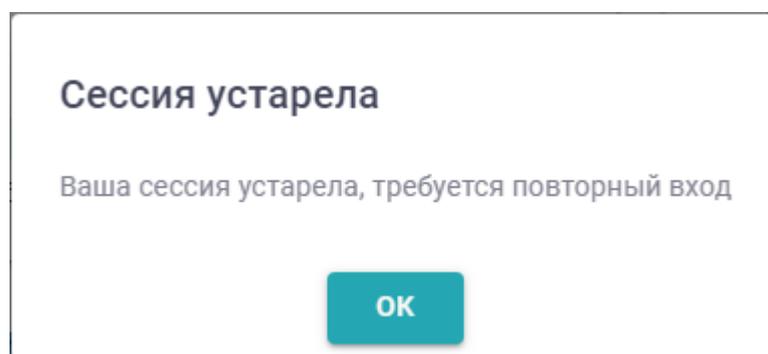


Рисунок 7 – Рисунок 8 – Окно перехода к повторной аутентификации в ПК «Efros ACS»

3.1.4. Просмотр уведомлений администраторами ACS и RO

В ПК «Efros ACS» реализована функциональная возможность автоматической рассылки уведомлений администраторам ACS и RO о следующих событиях, зарегистрированных в системном журнале ПК «Efros ACS»: о запуске/остановке системных служб RADIUS и TACACS+, о запуске/остановке и синхронизации модуля Active Directory, о проверке config-файла TACACS+ и перезапуск службы, которые происходят при создании, редактировании и удалении сущностей (устройств, пользователей, групп устройств, групп пользователей, политик доступа).

При фиксации события:

- запись о событии заносится в соответствующий системный журнал ПК «Efros ACS»;
- в правом верхнем углу экрана открывается всплывающее окно с текстом уведомления (рис. 9). Окно закрывается автоматически по истечении 15 секунд либо вручную пользователем по нажатию кнопки «Закрыть» (X).

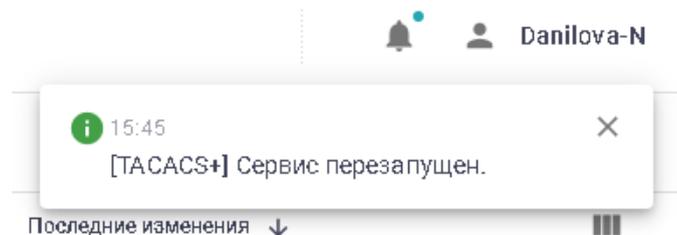


Рисунок 8 – Рисунок 9 – Окно с текстом уведомления

- в правом углу кнопки «Уведомления» (🔔) отображается пиктограмма непрочитанных уведомлений (●).

Последние 22 уведомления доступны для просмотра в окне уведомлений (рис. 10), которое открывается по нажатию кнопки «Уведомления» (🔔) в заголовке страницы.

По умолчанию в окне отображаются уведомления типов «Информационные» и «Ошибки» (в заголовке окна выбран фильтр «Все»). Уведомления отсортированы по убыванию даты и времени их получения и сгруппированы по дням фиксирования событий. Голубым фоном выделены уведомления, для которых не проставлен признак «Прочитано».

При наведении курсора на строку уведомления в строке отображаются кнопки:

- «✓» – для простановки отметки о прочтении уведомления;
- «🗑️» – для удаления уведомления из списка окна уведомлений.

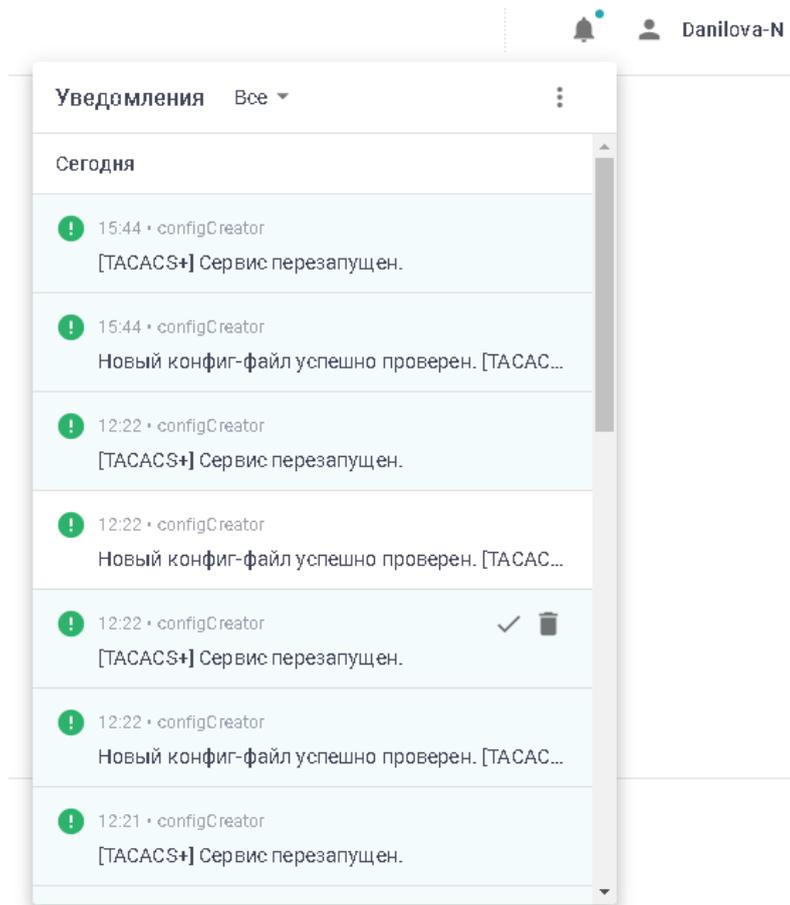


Рисунок 9 – Рисунок 10 – Окно просмотра уведомлений

Пользователь имеет возможность:

- 1) Отфильтровать список уведомлений по их типу, для чего – выбрать в заголовке окна вместо фильтра «Все» требуемый фильтр «Информационные» или «Ошибки».
 - 2) Отключить всплывающие окна уведомлений, для чего – перейти на страницу настройки аккаунта (см. рис. 10) и установить переключатель «Уведомления» в положение «Выключить» либо раскрыть меню окна уведомлений, нажав кнопку «⋮» (рис. 11), и выбрать пункт «Выключить уведомления».
- i** В режиме отключенных уведомлений всплывающие окна не отображаются, кнопка «Уведомления» (🔔) изменяет свой вид на (🔕), при этом признак непрочитанных уведомлений (при их наличии) отображается и уведомления доступны пользователю для просмотра в окне уведомлений.

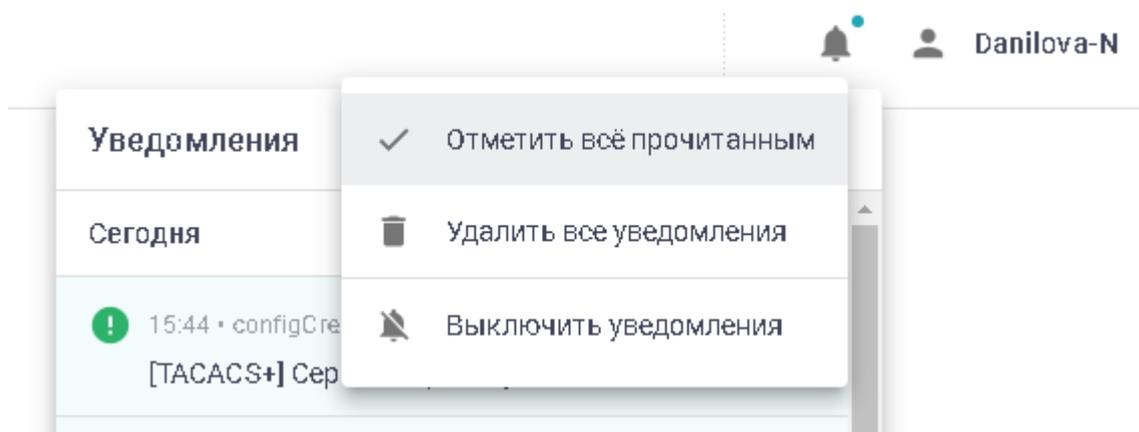


Рисунок 10 – Рисунок 11 – Меню окна просмотра уведомлений

Кроме того, пользователь имеет возможность групповых операций со списком уведомлений:

- проставить признак «Прочтено» для всех непрочтенных сообщений в окне, выбрав пункт меню «Отметить все прочитанным»;
- очистить список уведомлений в окне просмотра уведомлений, выбрав пункт меню «Удалить все уведомления».

3.1.5. Выбор настраиваемого сервера (при наличии подчиненных серверов)

В ПК «Efros ACS» с лицензией Premium доступна функциональная возможность ведения списка серверов, подчиненных главному серверу. Уровень доступа к каждому серверу назначается пользователям отдельно. Так пользователь, имеющий права администратора RO на главном сервере может иметь полные права администратора ACS на подчиненном сервере.

Для перехода к настройке или просмотру параметров подчиненного сервера пользователю необходимо после запуска веб-приложения ПК «Efros ACS» выбрать в панели главного меню в списке доступных серверов наименование требуемого сервера. На рисунке 12 в списке отображаются наименования главного сервера «CurrentNode» и подчиненного сервера «test_153». В текущий момент времени активным является главный сервер.

При переходе на подчиненный сервер управляющие элементы меню и страниц ПК «Efros ACS» будут доступны или не доступны в зависимости от прав пользователя на соответствующем сервере. Подраздел «Управление подчиненными серверами» раздела «Настройки системы» (см. п. 3.4.8) будет недоступен.

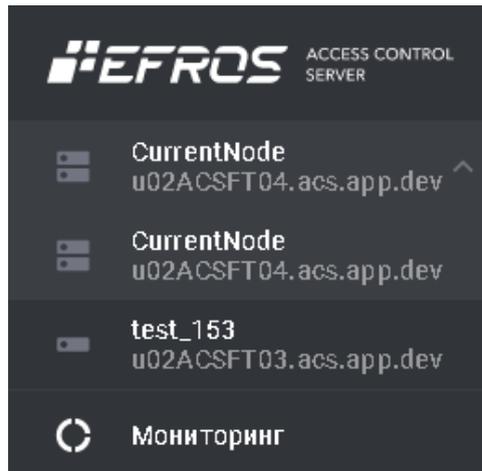


Рисунок 11 – Рисунок 12 – Список доступных пользователю серверов

3.2 Работа со списками сущностей ПК «Efros ACS». Общие сведения

Списки сущностей ПК «Efros ACS» (устройств, пользователей, администраторов и групп устройств и пользователей), а также политик безопасности, отображающиеся в рабочей области, выполнены в виде таблиц.

На рис. 13 приведена страница «Инфраструктура». Сетевое оборудование» с вкладкой «Устройства» для администраторов RO, все данные доступны только для просмотра. На рис. 14 приведена та же страница для администраторов ACS, данные доступны для редактирования.

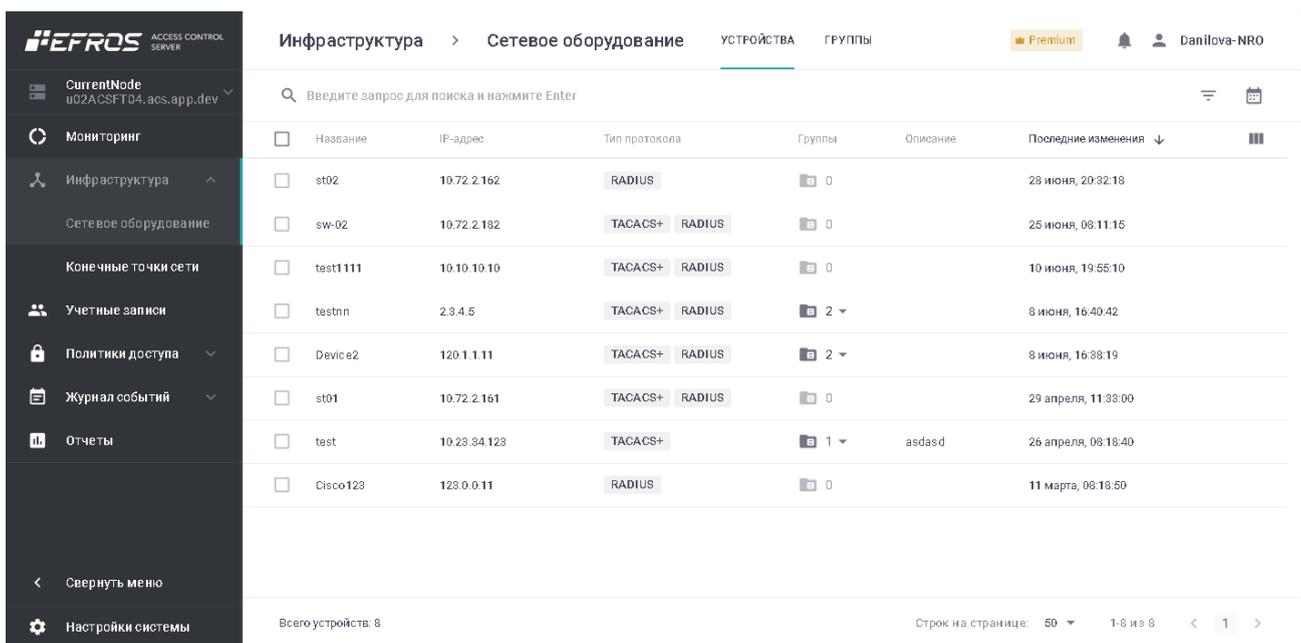


Рисунок 12 – Рисунок 13 – Страница списка АСО для администратора RO

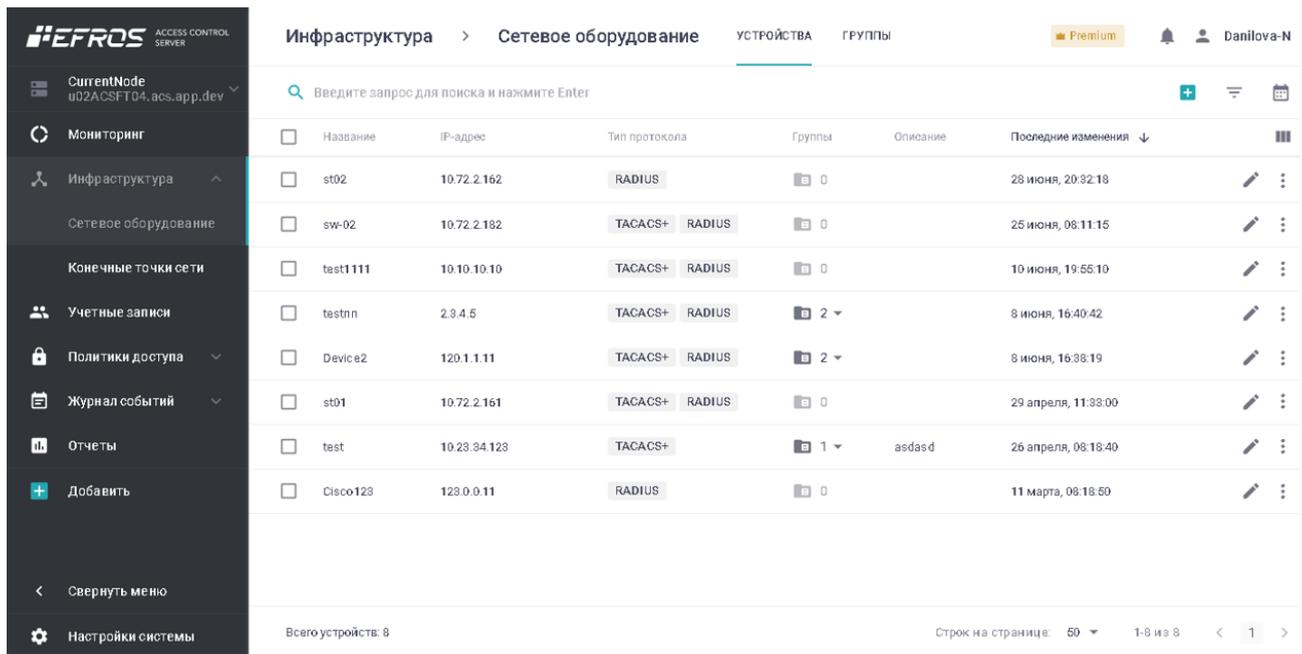


Рисунок 13 – Рисунок 14 – Страница списка АСО для администратора ACS

Над таблицами в зависимости от типа сущности могут быть доступны:

- поле поиска (🔍 Введите запрос для поиска и нажмите Enter) – для ввода последовательности символов из искомой записи. Процесс поиска запускается после ввода символов нажатием клавиши ENTER клавиатуры;
- кнопка «Добавить» (+) – для перехода на страницу добавления записи в список (доступна только администраторам ACS);
- кнопка «Добавить фильтр» (≡) – для перехода в окно фильтрации;
- кнопка «Выбрать период» (📅) – для перехода в окно выбора периода внесения последних изменений в данные сущностей.

📘 В полноэкранном режиме работы с веб-браузером справа от кнопок отображается их наименование. При уменьшении окна веб-браузера отображаются только пиктограммы кнопок, наименования кнопок отображаются во всплывающих подсказках при наведении курсора на кнопки.

Таблицы, кроме столбцов с данными сущностей содержат столбец с полями для флага. Для администраторов RO поля неактивны, для администраторов ACS – доступны для установки флага.

После установки флага в одном поле над таблицей в соответствии с рис. 15 отображается строка выбора операции, выполняемой с одной записью таблицы.

Пользователь имеет возможность:

- в списках устройств и пользователей – создать копию сущности, добавить сущность в группу сущностей, удалить выбранную сущность;
- в списках групп устройств, пользователей и политик доступа – создать копию сущности, удалить выбранную сущность.

Выбрано строк: 1  Создать копию  Добавить в группу  Удалить 

Рисунок 14 – Рисунок 15 – Строка выбора операции, выполняемой с одной записью таблицы

После установки флага в двух и более полях или в поле для флага в заголовке над таблицей в соответствии с рис. 16 отображается строка выбора операции, выполняемой с несколькими записями таблицы. Пользователь имеет возможность:

- в списках устройств и пользователей – создать группу сущностей, добавить выбранные сущности в группу сущностей, удалить выбранные сущности;
- в списках групп устройств, пользователей и политик доступа – удалить выбранные сущности.

Выбрано строк: 2  Создать группу  Добавить в группу  Удалить 

Рисунок 15 – Рисунок 16 – Строка выбора операции, выполняемой с несколькими записями таблицы

Для администраторов ACS таблицы дополнительно содержат столбец с кнопками выбора действия, например:

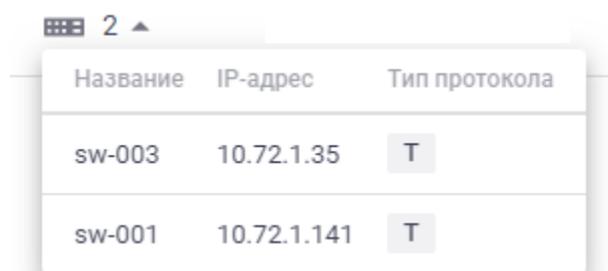
- «Изменить» () – для перехода на страницу редактирования записи списка;
- «Меню» () – для раскрытия меню с пунктами:
 - а) «Добавить в группу» () – при выборе меню открывается окно выбора группы, в которую добавляется пользователь;
 - б) «Создать копию» () – при выборе меню открывается страница создания нового пользователя, поля которой заполнены данными пользователя из соответствующей кнопке записи (см. п.п. 3.9.4.3);
 - в) «Удалить» () – для удаления соответствующей записи списка.

Значения в столбцах, которые содержат количественные характеристики сущности (например, количество устройств, включенных в группу « 2 ▾», или количество

наборов команд, назначенных пользователю («<> 1 ▼»), являются ссылкой, при выборе которой раскрывается соответственно список с данными устройств (рис. 17), список наборов команд (рис. 18).

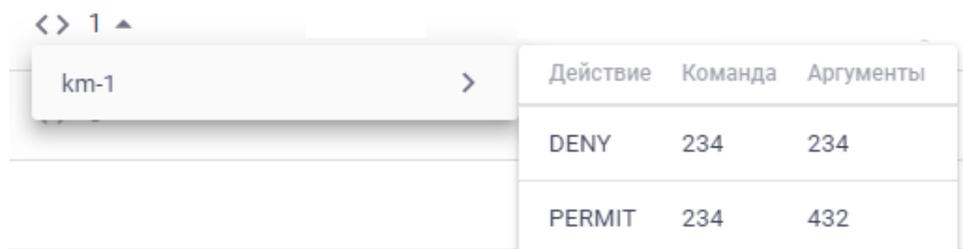
При выборе:

- наименования устройства – открывается страница просмотра/ редактирования (в зависимости от роли пользователя) параметров устройства;
- наименования набора команд – открывается окно просмотра данных выбранного набора команд (см. рис. 18).



Название	IP-адрес	Тип протокола
sw-003	10.72.1.35	T
sw-001	10.72.1.141	T

Рисунок 16 – Рисунок 17 – Окно с данными устройств



Действие	Команда	Аргументы
DENY	234	234
PERMIT	234	432

Рисунок 17 – Рисунок 18 – Список наборов команд с окном просмотра данных команд одного из наборов команд

В заголовке таблицы дополнительно расположена кнопка (☰) для перехода в окно выбора отображаемых в таблице столбцов.

На одной странице таблицы по умолчанию содержится 50 записей. В нижней части таблицы располагается строка настройки, содержащая:

- информационное поле с общим количеством записей списка;
- поле выбора количества отображаемых на странице строк таблицы. По умолчанию установлено значение «50». Пользователь имеет возможность выбрать другие значения – «10» или «25»;

- информационное поле с данными о номере по порядку просматриваемых в текущий момент времени записей таблицы и общем количестве записей таблицы (**1-9** из 9);
- группу кнопок навигации по страницам таблицы (< **1** >).

3.2.1. Выбор сортировки записей таблиц

По умолчанию записи списков сущностей отсортированы в порядке убывания даты и времени внесения последних изменений в данные сущности, записи списка политик доступа – в алфавитном порядке по наименованию.

Пользователь имеет возможность задать другой тип сортировки, выбрав заголовок требуемого столбца таблицы. В заголовке отобразится знак «↓», сортировка всех строк таблицы будет выполнена по убыванию значений выбранного столбца. Для изменения направления сортировки необходимо повторно выбрать заголовок столбца. В заголовке отобразится знак «↑».

3.2.2. Поиск данных в таблицах списков сущностей

Для поиска в таблице сущностей требуемых записей необходимо ввести в поле поиска последовательность символов из данных искомой записи списка и нажать клавишу клавиатуры ENTER. После чего:

- в таблице отобразятся записи сущностей, в данных которых содержатся введенные символы;
- слева над таблицей в соответствии с рис. 19 отобразится поле «Поиск» с заданной искомой последовательностью символов.

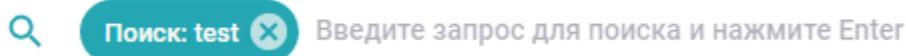


Рисунок 18 – Рисунок 19 – Поле «Ключевое слово»

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

3.2.3. Выбор периода внесения последних изменений в данные сущности

Для фильтрации списка сущностей по периоду внесения последних изменений в их данные необходимо нажать кнопку «Выбрать период» (). Откроется окно выбора периода, приведенное на рис. 20. Состав элементов окна и правила их заполнения приведены в таблице 2.

The screenshot displays a date selection interface. On the left, a vertical sidebar contains the following options: "Сегодня" (Today), "Вчера" (Yesterday), "Последние 7 дней" (Last 7 days), "Последние 14 дней" (Last 14 days), "Текущий месяц" (Current month), "Последние 30 дней" (Last 30 days), and "Прошлый месяц" (Last month). The main area shows a calendar for March 2021, with the date 11th highlighted. Navigation arrows and month/year labels are visible. At the bottom, there are three buttons: "Сбросить" (Reset), "Отменить" (Cancel), and "Применить" (Apply).

Рисунок 19 – Рисунок 20 – Окно выбора периода

Таблица 2 – Состав и описание элементов окна выбора периода

Элемент	Описание
Панель быстрого выбора периода	Содержит предустановленные варианты периодов времени. По умолчанию выбрано значение «Сегодня» и в таблице отображаются записи, в данные которых были внесены изменения в течение текущего дня
Панель календаря	Содержит в заголовке выбранные начальную и конечную даты периода и два блока выбора начальной и конечной дат периода времени. По умолчанию в качестве начальной и конечной дат периода выбрана текущая дата, в блоках отображаются календари на текущий и следующий месяцы
Кнопки управления	
Сбросить	По нажатию кнопки значения панелей окна выбора периода устанавливаются в положение по умолчанию
Отменить	По нажатию кнопки окно закрывается без применения введенных настроек
Применить	По нажатию кнопки окно закрывается, введенные настройки выбора периода применяются

Далее необходимо выбрать в панели быстрого выбора периода требуемый предустановленный период времени либо задать в панели календаря требуемые начальную и конечную даты периода и нажать кнопку «Применить».

После чего:

- окно выбора периода закроется;
- в таблице отобразятся записи, в данные которых были внесены изменения в заданный период времени;
- слева над таблицей в соответствии с рис. 21 отобразится поле с заданным периодом времени.

Если в окне выбора периода заданы:

- обе даты – в таблице отобразятся записи, в которые были внесены изменения в указанный период, включая начальную и конечную даты;
- только дата начала периода – в таблице отобразятся записи, в которые были внесены изменения в период, начиная с указанной даты и по текущую дату;
- только дата окончания периода – в таблице отобразятся записи, в которые были внесены изменения в период, начиная с самой ранней из имеющихся в таблице дат внесения изменений и по указанную дату.



Рисунок 20 – Рисунок 21 – Поле с заданным периодом времени

Для отмены заданных правил фильтрации и отображения в таблице всех записей с внесенными изменениями за текущие сутки необходимо нажать в поле кнопку «Очистить» (🗑️) либо раскрыть окно выбора периода и нажать последовательно кнопки «Сбросить» и «Применить».

3.2.4. Фильтрация данных в таблицах сущностей

Для фильтрации данных в таблицах сущностей необходимо нажать кнопку «Добавить фильтр» (🔍). Откроется окно фильтрации. Состав полей окна для разных разделов ПК «Efros ACS» отличается. На рис. 22 приведен пример окна фильтрации списка АСО.

Для задания правил фильтрации необходимо:

- выбрать нажатием кнопок и путем ввода параметров в полях окна параметры фильтрации;
- нажать кнопку «Применить».

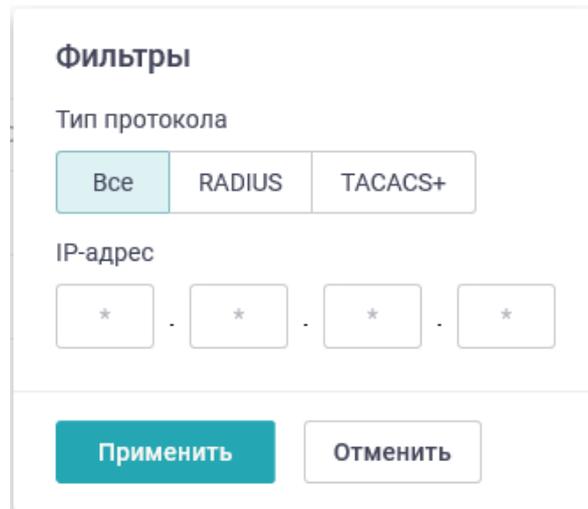


Рисунок 21 – Рисунок 22 – Окно фильтрации списка АСО

После чего:

- окно фильтрации закроется;
- в таблице сущностей отобразятся записи, соответствующие заданным параметрам фильтрации;
- слева над таблицей в соответствии с рис. 23 отобразятся поля с заданными параметрам фильтрации.

Для отмены заданных правил фильтрации и отображения в таблице всех записей необходимо нажать кнопку «Очистить» (🗑️) в каждом поле отдельно.



Рисунок 22 – Рисунок 23 – Отображение параметров фильтрации записей списка

3.2.5. Настройка состава отображаемых столбцов в таблицах списков сущностей

Для настройки состава отображаемых столбцов в таблицах сущностей необходимо нажать кнопку «Колонки» (☰). Откроется окно выбора столбцов таблицы. На рис. 24 приведено такое окно для списка устройств.

В окне отображаются строки с наименованиями всех столбцов таблицы. Им соответствуют поля для флага. Наличие в поле флага означает, что столбец выбран для отображения в таблице.

Для настройки состава отображаемых в таблице столбцов необходимо установить/отменить установку флагов. Состав столбцов изменяется по мере установки/отмены флагов.

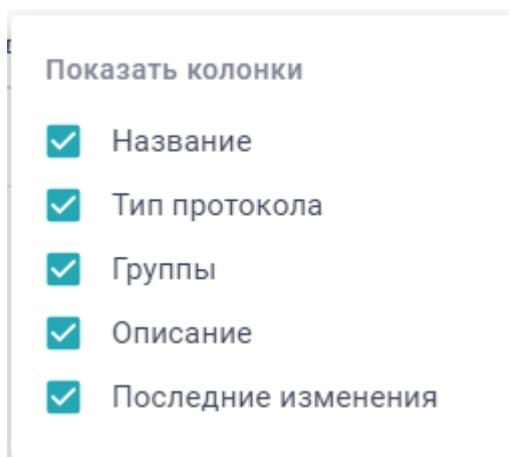


Рисунок 23 – Рисунок 24 – Окно выбора столбцов таблицы

3.2.6. Удаление сущностей

Удаление сущностей выполняется администратором ACS вручную средствами веб-приложения ПК «Efros ACS». Для удаления доступны только те записи списков ПК «Efros ACS», которые не использованы в карточках других сущностей ПК «Efros ACS». При попытке удаления таких сущностей, удаление выполнено не будет, отобразится соответствующее сообщение.

Удаление одной сущности из списка может быть выполнено двумя способами:

1) Способ 1:

- нажать в строке удаляемой записи кнопку «Удалить» (🗑️) либо нажать кнопку «Меню» (☰) и выбрать в раскрывшемся меню пункт «Удалить» (🗑️);
- нажать в открывшемся окне подтверждения кнопку «ОК».

2) Способ 2:

- установить флаг в строке удаляемой записи;
- нажать в строке операций над таблицей сущностей (см. рис. 14) кнопку «Удалить» (🗑️);
- нажать в открывшемся окне подтверждения кнопку «ОК».

В результате будет запущен процесс удаления сущности.

Для удаления нескольких сущностей из списка необходимо:

- 1) Установить флаг в полях крайней левой графы, соответствующих удаляемым записям. Для выбора всех записей на активной странице – установить флаг в заголовке таблицы. В верхней части таблицы отобразится строка выбора операций (см. рис. 15).
- 2) Нажать в строке кнопку «Удалить» (🗑️).

- 3) Нажать в открывшемся окне подтверждения кнопку «ОК». Будет запущен процесс удаления выбранных сущностей.

Примечание. Для удаления сущностей, записи которых расположены на другой странице списка, необходимо перейти на требуемую страницу и повторить действия перечислений 1 – 3.

После успешного завершения процесса удаления:

- сущности удаляются из списка сущностей;
- в журнал событий ПК «Efros ACS» для каждой удаленной сущности вносится сообщение типа «Инфо» в формате: «Администратор {имя_выполняющего_операцию_администратора}: Сущность {название_сущности} успешно удалена».

В случае возникновения ошибки в процессе удаления:

- сущности удаляются из списка сущностей;
- в журнал событий ПК «Efros ACS» для каждой такой сущности вносится сообщение типа «Ошибка» в формате: «Администратор {имя_выполняющего_операцию_администратора}: Ошибка удаления сущности {название_сущности} - {текст_ошибки}».

3.3 Мониторинг текущего состояния ПК «Efros ACS»

После успешной авторизации администратора ACS или RO в приложении ПК «Efros ACS» открывается страница раздела «Мониторинг», приведенная на рис. 2. Состав и описание элементов панелей страницы приведены в таблице 3.

-  При работе в других разделах приложения для перехода на страницу «Мониторинг» пользователю необходимо выбрать в главном меню ссылку «Мониторинг» и, если панель меню свернута – пиктограмму «».

Пользователь имеет возможность, перемещаясь по вкладкам панелей, просмотреть требуемые данные о работе ПК «Efros ACS».

Таблица 3 – Состав и описание панелей страницы «Мониторинг»

Элемент	Описание
Панель «Общая информация»	
Вкладка «Состояние системы»	Содержит информацию о: <ul style="list-style-type: none">— загрузке центрального процессорного устройства (ЦПУ);— количестве занятого и свободного объема оперативного запоминающего устройства (ОЗУ);

Элемент	Описание
	— количестве занятого и свободного объема БД ПК «Efros ACS»
Вкладка «О системе»	Содержит справочную информацию о ПК «Efros ACS»: название, сетевой адрес, хост и дата и время последнего обновления
Вкладка «О базе данных»	Содержит информацию о БД ПК «Efros ACS»: <ul style="list-style-type: none">— текущее состояние;— время безотказной работы;— версия БД;— максимально допустимое количество подключений;— количество открытых подключений
Вкладка «О кластере»	Содержит информацию о кластере: <ul style="list-style-type: none">— IP-адрес кластера;— доменное имя;— текущее состояние;— узлы кластера;— состояние кластера
Панель «Пользователи и устройства»	
Вкладка «Пользователи»	Содержит информацию в виде диаграммы об общем количестве пользователей с ролью «Пользователь», внесенных в список пользователей ПК «Efros ACS», а также о количестве активных и неактивных пользователей
Вкладка «Администраторы»	Содержит информацию в виде диаграммы об общем количестве пользователей с ролями «ACS Администратор» и «RO Администратор», внесенных в список администраторов ПК «Efros ACS», а также о количестве активных и неактивных администраторов
Вкладка «Устройства»	Содержит информацию в виде диаграммы об общем количестве зарегистрированных в ПК «Efros ACS» устройств, а также отдельно о количестве устройств, работающих по протоколу TACACS+, RADIUS, по обоим протоколам, и о количестве клиентского оборудования (конечные точки сети)
Вкладка «Группы»	Содержит информацию в виде диаграммы о количестве групп АСО, пользователей и групп конечных точек сети отдельно и об общем количестве групп в ПК «Efros ACS»
Панель «Состояние служб и модулей»	

Элемент	Описание
Вкладка «Службы AAA»	Содержит информацию о состоянии служб протоколов ПК «Efros ACS»: название службы; состояние службы (активен, неактивен). Для каждой службы доступна кнопка запуска () /остановки () службы  Отключение служб протоколов в режиме отказоустойчивости недоступно
Вкладка «Службы политик доступа»	Содержит информацию о состоянии служб обработки политик доступа для протоколов ПК «Efros ACS»: название службы; состояние службы (активен, неактивен)
Вкладка «ANKEY SIEM»	Содержит информацию о состоянии модуля взаимодействия с внешней системой ПК «Ankey SIEM»: название внешней системы; состояние модуля (активен, неактивен), и кнопку включения () /выключения () модуля
Вкладка «LDAP»	Содержит информацию о состоянии модулей взаимодействия с внешними источниками данных ПК «Ankey SIEM»: название внешнего источника; его состояние (активен, неактивен), и кнопки: — ручного перезапуска модуля (); — включения () /выключения () модуля
Панель «Журнал аварийных сигналов»	
Таблица	Содержит информацию о событиях, зафиксированных за текущие сутки в ПК «Efros ACS» при работе служб, модулей и приложения. Для каждого события указывается: — уровень события – «Ошибка» или «Предупреждение»; — поясняющий текст; — дата и время фиксирования события. Под таблицей приведено общее количество событий

3.4 Просмотр и настройка параметров работы ПК «Efros ACS»

3.4.1. Общие сведения

Для выполнения просмотра и настройки параметров работы ПК «Efros ACS» с внешними системами пользователю необходимо перейти на страницу раздела «Настройки системы», выбрав в панели главного меню ссылку «Настройки системы» или, если

панель свернута, – пиктограмму «». По умолчанию откроется страница «Корневые сертификаты» подраздела «Сертификаты» (рис. 25).

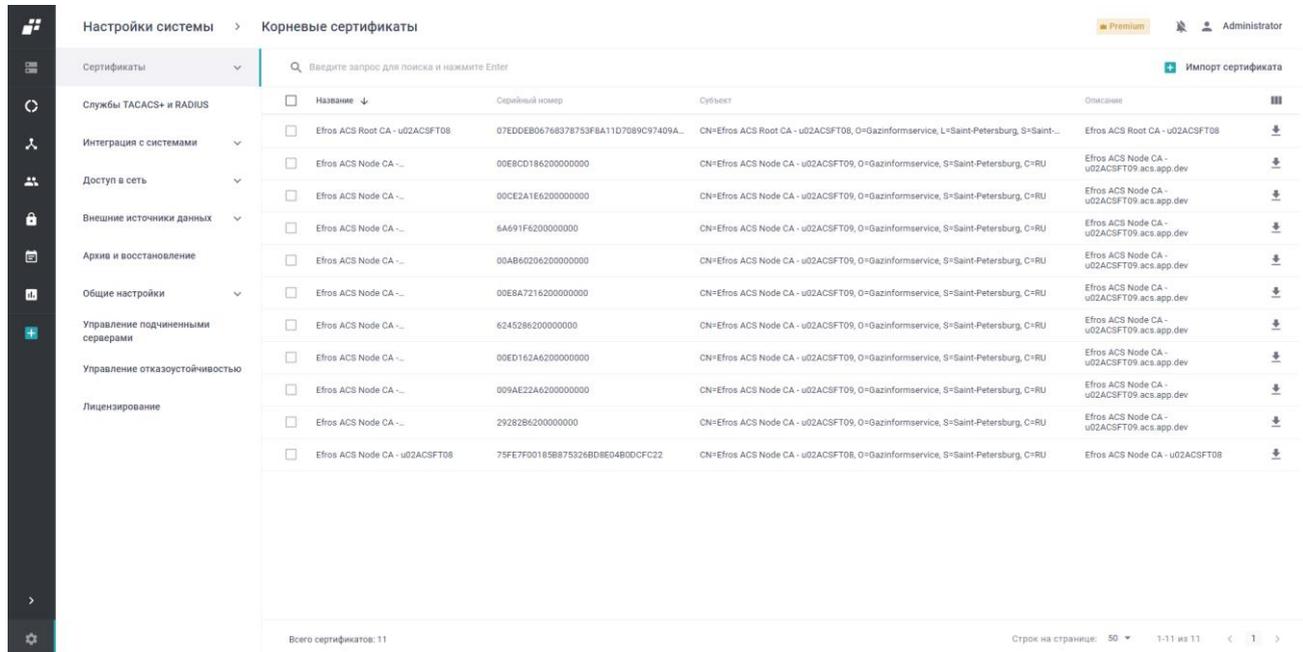


Рисунок 24 – Рисунок 25 – Страница раздела «Настройки системы» подраздел «Сертификаты: Корневые сертификаты» для администратора ACS

В разделе «Настройки системы» содержатся подразделы и вкладки подразделов для настройки работы ПК «Efros ACS»:

- 1) «Сертификаты». Подраздел содержит вкладки:
 - «Корневые» – предназначена для ведения списка корневых сертификатов;
 - «Серверные» – предназначена для ведения списка серверных сертификатов;
 - «Клиентские» – предназначена для ведения списка клиентских сертификатов;
 - «Шаблоны» – предназначена для ведения шаблонов клиентских сертификатов;
 - «Запросы на сертификаты» – предназначена для ведения списка запросов на сертификаты.
- 2) «Службы TACACS+ и RADIUS». Подраздел предназначен для настройки параметров работы ПК «Efros ACS» с сервисами протоколов TACACS+ и RADIUS.
- 3) «Интеграция с внешними системами». Подраздел содержит вкладки:
 - «Efros Config Inspector» – предназначена для настройки параметров работы ПК «Efros ACS» с ПК «Efros Config Inspector»;

- «Ankey SIEM» – предназначена для настройки параметров работы ПК «Efros ACS» с ПК «Ankey SIEM»;
- «Cisco ACS» – предназначена для настройки параметров работы ПК «Efros ACS» с ПО «Cisco ACS».

 Вкладки «Efros Config Inspector» и «Cisco ACS» доступны только администраторам ACS!

- 4) «Доступ в сеть». Подраздел предназначен для настройки доступа в сеть по EAP.
- 5) «Внешние источники данных». Подраздел содержит вкладки:
 - «LDAP» – предназначена для настройки параметров работы ПК «Efros ACS» со службой каталогов AD, в которой хранятся учетные записи пользователей, связанные с учетными записями пользователей ПК «Efros ACS»;
 - «Домен AD» – предназначена для настройки параметров работы ПК «Efros ACS» с контроллером домена, в которой хранятся учетные записи сетевых устройств, контролируемых ПК «Efros ACS»;
 - «Профили сертификатов» – предназначена для ведения списка профилей сертификатов, используемых при настройке политик аутентификации в политиках доступа устройств.
- 6) «Общие настройки». Подраздел содержит вкладки:
 - «Парольные политики» – предназначена для настройки сложности паролей пользователей и временных ограничений на доступ пользователей;
 - «Ротация журналов событий» – предназначена для настройки ротации и архивации журналов событий.
- 7) «Управление подчиненными серверами»⁵. Подраздел предназначен для ведения списка подчиненных серверов и настройки доступа к ним пользователей.
- 8) «Управление отказоустойчивостью»⁵. Подраздел предназначен для создания кластеров.
- 9) «Лицензирование». Подраздел предназначен для управления лицензией на комплекс.

Страницы подразделов и вкладок подразделов содержат поля для просмотра/ввода настраиваемых параметров. Пользователи с ролью «RO Администратор» (далее – администратор RO) имеют возможность только просмотра параметров работы ПК «Efros ACS» с внешними системами, пользователям с ролью «ACS Администратор» (далее – администратор ACS) параметры доступны для редактирования.

⁵ Раздел доступен только для лицензии ПК «Efros ACS» типа PREMIUM и только на главном сервере.

Для администраторов ACS вкладки дополнительно содержат кнопки:

- «Просмотреть» (👁) в полях ввода паролей пользователей – для просмотра введенных данных;
- «Отменить» – для выхода из режима редактирования параметров настройки без сохранения внесенных изменений;
- «Сохранить» – для выхода из режима редактирования параметров настройки с сохранением внесенных изменений.

Для просмотра настроек параметров работы с одной из внешних систем пользователю необходимо на странице раздела «Настройки системы» выбрать соответствующий раздел и вкладку, просмотреть данные, продолжить работу.

Для настройки параметров работы с одной из внешних систем администратору ACS необходимо на странице раздела «Настройки системы» выбрать соответствующий раздел и вкладку, выполнить действия в соответствии с п.п. 3.4.2 - 3.4.7.

После завершения обновления (успешного или неуспешного) параметров в журнал событий «Система» будут занесены соответствующие сообщения (см. п. 3.4.2 - 3.4.7).

3.4.2. Ведение списков цифровых сертификатов

Для ведения списков SSL-сертификатов, используемых в работе ПК «Efros ACS», пользователю необходимо в подразделе «Сертификаты»:

- 1) Сформировать во вкладке «Корневые» список корневых сертификатов центров сертификации.
- 2) Сформировать во вкладке «Запросы на сертификаты» запрос на выпуск серверного сертификата.
- 3) Сформировать во вкладке «Серверные» список серверных сертификатов, полученных по запросам.
- 4) Сформировать во вкладке «Шаблоны» список шаблонов клиентских сертификатов.
- 5) Сформировать во вкладке «Клиентские» список клиентских сертификатов.

После установки и первичной настройки ПК «Efros ACS» в ПК «Efros ACS» используются самоподписанные корневой и серверный сертификаты (далее – сертификаты «по умолчанию»). Удаление сертификатов «по умолчанию» не доступно администраторам ACS. Состав и описание элементов вкладок подраздела «Сертификаты» приведены в таблице 4.

 Если в ПК «Efros ACS» отсутствуют/удалены все серверные сертификаты, то ПК «Efros ACS» автоматически возвращается к самоподписанным сертификатам.

Таблица 4 – Состав и описание элементов вкладок подраздела «Сертификаты»

Элемент	Описание
Вкладка «Корневые»	
Поле поиска	Правила поиска приведены в п. 3.2.2
Кнопка «Импорт» ()	Для перехода в окно импортирования корневого сертификата
Кнопка «Добавить фильтр» ()	Для перехода в окно фильтрации. Правила фильтрации приведены в п. 3.2.4
Таблица корневых сертификатов	<p>Таблица содержит данные импортированных в БД ПК «Efros ACS» корневых сертификатов. Для каждого сертификата отображаются:</p> <ol style="list-style-type: none"> 1. Поле для флага (используется для выбора записей, с которыми необходимо выполнить действия: экспортировать, удалить и т.д.). 2. Данные: <ul style="list-style-type: none"> — название, присвоенное при импортировании; — серийный номер, присвоенный центром сертификации; — параметры сертификата, указанные в самом сертификате; — описание, введенное при импортировании. 3. Кнопки: <ul style="list-style-type: none"> — «Редактировать» () – для перехода в окно редактирования параметров сертификата: название, описание, статус; — «Экспортировать» () – для экспорта сертификата на локальную ЭВМ пользователя; — «Удалить» () – для удаления сертификата
Вкладка «Серверные»	
Поле поиска	Правила поиска приведены в п. 3.2.2
Кнопка «Импорт» ()	Для перехода в окно импортирования серверного сертификата

Элемент	Описание
Таблица серверных сертификатов	<p>Таблица содержит данные импортированных в БД ПК «Efros ACS» серверных сертификатов. Для каждого сертификата отображаются:</p> <p>4. Поле для флага (используется для выбора удаляемых записей).</p> <p>5. Данные:</p> <ul style="list-style-type: none"> — название, присвоенное при импортировании; — статус. Поле содержит одно из двух значений «Сертификат загружен» (сертификат загружен в БД «Efros ACS», но не найден связанный с ним корневой сертификат), «Связан с корневым» (в БД «Efros ACS» есть связанный с серверным сертификатом корневой сертификат); — данные об использовании сертификата в ПК «Efros ACS». Пиктограмма « WEB » означает, что сертификат используется для установки доверенного соединения при доступе к веб-приложению ПК «Efros ACS», пиктограмма « EAP »⁶ – для установки доверенного соединения при доступе устройств в сеть; — серийный номер, присвоенный центром сертификации; — параметры сертификата, указанные в самом сертификате; — описание, введенное при импортировании. <p>6. Кнопки:</p> <ul style="list-style-type: none"> — «Редактировать» (✎) – для перехода в окно редактирования параметров сертификата: название, описание, тип применения; — «Удалить» (🗑) – для удаления сертификата
Вкладка «Клиентские»	
Поле поиска	Правила поиска приведены в п. 3.2.2

⁶ Использование серверного сертификата для установки доверенного соединения при доступе устройств в сеть возможно после предварительной настройки TLS (Доступ в сеть → Настройки TLS). В данном случае, после привязки сертификата появится вариант использования EAP

Элемент	Описание
Таблица клиентских сертификатов	<p>Таблица содержит данные сгенерированных в ПК «Efros ACS» клиентских сертификатов. Для каждого сертификата отображаются:</p> <p>7. Поле для флага (используется для выбора удаляемых записей).</p> <p>8. Данные:</p> <ul style="list-style-type: none"> — данные субъекта сертификата; — статус. Поле содержит одно из двух значений «Активен» (сертификат действует), «Отозван» (сертификат отозван); — дата отзыва сертификата (для отозванных сертификатов)⁷; — данные издателя сертификата; — альтернативное имя; — серийный номер, присвоенный сертификату при его генерации в ПК; — дата генерации сертификата; — дата окончания срока действия сертификата. <p>9. Кнопки:</p> <ul style="list-style-type: none"> — «Отозвать»  – для отзыва сертификата; — «Экспортировать»  – для экспорта архива с сертификатом и ключом сертификата. По нажатию кнопки открывается меню выбора формата выгрузки. Подробно см. п. Выпуск клиентских сертификатов
Вкладка «Шаблоны»	
Поле поиска	Правила поиска приведены в п. 3.2.2
Кнопка «Добавить» 	Для перехода в окно создания нового шаблона клиентского сертификата

⁷ По умолчанию столбец «Дата отзыва» скрыт. Для его отображения в таблице необходимо нажать кнопку «Колонки»  в заголовке таблицы и в открывшемся окне установить флаг в поле «Дата отзыва» (см. п. 3.2.5)

Элемент	Описание
Таблица шаблонов клиентских сертификатов	Таблица содержит данные импортированных в БД ПК «Efros ACS» серверных сертификатов. Для каждого сертификата отображаются: 1. Поле для флага (используется для выбора удаляемых записей). 2. Данные: — название шаблона; — данные субъекта сертификата; — описание шаблона; — срок действия сертификата. 3. Кнопки: — «Редактировать» (✎) – для перехода в окно редактирования шаблона; — «Удалить» (🗑) – для удаления шаблона
Вкладка «Запросы на сертификаты»	
Поле поиска	Правила поиска приведены в п. 3.2.2
Кнопка «Добавить запрос» (+)	Для перехода в окно формирования запроса на сертификат
Таблица запросов на сертификаты	Таблица содержит данные сформированных ранее в ПК «Efros ACS» запросов на сертификаты. Для каждого запроса отображаются: 1. Поле для флага (используется для выбора экспортируемых или удаляемых записей). 2. Данные: — название, присвоенное при создании запроса; — статус: «Сформирован» (после создания), «Подтвержден» (после привязки сформированного по запросу сертификата); — параметры сертификата, указанные в самом сертификате; — альтернативные параметры, указанные при формировании запроса; — дата и время создания запроса.

Элемент	Описание
	<p>3. Кнопки:</p> <ul style="list-style-type: none">— «Привязать сертификат» (🔗) – для перехода в окно выбора файла с привязываемым сертификатом. Отображается только в строке запросов в статусе «Сформирован»;— «Экспортировать» (📄) – для экспорта файла запроса на локальную ЭВМ пользователя;— «Удалить» (🗑) – для удаления запроса на сертификат

Корневые сертификаты добавляются в список вкладки «Корневые» путем импорта из файла (см. п.п. 3.4.2.1). Серверные сертификаты добавляются в список вкладки «Серверные» либо автоматически после привязки к созданному ранее в ПК «Efros ACS» запросу сертификата (см. п.п. 3.4.2.2), либо путем импорта уже имеющегося в организации серверного сертификата в БД ПК «Efros ACS» (аналогично импорту корневых сертификатов).

При привязке или импорте серверного сертификата автоматически определяется соответствующий ему корневой сертификат. Если в БД ПК «Efros ACS» не обнаружен соответствующий корневой сертификат, то серверный сертификат добавляется в список подраздела «Сертификаты: Серверные», но не может быть выбран в настройках доступа в сеть (см. п. 3.4.5) в качестве серверного сертификата, используемого при аутентификации устройств на сервере аутентификации. При этом соответствующий корневой сертификат может быть добавлен в список подраздела «Сертификаты: Корневые» после добавления серверного сертификата, в процессе добавления будет выполнена автоматическая привязка серверного сертификата к добавленному корневому, после чего серверный сертификат будет доступен для выбора при настройке доступа в сеть в качестве серверного сертификата, используемого при аутентификации устройств на сервере аутентификации.

Для обеспечения взаимной аутентификации клиентских ЭВМ и сервера ПК «Efros ACS» в ПК «Efros ACS» выпускается клиентский сертификат (на основе одного из созданных ранее шаблонов), далее на клиентскую ЭВМ устанавливается полученный при выпуске сертификата архив файлов.

Клиентские сертификаты добавляются в список вкладки «Клиентские» администратором ACS и администратором CER на основе ранее созданных во вкладке «Шаблоны» шаблонов клиентских сертификатов.

Примечание. Использование шаблонов позволяет унифицировать и ускорить процесс выпуска сертификатов, поскольку параметры субъекта сертификата "Организация", "Подразделение", "Страна", "Город", "Область" могут быть одинаковыми для клиентских ЭВМ.

3.4.2.1. Ведение списка корневых сертификатов

Для добавления в БД ПК «Efros ACS» корневого сертификата администратору необходимо:

- 1) Перейти на вкладку «Корневые» подраздела «Сертификаты» (см. рис. 25).
- 2) Нажать кнопку «Импорт сертификата» (+). Страница «Новый корневой сертификат», приведенная на рис. 26.
- 3) Выбрать файл с добавляемым сертификатом, для чего:
 - нажать кнопку «Выбрать файл»;
 - выбрать в стандартном окне ОС файл сертификата.
- 4) Ввести в полях «Название» и «Описание» соответствующие данные сертификата.

← Новый корневой сертификат Premium Danilova-N

Файл сертификата ? **Выбрать файл** Файл не выбран

Название ? Введите название
Обязательное поле 0/50

Описание Введите описание 0/250

Добавить Отменить

Рисунок 25 – Рисунок 26 – Страница «Новый корневой сертификат»

- 5) Нажать кнопку «Добавить». Откроется таблица корневых сертификатов, в таблице добавится строка с данными нового сертификата.

Администратор имеет возможность просмотреть данные сертификата и изменить название и описание, для чего необходимо:

- 1) Нажать в строке сертификата кнопку «Изменить».
- 2) На открывшейся странице (рис. 27):
 - просмотреть данные сертификата;

- внести требуемые изменения и нажать кнопку «Изменить». Откроется таблица корневых сертификатов, внесенные изменения будут сохранены.

Удаление сертификатов выполняется в соответствии с п. 3.2.6. Удаление сертификата «по умолчанию» не доступно.

← Редактирование корневого сертификата		Premium	🔔	👤 Danilova-N
Название ⓘ	dsad	4/50		
Описание	Введите описание	0/250		
Субъект	CN=Efros ACS Node CA - u02ACSFT05, O=Gazinformservice, S=Saint-Petersburg, C=RU			
Издатель	CN=Efros ACS Root CA - u02ACSFT05, O=Gazinformservice, L=Saint-Petersburg, S=Saint-Petersburg, C=RU			
Действителен с	Вторник, 09 марта, 2021, 07:37:26 (+03:00)			
Действителен до	Воскресенье, 09 марта, 2031, 07:37:26 (+03:00)			
Серийный номер	4486B38476F78B4B8B5E9207780DED5A			

Сохранить Отменить

Рисунок 26 – Рисунок 27 – Страница «Редактирование корневого сертификата»

Кроме того, администратор имеет возможность экспортировать корневой сертификат на локальную ЭВМ, для чего необходимо:

1) Способ 1:

- нажать в строке требуемого сертификата кнопку «Экспортировать» (📄);
- нажать в информационной строке операции кнопку «Сохранить».

2) Способ 2:

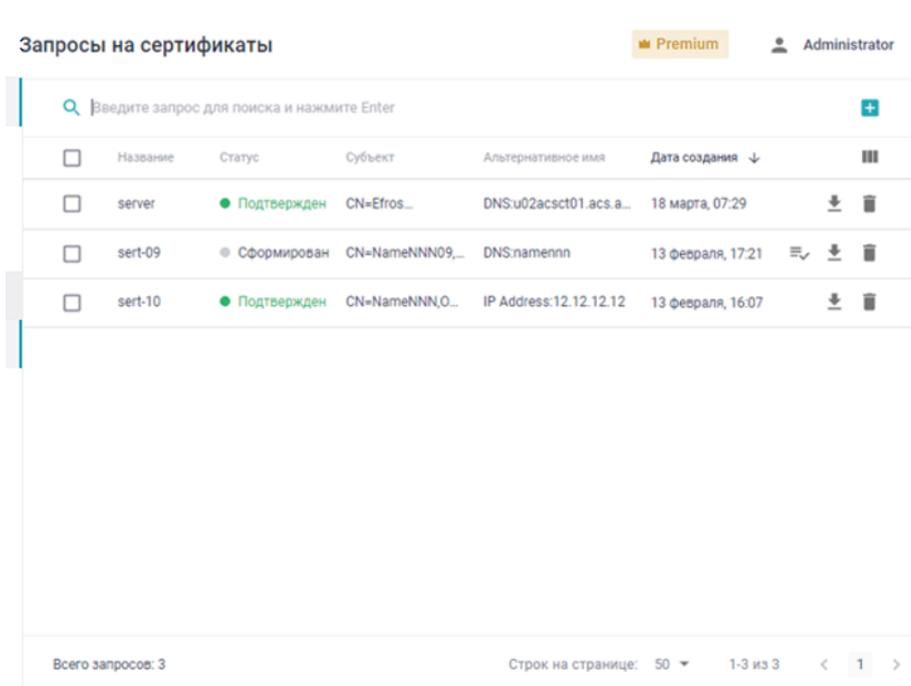
- установить флаг в строке требуемого сертификата;
- нажать в строке операций над таблицей сертификатов кнопку «Экспорт» (📄);
- нажать в информационной строке операции кнопку «Сохранить».

3.4.2.2. Ведение списка запросов на сертификаты

Для формирования нового запроса на сертификат администратору необходимо:

- 1) Перейти на вкладку «Запросы на сертификаты» подраздела «Сертификаты» (рис. 28).

Примечание. После установки ПК «Efros ACS» список запросов на сертификаты пуст, на странице отображается сообщение «В системе нет запросов на сертификаты» и кнопка «Добавить» () для перехода на страницу создания нового запроса на сертификат.



<input type="checkbox"/>	Название	Статус	Субъект	Альтернативное имя	Дата создания ↓	
<input type="checkbox"/>	server	● Подтвержден	CN=Efros...	DNS:u02acsct01.acs.a...	18 марта, 07:29	⬇️ 🗑️
<input type="checkbox"/>	sert-09	● Сформирован	CN=NameNNN09,...	DNS:namennn	13 февраля, 17:21	⬇️ 🗑️
<input type="checkbox"/>	sert-10	● Подтвержден	CN=NameNNN,O...	IP Address:12.12.12.12	13 февраля, 16:07	⬇️ 🗑️

Рисунок 27 – Рисунок 28 – Вкладка «Запросы на сертификаты»

- 2) Нажать кнопку «Добавить запрос» (). Откроется страница «Новый запрос на сертификат», приведенная на рис. 29.
- 3) Ввести название запроса, заполнить поля группы «Субъект» данными организации.
- 4) Указать альтернативное имя (одно или несколько) сервера, для чего в группе «Альтернативное имя (SAN)»:
 - выбрать в поле со списком тип дополнительного параметра: «DNS», «IP-адрес», «URL ресурса» или «Директория»;
 - ввести проверяемое при проверке сертификата значение параметра;

- в автоматически добавленной строке группы указать тип и значение второго альтернативного имени;
 - повторить действия по добавлению для всех требуемых параметров;
 - удалить ошибочно добавленные параметры, нажав соответствующие им кнопки «Удалить» (🗑️).
- 5) Нажать кнопку «Добавить». Откроется страница со списком запросов, в таблице добавится строка с данными нового запроса, запросу будет присвоен статус «Сформирован». В журнал событий ПК «Efros ACS» будет внесено сообщение о создании запроса.

← Новый запрос на сертификат Premium Danilova-N

Название ? Введите название 0/50

Субъект

Общее имя (CN) ? Введите общее имя 0/50

Организация (O) ? Введите организацию 0/50

Подразделение (OU) ? Введите подразделение 0/50

Страна (C) ? Введите страну 0/2

Город (L) ? Введите город 0/50

Область (ST) ? Введите область 0/50

Альтернативное имя (SAN) ? Выберите тип 0/50

Добавить Отменить

Рисунок 28 – Рисунок 29 – Страница «Новый запрос на сертификат»

Администратор имеет возможность просмотреть параметры запроса, для чего необходимо нажать в строке запроса на текст-ссылку в графе «Название». Откроется окно просмотра, приведенное на рис. 30. Окно содержит две вкладки:

- 1) «Информация о запросе» – с параметрами запроса.
- 2) «Тело запроса» – с текстом запроса.

sert-09 ● Сформирован

ИНФОРМАЦИЯ О ЗАПРОСЕ ТЕЛО ЗАПРОСА

Название запроса	sert-09
Альтернативное имя	DNS:namennn
Субъект	CN=NameNNN09,OU=OZR,O=Gis,L=SPb,ST=SPb,C=RU
Дата создания	13 февраля 2020, 17:32

ЗАКРЫТЬ

Рисунок 29 – Рисунок 30 – Окно просмотра параметров запроса на сертификат

Для экспорта запроса на локальную ЭВМ администратору необходимо:

1) Способ 1:

- нажать в строке запроса кнопку «Экспортировать» (↓);
- нажать в информационной строке операции кнопку «Сохранить».

2) Способ 2:

- установить флаг в строке требуемого запроса;
- нажать в строке операций над таблицей запросов кнопку «Экспорт» (↓);
- нажать в информационной строке операции кнопку «Сохранить».

Удаление запросов выполняется в соответствии с п. 3.2.6.

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

- 1) Нажать в строке запроса кнопку «Привязать сертификат» (≡✓).
- 2) На открывшейся странице (рис. 31) выбрать файл с сертификатом, нажав кнопку «Выбрать файл» и выбрав в стандартном окне ОС требуемый файл.

← Привязка сертификата Premium Danilova-N

Файл сертификата ? файл не выбран

Название ? Введите название
Обязательное поле 0/50

Для чего используется ? WEB-консоль

Рисунок 30 – Рисунок 31 – Страница привязки сертификата к запросу

- 3) Ввести название сертификата, которое будет использоваться в ПК «Efros ACS».
- 4) Указать, при необходимости, установкой флага в поле «WEB-консоль» использование сертификата для установки доверенного соединения при доступе к веб-приложению ПК «Efros ACS».
- 5) Нажать кнопку «Привязать». Страница 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 (рис. 32);
 - сертификат будет добавлен в список серверных сертификатов ПК «Efros ACS» (см. п.п. 3.4.2.3).

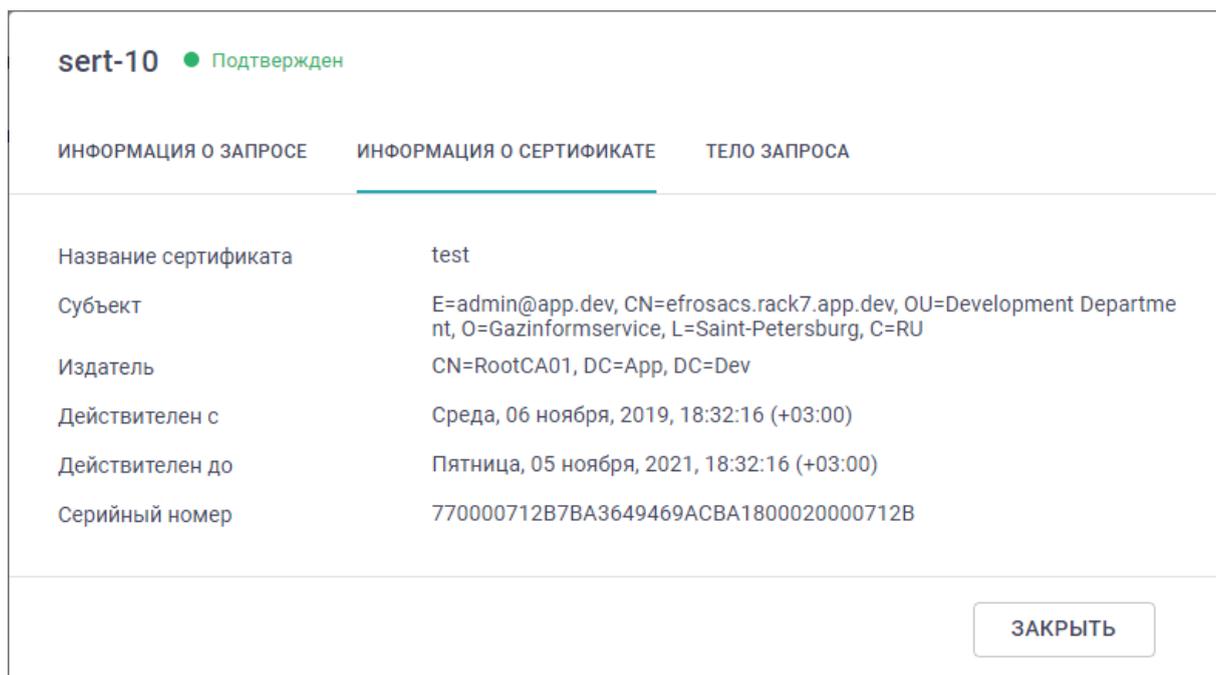


Рисунок 31 – Рисунок 32 – Окно просмотра запроса с вкладкой «Информация о сертификате»

3.4.2.3. Ведение списка серверных сертификатов

Добавление серверных сертификатов выполняется автоматически после привязки к запросу сертификата, полученного от центра сертификации (см. п.п. 3.4.2.2), либо путем импорта уже имеющегося в организации серверного сертификата в БД ПК «Efros ACS».

Импорт серверного сертификата выполняется аналогично импорту корневых сертификатов (см. п.п. 3.4.2.1), за исключением того, что на странице окне «Новый серверный сертификат» (рис. 33):

- 1) Выбирается не только файл сертификата, но и файл закрытого ключа для сертификата.
- 2) Не задается статус сертификата.
- 3) Выбирается, при необходимости, тип использования сертификата «WEB-консоль» – для установки доверенного соединения при доступе к веб-приложению ПК «Efros ACS».

← Новый серверный сертификат Premium Danilova-N

Файл сертификата ? Файл не выбран

Закрытый ключ Файл не выбран

Название ? 0/50

Описание 0/250

Для чего используется ? WEB-консоль

Рисунок 32 – Рисунок 33 – Страница «Новый серверный сертификат»

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

- 1) Перейти на вкладку «Серверные» подраздела «Сертификаты» (рис. 34).
- 2) Выбрать в строке требуемого сертификата его название. Откроется страница редактирования серверного сертификата (рис. 35).
- 3) Внести требуемые изменения в название и/или описание сертификата.
- 4) Установкой/отменой установки флага в поле группы «Для чего используется» указать тип использования сертификата: «WEB-консоль».
- 5) Нажать кнопку «Изменить». Внесенные изменения будут сохранены.

Удаление сертификатов выполняется в соответствии с п. 3.2.6. Удаление сертификата «по умолчанию» не доступно.

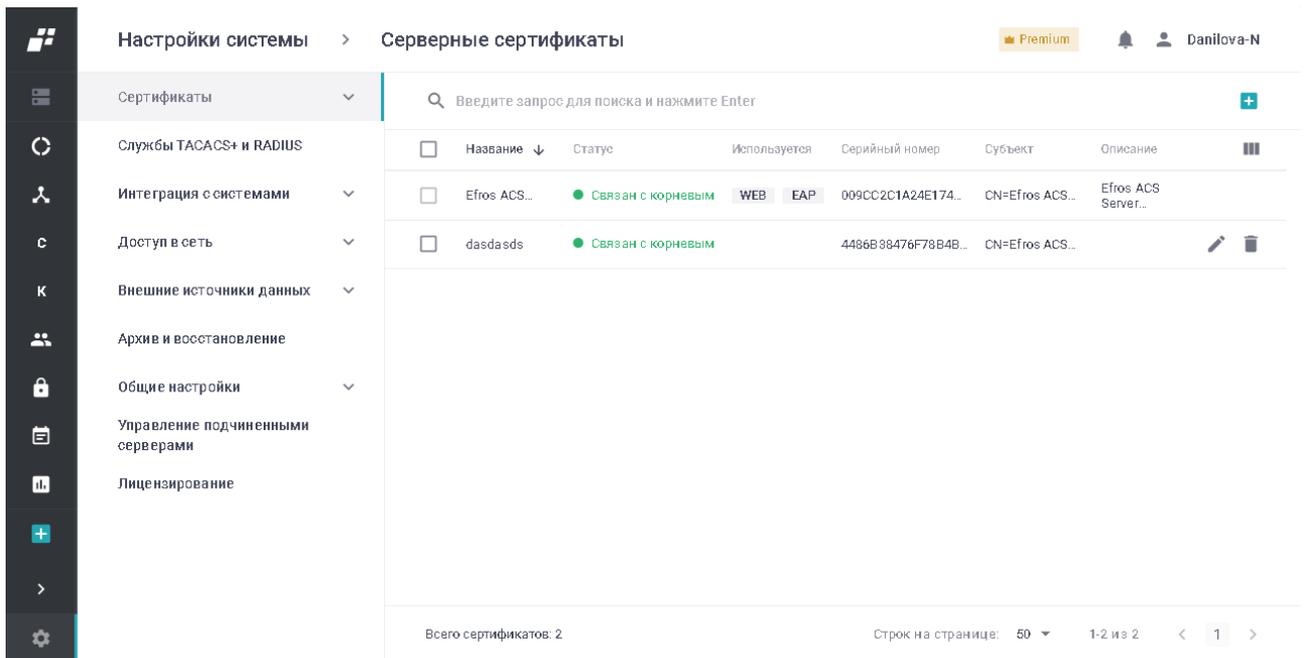


Рисунок 33 – Рисунок 34 – Вкладка «Серверные сертификаты»

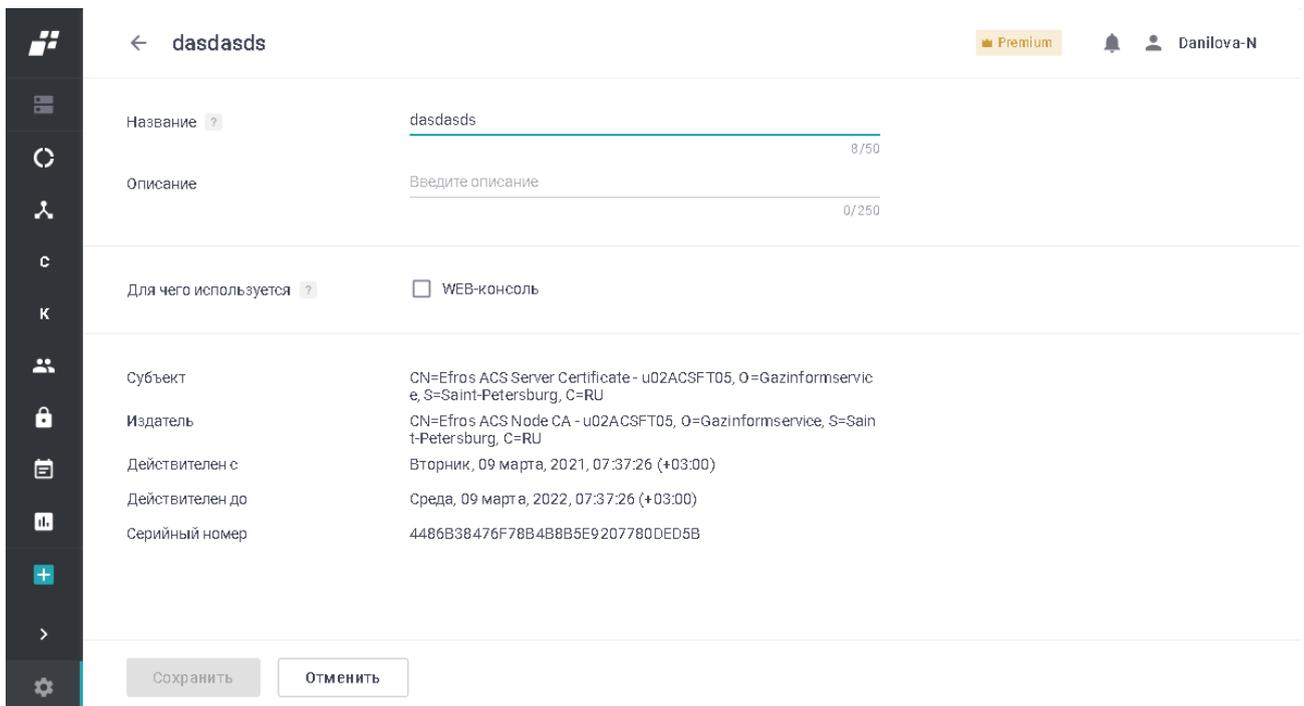


Рисунок 34 – Рисунок 35 – Страница редактирования серверного сертификата

3.4.2.4. Ведение списка шаблонов клиентских сертификатов

Для добавления в БД ПК «Efros ACS» нового шаблона клиентского сертификата администратору необходимо:

- 1) Перейти на вкладку «Шаблоны сертификатов» подраздела «Сертификаты» (рис. 36).

<input type="checkbox"/>	Название ↓	Субъект	Описание	Срок действия сертификата	
<input type="checkbox"/>	testnnp	CN=nnn1,O=nnn,ST=jdh,C=ru	nnp	1000 дней	
<input type="checkbox"/>	te	CN=tr,OU=te,O=te,L=te,ST=te,C=te	te	190 дней	

Рисунок 35 – Рисунок 36 – Вкладка «Шаблоны сертификатов»

- 2) Нажать кнопку «Добавить шаблон» (). Откроется страница «Новый шаблон сертификата», приведенная на рис. 37.
- 3) Ввести название и описание шаблона.
- 4) Ввести срок действия сертификата (от 180 до 3652⁸ дней).
- 5) Заполнить поля группы «Субъект» данными клиента.
- 6)

Все поля шаблона, кроме полей «Описание» и «Общее имя (CN)» обязательны для заполнения. Общее имя (CN) (идентификатор машины (суппликанта), на которую выпускается сертификат) может быть задано при выпуске сертификата (см. п.п. 3.4.2.5).

- 7) Нажать кнопку «Добавить».

⁸ Максимально допустимое значение 3652 дня соответствует значению – 10 лет

← Новый шаблон сертификата Premium Danilova-N

Название ? Введите название шаблона 0/50

Описание Введите описание шаблона 0/250

Срок действия сертификата ? 0 дней

Субъект

Общее имя (CN) ? Введите общее имя 0/50

Организация (O) ? Введите организацию 0/50

Подразделение (OU) ? Введите подразделение 0/50

Страна (C) ? Введите страну 0/2

Город (L) ? Введите город 0/50

Область (ST) ? Введите область 0/50

Добавить Отменить

Рисунок 36 – Рисунок 37 – Страница «Новый шаблон сертификата»

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

Администратор имеет возможность создать новый шаблон или, нажав кнопку «Отменить», перейти на страницу вкладки «Шаблоны сертификатов», в таблице которой добавится строка с данными созданного шаблона.

Далее администратор имеет возможность:

- просмотреть и отредактировать параметры шаблона, для чего необходимо нажать в строке шаблона кнопку «Редактировать» (✎), внести требуемые изменения в поля страницы редактирования и нажать кнопку «Изменить»;
- удалить шаблон – в соответствии с п. 3.2.6.

Сообщения о выполненных с шаблонами действиях будут внесены в журнал событий ПК «Efros ACS».

3.4.2.5. Выпуск клиентских сертификатов

Выпуск клиентских сертификатов выполняется администратором CI на отдельной странице ПК «Efros ACS», которая открывается сразу после запуска ПК «Efros ACS» (рис. 38), либо администратором ACS на странице раздела «Сертификаты», которая открывается по нажатию кнопки «Добавить сертификат» (+) над таблицей клиентских сертификатов (см. п.п. 3.4.2.6).

Инициализация сертификата

Шаблон ⓘ Выберите шаблон

Общее имя (CN) ⓘ Введите общее имя 0/50

Альтернативное имя (SAN) ⓘ Выберите тип 0/50 +

Формат загрузки ⓘ Выберите формат загрузки

СГЕНЕРИРОВАТЬ

Рисунок 37 – Рисунок 38 – Страница выпуска клиентского сертификата

Для выпуска сертификата администратору необходимо:

- 1) Выбрать в поле «Шаблон» название требуемого шаблона, созданного ранее в ПК «Efros ACS».
- 2) 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.
- 3) Указать альтернативное имя (одно или несколько) клиентской ЭВМ, для чего в группе «Альтернативное имя (SAN)»:
 - выбрать в поле со списком тип дополнительного параметра: «DNS», «IP-адрес», «URL ресурса» или «Директория»;

- ввести проверяемое при проверке сертификата значение параметра;
 - в автоматически добавленной строке группы указать тип и значение второго альтернативного имени;
 - повторить действия по добавлению для всех требуемых параметров;
 - удалить ошибочно добавленные параметры, нажав соответствующие им кнопки «Удалить» (■).
- 4) Выбрать один из форматов загрузки клиентского и публичной части корневого сертификатов:
- «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.

- 5) Нажать кнопку «Сгенерировать». Будет запущен процесс генерации архива с сертификатом и ключом. По окончании процесс отобразит соответствующее сообщение.

Выпущенный сертификат будет внесен в список клиентских сертификатов (см. п.п. 3.4.2.6) и будет доступен администратору ACS для отзыва и удаления. В журнал событий ПК «Efros ACS» будет внесено сообщение о генерации сертификата.

Далее поля формы выпуска сертификата очистятся, и администратор имеет возможность выпустить другой сертификат или завершить работу с ПК «Efros ACS».

Полученные в результате сертификат и ключ необходимо загрузить на клиентскую ЭВМ.

3.4.2.6. Ведение списка клиентских сертификатов

Список выпущенных в ПК «Efros ACS» клиентских сертификатов во вкладке «Клиентские сертификаты» раздела «Сертификаты» (рис. 39) доступен:

- администраторам ACS – для просмотра, отзыва и экспорта сертификатов;
- администраторам RO – для просмотра.

Для просмотра сертификата администратору необходимо нажать в строке сертификата на текст-ссылку в графе «Субъект». Откроется окно просмотра с данными сертификата. Для завершения просмотра – нажать в окне кнопку «Закреть».

Клиентские сертификаты Premium Danilova-N

Введите запрос для поиска и нажмите Enter +

Субъект ↓	Статус	Издатель	Альтернативное имя	Серийный номер	Дата создания	Дата окончания	
CN=tr, OU=...	Активен	CN=Efros ACS...	email:11-11-11-11-11-11	008368E94D4EE5D...	12.03.21	18.09.21	
CN=tr, OU=...	Активен	CN=Efros ACS...	email:00-14-22-04-25-37	3C8DD83849E5D888	12.03.21	18.09.21	
CN=tr, OU=...	Активен	CN=Efros ACS...	email:00-14-22-04-25-23	00F553028445E6D8...	12.03.21	18.09.21	
CN=tr, OU=...	Активен	CN=Efros ACS...	email:00-14-22-04-25-37	00E03399E06EE4D8...	11.03.21	17.09.21	
CN=tr, OU=...	Активен	CN=Efros ACS...	email:00-14-22-04-25-34	102741C674E4D888	11.03.21	17.09.21	
CN=tr, OU=...	Активен	CN=Efros ACS...	email:00-14-22-04-25-30	0080D8DB4271E4D...	11.03.21	17.09.21	
CN=tr, OU=...	Активен	CN=Efros ACS...	email:00-14-22-04-25-37	282D13E758E5D888	12.03.21	18.09.21	
CN=tr, OU=...	Отозван	CN=Efros ACS...	DNS:123.1.1.11	0099CA2B1688E4D...	11.03.21	17.09.21	
CN=tr, OU=...	Активен	CN=Efros ACS...	email:00-14-22-04-25-38	3B0CF1A96FE4D888	11.03.21	17.09.21	
CN=trdsad...	Активен	CN=Efros ACS...	email:11-11-11-11-11-11	00B1BDD6434EE5D...	12.03.21	18.09.21	

Всего сертификатов: 10 Строк на странице: 50 1-10 из 10 < 1 >

Рисунок 38 – Рисунок 39 – Вкладка «Клиентские сертификаты»

Для отзыва сертификата администратору необходимо нажать в строке отзываемого сертификата кнопку «Отозвать» () и в открывшемся окне подтверждения – кнопку «ОТОЗВАТЬ». Сертификат будет отозван, клиент не сможет по нему получить доступ в сеть через ПК «Efros ACS».

Для экспорта сертификата на локальную ЭВМ администратору необходимо:

- 1) Нажать в строке запроса кнопку «Экспортировать» ()
- 2) Выбрать в раскрывшемся меню формат загрузки клиентского и публичной части корневого сертификатов:
 - «Сертификат (PEM) и ключ (PKCS8 PEM)» – будет выгружен следующий состав файлов: «ca.pem», «client.key», «client.pem»;
 - «Сертификат и ключ (PKCS12)» – будет выгружен следующий состав файлов: «ca.pem», «client.key», «client.p12».
- 3) При выборе формата «Сертификат и ключ (PKCS12)» ввести в дополнительном поле пароль для закрытого ключа и нажать кнопку «Скачать».
- 4) Полученные в результате сертификат и ключ необходимо загрузить на клиентскую ЭВМ.

Сообщения о выполненных с клиентскими сертификатами действиях будут внесены в журнал событий ПК «Efros ACS».

3.4.3. Настройка служб протоколов TACACS+ и RADIUS

Для выполнения настройки подключения к сервисам протоколов TACACS+ и RADIUS пользователю необходимо:

- 1) Выбрать на странице «Настройки системы» раздел «Службы TACACS+ и RADIUS». Откроется страница «Службы TACACS+ и RADIUS» (рис. 40). Состав и описание элементов страницы приведены в таблице 5.
- 2) Ввести в поля вкладки требуемые значения параметров.
- 3) Нажать кнопку «Сохранить».

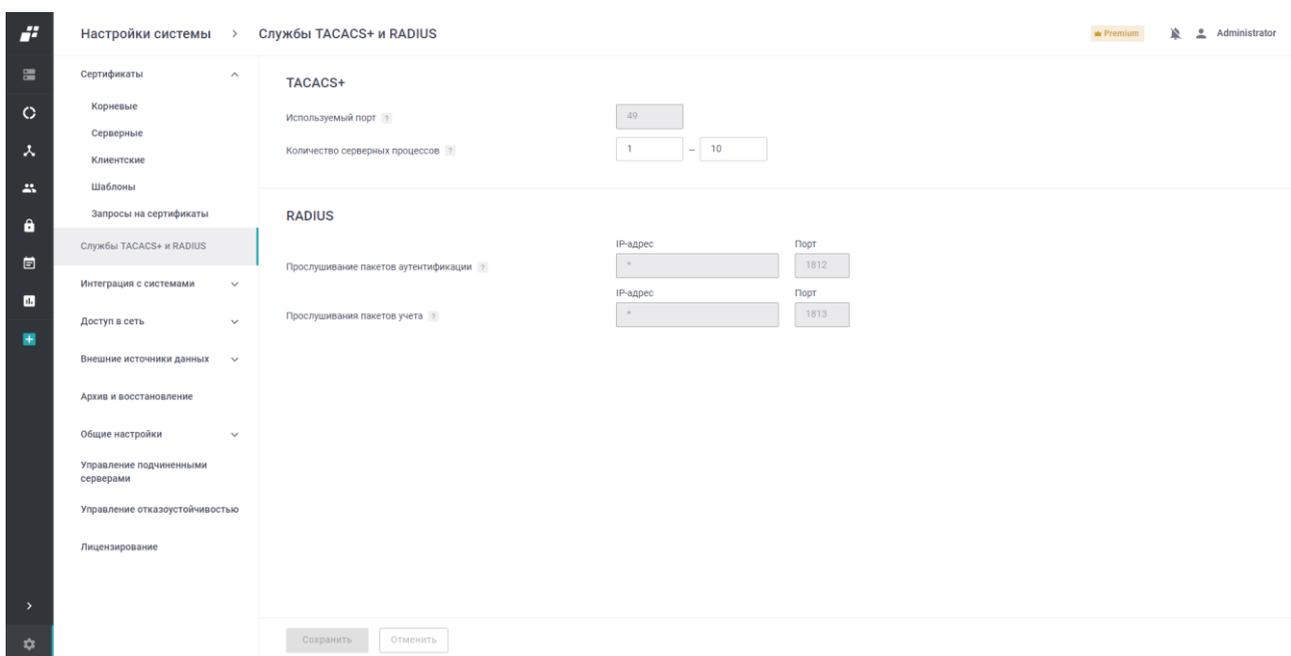


Рисунок 39 – Рисунок 40 – Страница раздела «Службы TACACS+ и RADIUS»

Таблица 5 – Состав и описание элементов страницы раздела «Службы TACACS+ и RADIUS»

Элемент	Описание
Группа полей «TACACS+»	
*Поле «Используемый порт»	Числовое поле для ввода номера порта сервера ПК «Efros ACS» для протокола TACACS+. По умолчанию содержит значение 49
*Поле «Количество серверных процессов»	Числовые поля для ввода минимального и максимального количества процессов для службы TACACS+. По умолчанию содержит значения 1, 10
Группа полей «RADIUS»	

Элемент	Описание
Поле «Прослушивание пакетов аутентификации»	Содержит поля: — для ввода IP-адресов прослушиваемых серверов; — для ввода номера порта прослушивания пакетов аутентификации. По умолчанию прослушиваются все сервера в сети (значение «») и порт прослушивания - 1812
Поле «Прослушивание пакетов учета»	Содержит поля: — для ввода IP-адресов прослушиваемых серверов; — для ввода номера порта прослушивания пакетов учета. По умолчанию прослушиваются все сервера в сети (значение «») и порт прослушивания - 1813

Введенные значения будут сохранены в БД ПК «Efros ACS», будет запущен процесс обновления конфигурационного файла сервиса. После завершения обновления (успешного или неуспешного) в журнал событий «Система» будут занесены сообщения в соответствии с таблицей 6.

Таблица 6 – Сообщения по результатам обновления параметров работы ПК «Efros ACS» с протоколами

Объект настройки	Тип события	Сообщение	Описание
TACACS+	Инфо	Новый config-файл успешно проверен. TACACS+ перезапускается	Фиксируется в тот момент, когда конфигурационный файл протокола успешно обновлен
		[TACACS+] Сервис перезапущен	Фиксируется в момент, когда сервис перезапущен без ошибок
	Ошибка	[TACACS+] Ошибка проверки config-файла: {текст_ошибки}	Фиксируется в тот момент, когда конфигурация протокола обновлена, но в новой конфигурации обнаружена ошибка и сервис не может начать работать с новой конфигурацией. В таком случае производится возврат к старой конфигурации протокола.

Объект настройки	Тип события	Сообщение	Описание
			{текст_ошибки} – описание ошибки, пришедшее с сервера
		[TACACS+] Ошибка перезапуска: {текст_ошибки}	Фиксируется в тот момент, когда произошла ошибка при перезапуске сервиса протокола.
RADIUS	Инфо	[RADIUS] Запись файла ldap	Выполнено изменение параметров подключения сервиса протокола RADIUS к AD
		[RADIUS] Сервис перезапущен	Перезапуск сервиса протокола RADIUS успешен
	Ошибка	[RADIUS] ошибка перезапуска: {текст_ошибки}	Фиксируется в случае, если во время перезапуска сервиса RADIUS произошла ошибка

3.4.4. Настройка интеграции с внешними системами

3.4.4.1. Настройка подключения к ПК «Efros Config Inspector». Импорт данных из ПК «Efros Config Inspector»

Для выполнения настройки подключения к ПК «Efros Config Inspector» пользователю необходимо:

- 1) Выбрать на странице «Настройки системы» в подразделе «Интеграция с внешними системами» вкладку «Efros Config Inspector». Откроется страница вкладки «Efros Config Inspector» (рис. 41). Состав и описание элементов страницы приведены в таблице 7.
- 2) Ввести в поля вкладки требуемые значения параметров.
- 3) Проверить успешность подключения к указанному серверу установки ПК «Efros Config Inspector», нажав кнопку «Проверить соединение».

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

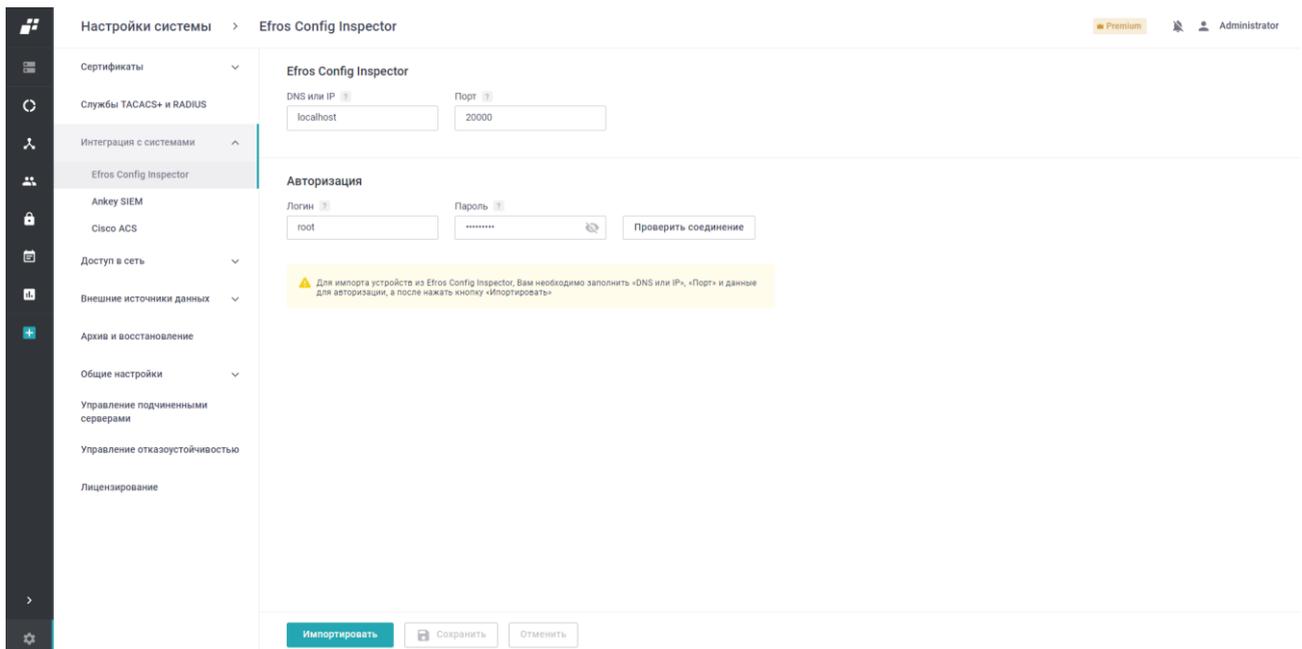


Рисунок 40 – Рисунок 41 – Вкладка «Efras Config Inspector»

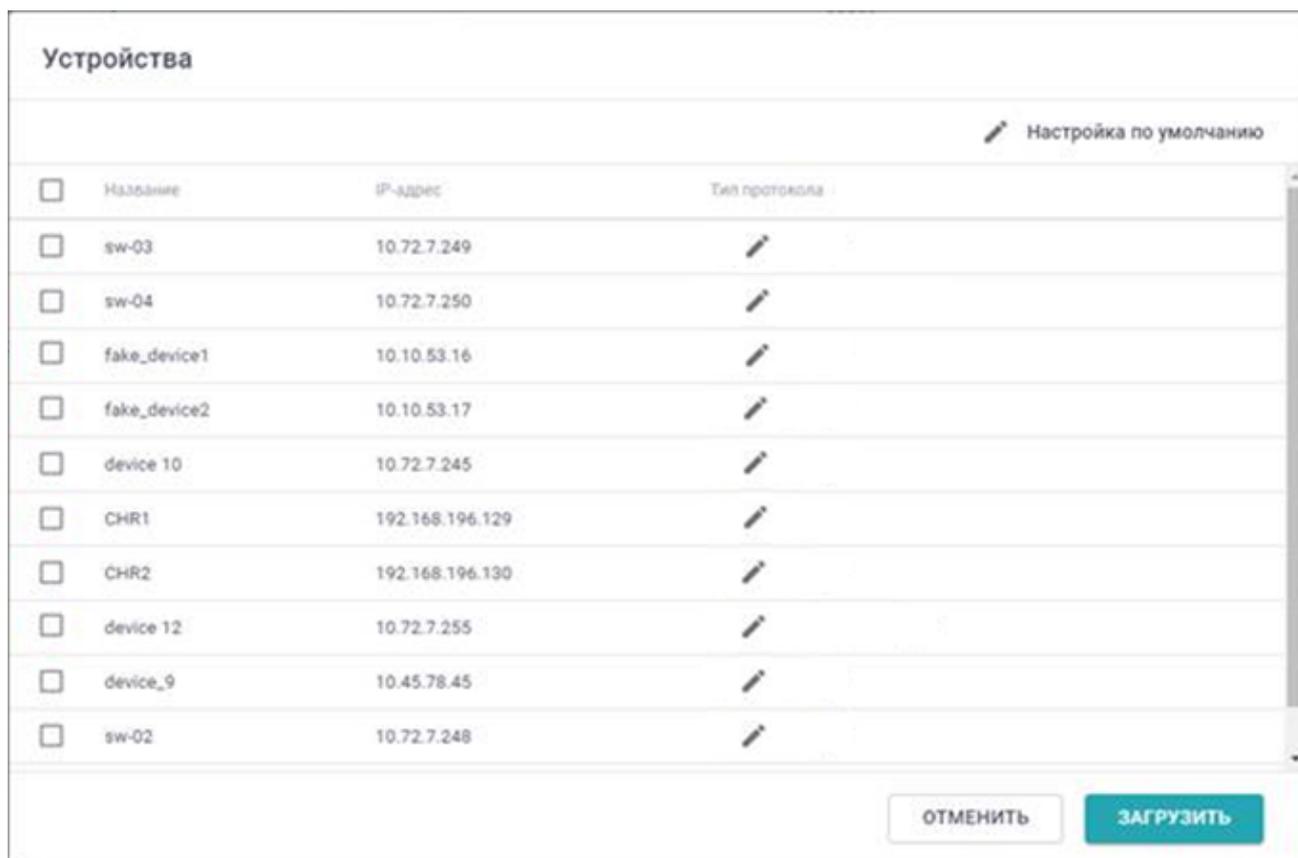
Таблица 7 – Состав и описание элементов страницы вкладки «Efras Config Inspector»

Элемент	Описание
*Поле «DNS или IP»	Поле для ввода DNS-имени или IP-адреса домена установки ПК «Efras Config Inspector», с которым настраивается соединение
*Поле «Порт»	Числовое поле для ввода номера порта сервера ПК «Efras ACS» для взаимодействия с ПО «Efras Config Inspector». По умолчанию содержит значение 20000
*Поле «Логин»	Поле для ввода имени пользователя, под которым выполняется подключение к ПО «Efras Config Inspector».
*Поле «Пароль»	Поле для ввода пароля пользователя, под которым выполняется подключение к ПО «Efras Config Inspector». При вводе символы пароля заменяются знаком «●». Для просмотра введенного значения необходимо нажать в поле ввода кнопку «Просмотреть» (👁)
Поле «Проверка соединения»	Содержит кнопку «ПРОВЕРИТЬ». По нажатию кнопки выполняется проверка успешности установления соединения с введенными параметрами к указанному серверу ПК «Efras Config Inspector».

Элемент	Описание
	Кнопка доступна как администраторам ACS, так и администраторам RO. После успешного завершения проверки в верхней части страницы отображается сообщение «Соединение с Config Inspector активно». Если проверка завершилась с ошибкой, то сообщение «Соединение с Config Inspector неактивно»
Поле «Сохранить учетные данные»	Поле для флага. При наличии в поле флага, после внесения в поля «Логин» и «Пароль» страницы изменений и успешного завершения проверки соединения с сервером ПК «Efros Config Inspector», внесенные данные сохраняются и применяются при следующем подключении к серверу ПК «Efros Config Inspector»
Кнопка «Импортировать»	По нажатию кнопки выполняется загрузка списка устройств БД ПК «Efros Config Inspector» в окно выбора импортируемых в ПК «Efros ACS» устройств. Далее пользователь имеет возможность выбрать импортируемые устройства, выбрать для них протокол работы и загрузить данные
* – Справа от поля расположен знак «?», при наведении на который курсора открывается всплывающая подсказка с правилами заполнения поля	

- 4) После получения сообщения об успешном подключении, проконтролировать наличие флага в поле «Сохранить учетные данные» и нажать кнопку «Импортировать».

После чего введенные параметры будут сохранены в БД ПК «Efros ACS», будет выполнен импорт устройств из БД ПК «Efros Config Inspector», откроется окно со списком устройств из БД ПК «Efros Config Inspector», приведенное на рис. 42.



<input type="checkbox"/>	Название	IP-адрес	Тип протокола
<input type="checkbox"/>	sw-03	10.72.7.249	
<input type="checkbox"/>	sw-04	10.72.7.250	
<input type="checkbox"/>	fake_device1	10.10.53.16	
<input type="checkbox"/>	fake_device2	10.10.53.17	
<input type="checkbox"/>	device 10	10.72.7.245	
<input type="checkbox"/>	CHR1	192.168.196.129	
<input type="checkbox"/>	CHR2	192.168.196.130	
<input type="checkbox"/>	device 12	10.72.7.255	
<input type="checkbox"/>	device_9	10.45.78.45	
<input type="checkbox"/>	sw-02	10.72.7.248	

Рисунок 41 – Рисунок 42 – Окно списка устройств, полученного из ПК «Efros Config Inspector»

Далее необходимо выбрать устройства, импортируемые в ПК «Efros ACS», для чего:

- 1) Установить флаг в полях левого столбца списка, соответствующих импортируемым устройствам.
- 2) Выбрать для устройств протоколы, по которым устройства работают. Для выбора протокола или обоих протоколов для одного устройства:
 - нажать кнопку «Редактировать» () в правом столбце списка, соответствующую устройству;
 - установить в открывшемся окне (рис. 43) флаг в поле слева от требуемого протокола или обоих протоколов;
 - для выбранного протокола ввести указанный на устройстве разделяемый ключ. При вводе символы ключа заменяются знаком «●». Для просмотра введенного значения необходимо нажать в поле ввода кнопку «Просмотреть» ()

TACACS+

RADIUS

Рисунок 42 – Рисунок 43 – Окно выбора протоколов

— нажать кнопку «СОХРАНИТЬ». Окно выбора протоколов закрывается, в строке устройства в столбце «Тип протокола» отображаются наименования выбранных протоколов (рис. 44).

Устройства			
<input type="checkbox"/>	Название	IP-адрес	Тип протокола
<input type="checkbox"/>	sw-03	10.72.7.249	TACACS+
<input checked="" type="checkbox"/>	sw-04	10.72.7.250	TACACS+ RADIUS
<input checked="" type="checkbox"/>	fake_device1	10.10.53.16	TACACS+
<input checked="" type="checkbox"/>	fake_device2	10.10.53.17	TACACS+
<input type="checkbox"/>	device 10	10.72.7.245	TACACS+
<input checked="" type="checkbox"/>	CHR1	192.168.196.129	RADIUS
<input type="checkbox"/>	CHR2	192.168.196.130	TACACS+
<input checked="" type="checkbox"/>	device 12	10.72.7.255	TACACS+ RADIUS
<input type="checkbox"/>	device_9	10.45.78.45	TACACS+
<input type="checkbox"/>	sw-02	10.72.7.248	TACACS+

Настройка по умолчанию

Рисунок 43 – Рисунок 44 – Окно списка устройств с выбранными устройствами и выбранными для них протоколами

-  Администратор имеет возможность выбрать единую настройку для всех устройств: применяемые протоколы и задать для них разделяемые ключи, для чего:
- нажать над таблицей списка кнопку «Настройка по умолчанию»;
 - задать в открывшемся окне выбора протоколов (см. рис. 43) требуемые параметры;
 - нажать кнопку «СОХРАНИТЬ».

Для всех устройств списка будут выбраны указанные в окне протоколы с заданными ключами. После чего администратор имеет также возможность внести изменения в заданную настройку для любого устройства отдельно, нажав кнопку «Редактировать» () , соответствующую устройству.

3) Нажать кнопку «ЗАГРУЗИТЬ».

Будет запущен процесс импорта данных выбранных устройств в БД ПК «Efros ACS». В процессе импорта выполняется проверка на наличие в БД ПК «Efros ACS» устройств, совпадающих с импортируемыми устройствами по названию и IP-адресу. Если совпадение:

- 4) Найдено и это устройство ранее было уже импортировано из ПК «Efros Config Inspector», то:
- обновляются данные устройства: описание и заданные в окне списка устройств протоколы;
 - устройство вносится в список успешно импортированных устройств.
- 5) Найдено, но устройство было создано в ПК «Efros ACS» администратором ранее вручную, то:
- устройство будет отмечено как дубликат;
 - устройство вносится в список устройств, при импорте которых произошла ошибка.
- 6) Не найдено, то:
- устройство будет добавлено в список устройств ПК «Efros ACS»;
 - устройство вносится в список успешно импортированных устройств.

После завершения процесса импорта открывается окно с результатами импорта (рис. 45). Окно содержит вкладки:

- «Успешно» – со списком успешно импортированных устройств;
- «Неуспешно» – со списком устройств, при импорте которых произошла ошибка.

Устройства				
УСПЕШНО: 4		НЕУСПЕШНО: 1		
Название	IP-адрес	Тип протокола	Описание	Сообщение
sw-04	10.72.7.250	TACACS+ RADIUS		Устройство успешно создано
CHR1	192.168.196.129	RADIUS		Устройство успешно создано
fake_device2	10.10.53.17	TACACS+		Устройство успешно создано
fake_device1	10.10.53.16	TACACS+		Устройство успешно создано

[ЗАКРЫТЬ](#)

Рисунок 44 – Рисунок 45 – Окно результатов импорта устройств

После завершения импорта устройств необходимо для новых устройств (и, при необходимости, для обновленных устройств) выбрать группы, в которые устройства входят, и настроить права доступа пользователей ПК «Efros ACS» к устройствам в соответствии с пунктом 3.5.

3.4.4.2. Настройка подключения ПК «Ankey SIEM»

Для выполнения настройки подключения ПК «Ankey SIEM» пользователю необходимо:

- 1) Выбрать на странице «Настройки системы» в подразделе «Интеграция с внешними системами» вкладку «Ankey SIEM». Откроется страница вкладки «Ankey SIEM» (рис. 46). Состав и описание элементов страницы приведены в таблице 8.
- 2) Установить переключатель в поле «Служба Ankey SIEM» в положение «Включена».
- 3) Ввести в поля вкладки требуемые значения.
- 4) Нажать кнопку «сохранить». После чего:
 - введенные параметры будут сохранены в БД ПК «Efros ACS»;

— пользователь ПК «Ankey SIEM» с указанными параметрами сможет выполнить запрос данных в ПК «Efros ACS».

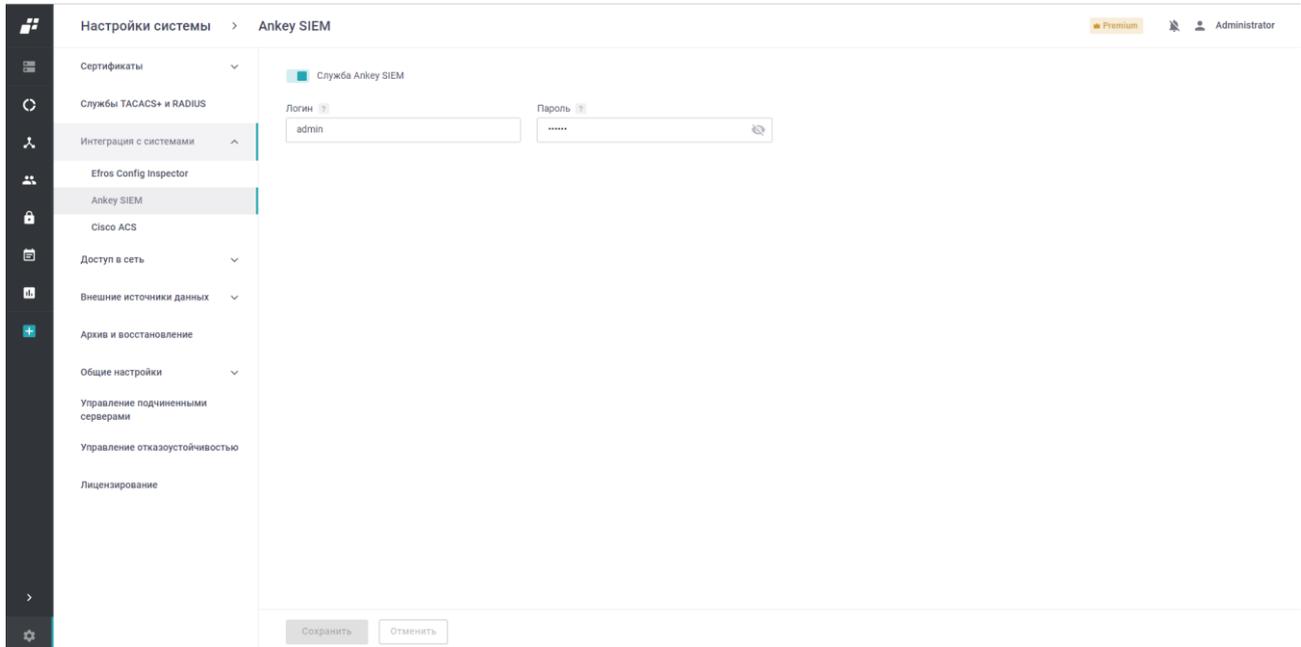


Рисунок 45 – Рисунок 46 – Страница вкладки «Ankey SIEM»

Таблица 8 – Состав и описание элементов страницы вкладки «Ankey SIEM»

Элемент	Описание
Переключатель «Служба Ankey SIEM»	<p>Переключатель с двумя положениями:</p> <ul style="list-style-type: none"> — «Включена» (☑️) – подключение к ПК «Ankey SIEM» включено; — «Выключена» (☐️) – подключение к ПК «Ankey SIEM» выключено. <p>По умолчанию установлено положение «Выключена», все параметры подключения к ПК «Ankey SIEM» (см. ниже) не заданы.</p> <p>Для администратора RO редактирование положения переключателя не доступно</p>
*Поле «Логин»	Поле для ввода имени пользователя, под которым должны выполняться запросы из ПК «Ankey SIEM»
*Поле «Пароль»	Поле для ввода пароля пользователя, под которым должны выполняться запросы из ПК «Ankey SIEM». При вводе символы пароля заменяются знаком «•». Для просмотра

Элемент	Описание
	введенного значения необходимо нажать в поле ввода кнопку «Просмотреть» (👁)
* – Справа от поля расположен знак «?», при наведении на который курсора открывается всплывающая подсказка с правилами заполнения поля	

Для отмены подключения ПК «Ankey SIEM» к ПК «Efros ACS» необходимо:

- 1) Выбрать на странице «Настройки системы» в подразделе «Интеграция с внешними системами» вкладку «Ankey SIEM».
- 2) Установить переключатель в поле «Служба Ankey SIEM» в положение «Выключена».
- 3) Нажать кнопку «СОХРАНИТЬ». После чего подключение ПК «Ankey SIEM» к ПК «Efros ACS» будет недоступно. При этом параметры подключения, установленные ранее, не удаляются и при повторном активировании подключения будут применены для установки соединения.

Все действия фиксируются в журнале событий в соответствии с таблицей 9.

Таблица 9 – Сообщения по результатам обновления параметров работы ПК «Efros ACS» с ПК «Ankey SIEM»

Объект настройки	Тип события	Сообщение	Описание
ANKEY SIEM	Инфо	Отправлены данные в ПК «Ankey SIEM»	ПК «Ankey SIEM» успешно подключился и забрал данные

3.4.4.3. Импорт данных из системы «Cisco ACS»

Для выполнения импорта данных (списков устройств или пользователей) из системы «Cisco ACS» пользователю необходимо:

- 1) Выгрузить требуемые данные из системы «Cisco ACS» в файл формата CSV.
- 2) Выбрать на странице «Настройки системы» в подразделе «Интеграция с внешними системами» вкладку «Cisco ACS». Откроется страница вкладки «Cisco ACS» (рис. 47).
- 3) Нажать кнопку «ВЫБРАТЬ ФАЙЛ».
- 4) В открывшемся стандартном окне используемой ОС выбрать файл с загружаемыми данными и нажать кнопку «ОК».

Будет запущен процесс загрузки данных, выгруженных из системы «Cisco ACS», в БД ПК «Efros ACS». В ходе загрузки проверяются параметры устройств/пользователей в БД ПК «Efros ACS»: были ли они импортированы ранее, изменились ли их данные, есть ли дубликаты (локальные записи устройств/пользователей (без отметки их импорта из системы Cisco ACS)). Дубликаты устройств определяются по названию и IP-адресу, дубликаты пользователей – по логину.

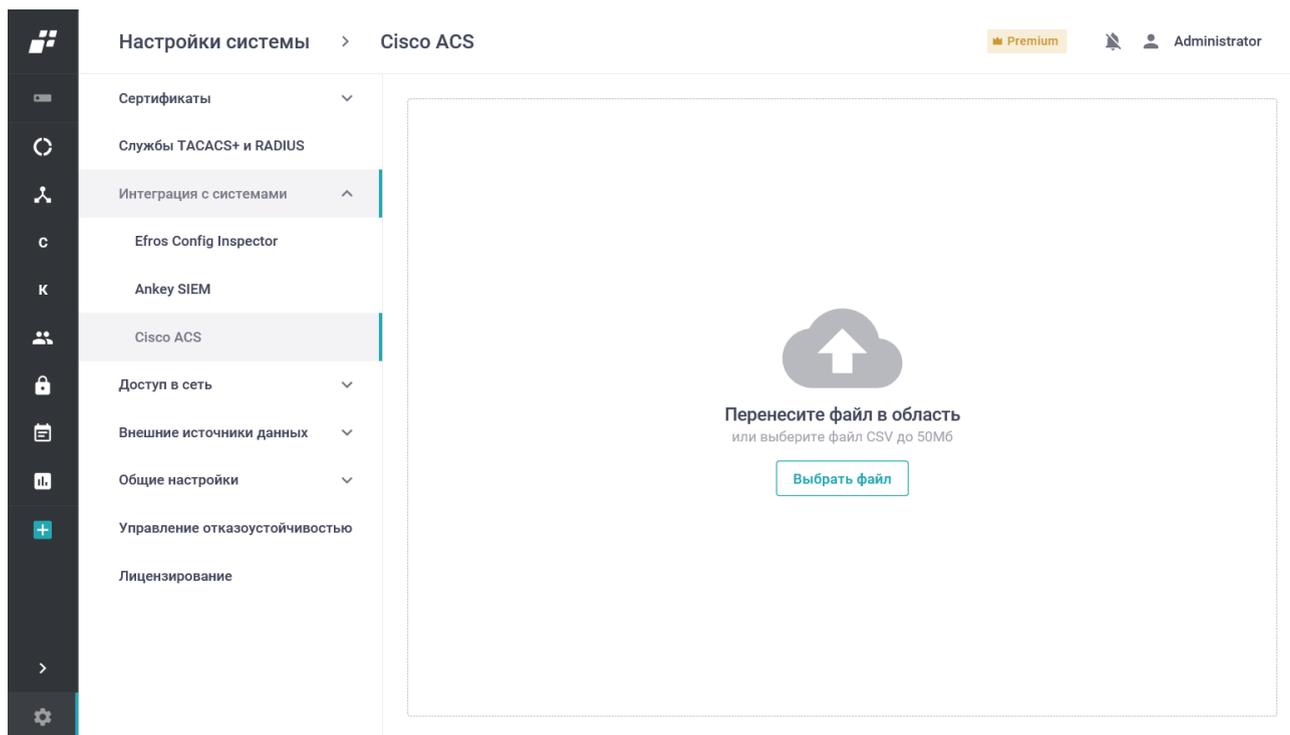


Рисунок 46 – Рисунок 47 – Страница вкладки «Cisco ACS»

После завершения проверки открывается окно результатов проверки. Окно содержит вкладки:

- «Успешно» – со списком устройств/пользователей, прошедших проверку успешно;
- «Неуспешно» – со списком устройств/пользователей, при проверке которых выявлено наличие дубликата.

На рис. 48 приведено окно результатов проверки при загрузке списка устройств. Во вкладке «Успешно» для каждой записи указывается сообщение о возможности ее добавления или обновления, во вкладке «Неуспешно» – сообщение «Устройство/Пользователь уже существует в системе».

Устройства					
		УСПЕШНО: 2	НЕУСПЕШНО: 0		
<input type="checkbox"/>	Название	Список ip адресов / диапазонов	Тип протокола	Описание	Сообщение
<input type="checkbox"/>	Device1	1.1.1.1	TACACS+ RADIUS	Device2	Устройство будет создано
<input type="checkbox"/>	Device2	192.168.0.0/24;10.7.10.0/8	TACACS+ RADIUS	Device2	Устройство будет создано

Рисунок 47 – Рисунок 48 – Окно результатов импорта устройств из системы «Cisco ACS»

Далее необходимо выбрать устройства/пользователей, импортируемых в ПК «Efros ACS», для чего:

- 1) Установить флаг в полях левого столбца списка, соответствующих импортируемым устройствам/пользователям.
- 2) Нажать кнопку «ЗАГРУЗИТЬ».

Будет запущен процесс импорта данных выбранных устройств/пользователей в БД ПК «Efros ACS». В процессе импорта выполняется корректировка списка (добавление, обновление данных) устройств/пользователей ПК «Efros ACS». При обновлении устройств обновляются их описание и поддерживаемые протоколы, при обновлении пользователей – описание.

Все действия фиксируются в журнале событий в соответствии с таблицей 10.

Таблица 10 – Сообщения по результатам обновления параметров работы ПК «Efros ACS» с системой «Cisco ACS»

Объект настройки	Тип события	Сообщение	Описание
ИМПОРТ	Ошибка	Произошла ошибка при загрузке файла	При загрузке файла, содержащего импортируемые объекты из

Объект настройки	Тип события	Сообщение	Описание
		импорта из Cisco ACS – {текст_ошибки}	системы Cisco ACS, произошла ошибка. Описание ошибки указывается в {текст_ошибки}
		При сохранении пользователей Cisco ACS произошла ошибка – {текст_ошибки}	При сохранении пользователей, импортированных из системы Cisco ACS, произошла ошибка. Текст ошибки указывается в {текст_ошибки}
		При сохранении устройств Cisco ACS произошла ошибка: – {текст_ошибки}	При сохранении устройств, импортированных из системы Cisco ACS, произошла ошибка. Текст ошибки указывается в {текст_ошибки}

После завершения импорта данных необходимо для добавленных:

- устройств – выбрать группы, в которые устройства входят, и настроить права доступа пользователей ПК «Efros ACS» к устройствам в соответствии с п. 3.7;
- пользователей ПК «Efros ACS» – выбрать группы, в которые пользователи входят, и настроить права доступа к АСО, контролируемым ПК «Efros ACS», в соответствии с п. 3.6.

3.4.5. Настройка доступа в сеть

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

После завершения редактирования и сохранения измененных параметров настройки:

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

3.4.5.1. Настройка EAP

Для выполнения настройки EAP пользователю необходимо:

- 1) Выбрать на странице «Настройки системы» в подразделе «Доступ в сеть» вкладку «Настройки EAP». Откроется страница вкладки «Настройки EAP» (рис. 49). Состав и описание полей страницы приведены в таблице 11.
- 2) Выбрать используемый по умолчанию тип EAP.

- 3) Ввести в поля вкладки требуемые значения параметров:
 - время хранения данных аутентификатора между запросами и ответами на EAP-пакеты;
 - максимальное количество открытых сессий.
- 4) Нажать кнопку «Сохранить». Введенные настройки EAP будут сохранены, перезапустится служба протокола для применения новых настроек. В журнале событий «Система» будут внесены сообщения с уровнем «Инфо»: «[RADIUS] параметры применены» и «Настройки EAP сохранены».

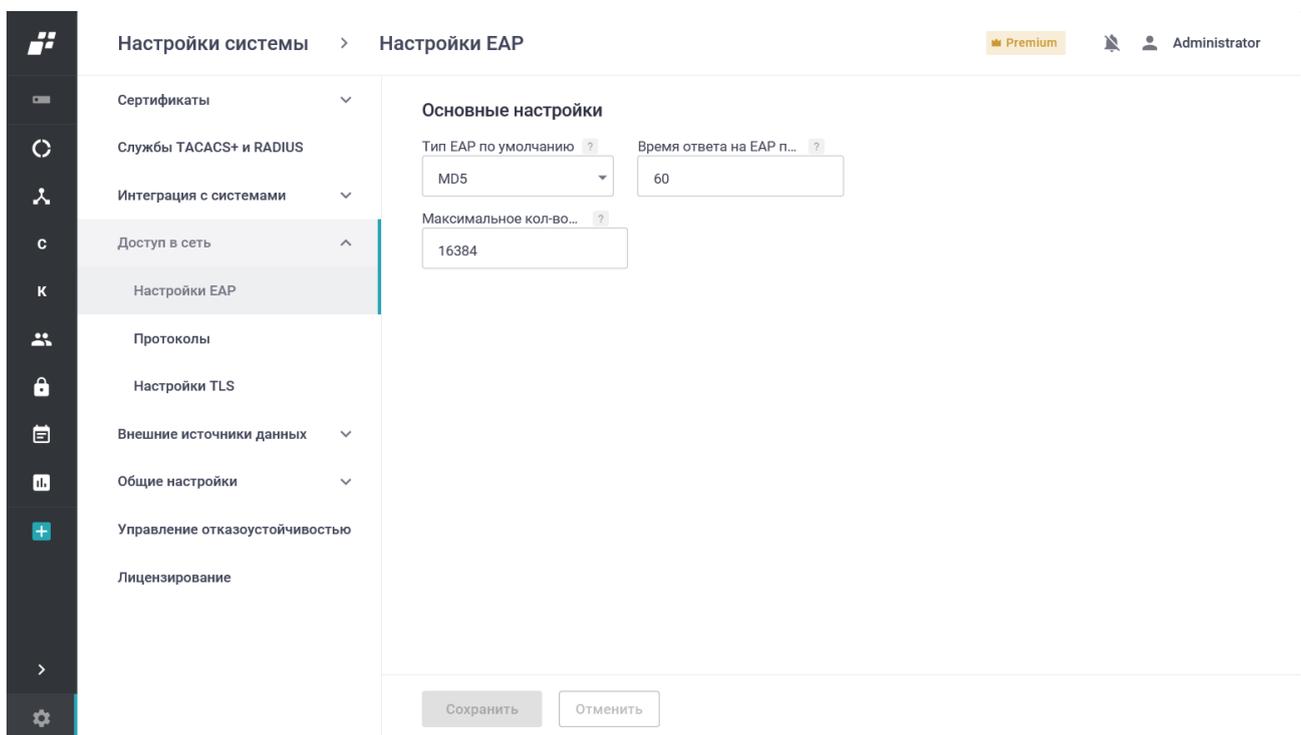


Рисунок 48 – Рисунок 49 – Страница вкладки «Настройки EAP» подраздела «Доступ в сеть»

Таблица 11 – Состав и описание полей страницы вкладки «Настройки EAP» подраздела «Доступ в сеть»

Поле	Описание
Тип EAP по умолчанию	Поле со списком для выбора типа EAP, используемого по умолчанию при получении запроса на аутентификацию от АСО. Список может содержать следующие типы EAP: MD5, PEAP, TLS, TTLS. По умолчанию выбран тип «PEAP»

Поле	Описание
Время ответа на EAP пакет	Поле для ввода времени хранения данных аутентификатора между запросами и ответами на EAP-пакеты (в секундах). По истечении заданного интервала времени данные удаляются. Допустимые значения: от 1 до 16384. Значение по умолчанию: 60
Максимальное кол-во открытых сессий	Поле для ввода максимального допустимого количества сеансов, отслеживаемых ПК «Efros ACS». Допустимые значения: от 1 до 16384. Значение по умолчанию: 16384

3.4.5.2. Настройка используемых методов EAP (протоколов)

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

- 1) Выбрать на странице «Настройки системы» в подразделе «Доступ в сеть» вкладку «Протоколы». Откроется страница вкладки «Протоколы» (рис. 50), содержащая блоки для настройки параметров используемых протоколов. Состав и описание полей блоков страницы приведены в таблице 12. В заголовке каждого блока расположен переключатель с двумя положениями:
 - «Включен» () – в ПК «Efros ACS» включена поддержка соответствующего протокола;
 - «Выключен» () – в ПК «Efros ACS» выключена поддержка соответствующего протокола.
- 2) Настроить список используемых протоколов, установкой переключателей в блоках вкладки в соответствующее положение.
- 3) Внести, при необходимости изменения в параметры отдельных протоколов, для корректировки одного протокола:
 - установить курсор в области блока требуемого протокола;
 - внести требуемые изменения в отобразившихся полях блока в соответствии с таблицей 12.
 -

 Блок «EAP-MD5» не содержит дополнительных параметров.

- 4) Нажать кнопку «Сохранить».

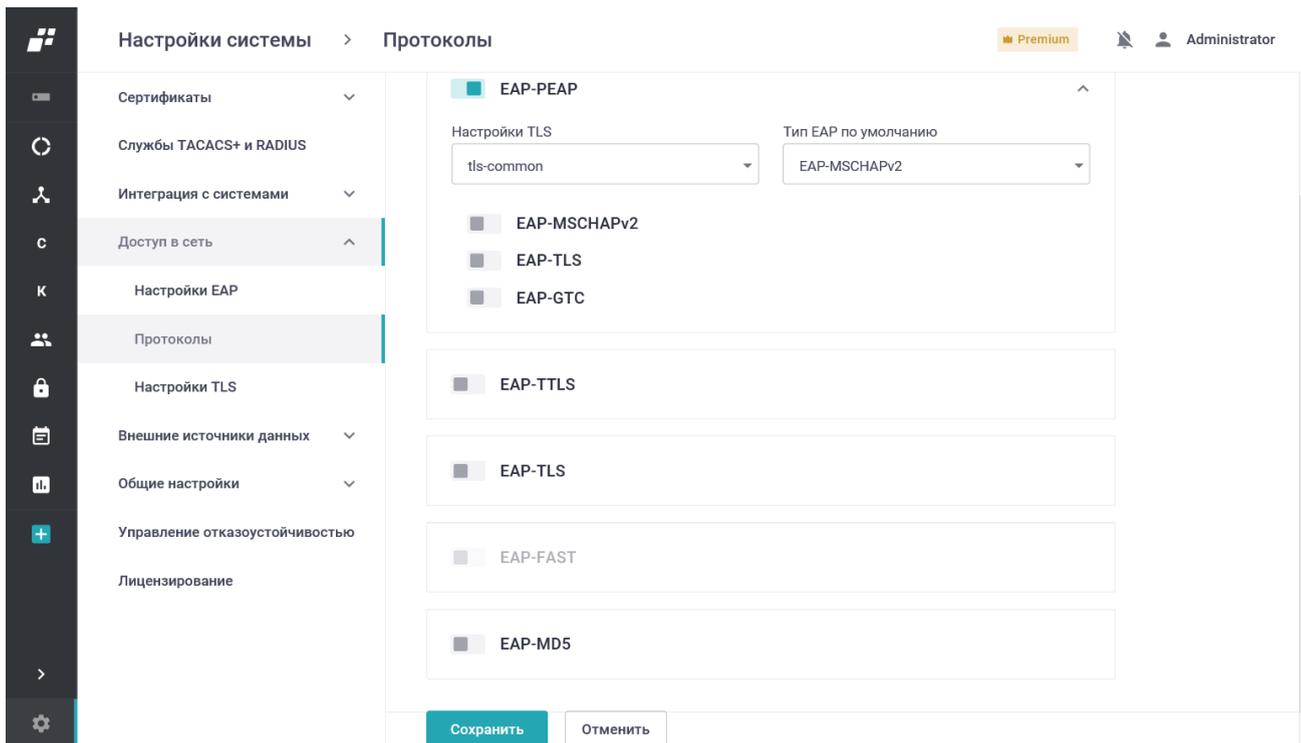


Рисунок 49 – Рисунок 50 – Страница вкладки «Протоколы» подраздела «Доступ в сеть»

Таблица 12 – Состав и описание полей страницы вкладки «Протоколы» подраздела «Доступ в сеть»

Поле	Описание
Блок «EAP-PEAP»	
Настройки TLS	Поле со списком для выбора используемой конфигурации TLS. Список содержит наименования конфигураций в соответствии со списком вкладки «Настройки TLS» подраздела «Доступ в сеть»
Тип EAP по умолчанию	Поле со списком для выбора типа EAP, используемого методом по умолчанию при получении запроса на аутентификацию от АСО. Список содержит следующие типы EAP: GTC, TLS, MSCHAPv2. Для выбранного типа переключатель в соответствующей группе полей блока должен быть установлен в положение «Включен» (<input checked="" type="checkbox"/>) (см. ниже)
Группа полей «EAP-MSCHAPv2»	

Поле	Описание
Переключатель «Включен» (<input checked="" type="checkbox"/>) / «Выключен» (<input type="checkbox"/>)	Предназначен для включения/выключения использования соответствующего типа EAP
Идентификатор сервера	Поле для ввода/редактирования идентификатора ПК «Efros ACS»
Отправлять сообщения об ошибках клиенту	Поле для флага. При наличии в поле флага клиенту при неуспешной аутентификации отправляется сообщение об ошибке с причиной ошибки аутентификации
Группа полей «EAP-TLS»	
Переключатель «Включен» (<input checked="" type="checkbox"/>) / «Выключен» (<input type="checkbox"/>)	Предназначен для включения/выключения использования соответствующего типа EAP
Настройки TLS	Поле со списком для выбора используемой конфигурации TLS. Список содержит наименования конфигураций в соответствии со списком вкладки «Настройки TLS» подраздела «Доступ в сеть»
Группа полей «EAP-GTC»	
Переключатель «Включен» (<input checked="" type="checkbox"/>) / «Выключен» (<input type="checkbox"/>)	Предназначен для включения/выключения использования соответствующего типа EAP
Блок «EAP-TTLS»	
Настройки TLS	Поле со списком для выбора используемой конфигурации TLS. Список содержит наименования конфигураций в соответствии со списком вкладки «Настройки TLS» подраздела «Доступ в сеть»
Тип EAP по умолчанию	Поле со списком для выбора типа EAP, используемого методом по умолчанию при получении запроса на аутентификацию от АСО. Список содержит следующие типы EAP: EAP-GTC, EAP-MD5, EAP-MSCHAPv2, EAP-TLS.

Поле	Описание
	Для выбранного типа переключатель в соответствующей группе полей блока должен быть установлен в положение «Включен» () (см. ниже)
Группы полей «EAP-MSCHAPv2», «EAP-TLS» и «EAP-GTC»	Состав групп аналогичен составу групп в блоке «EAP-PEAP» (см. выше)
Блок «EAP-TLS»	
Настройки TLS	Поле со списком для выбора используемой конфигурации TLS. Список содержит наименования конфигураций в соответствии со списком вкладки «Настройки TLS» подраздела «Доступ в сеть»
Группа полей «EAP-MD5»	
Переключатель «Включен» () / «Выключен» ()	Предназначен для включения/выключения использования соответствующего типа EAP. Блок «EAP-MD5». Не содержит дополнительных параметров

3.4.5.3. Настройка конфигураций TLS

Для выполнения настройки конфигураций TLS пользователю необходимо выбрать на странице «Настройки системы» в подразделе «Доступ в сеть» вкладку «Настройки TLS». Откроется страница вкладки «Настройки TLS» (рис. 51).

Страница содержит:

- кнопку «Добавить настройки» для перехода на страницу создания новой конфигурации TLS;
- блоки созданных ранее конфигураций. Заголовок блока содержит наименование конфигурации и кнопки «Редактировать» () , «Удалить» () и кнопку управления отображением полей блока «Развернуть» () / «Свернуть» () .

При установке комплекса по умолчанию установлена одна конфигурация с названием tls-common. Пользователь имеет возможность создавать новые конфигурации, вносить изменения в имеющиеся и удалять конфигурации. Для удаления доступны только те конфигурации, которые не привязаны ни к одному из протоколов (см. п.п. 3.4.5.2).

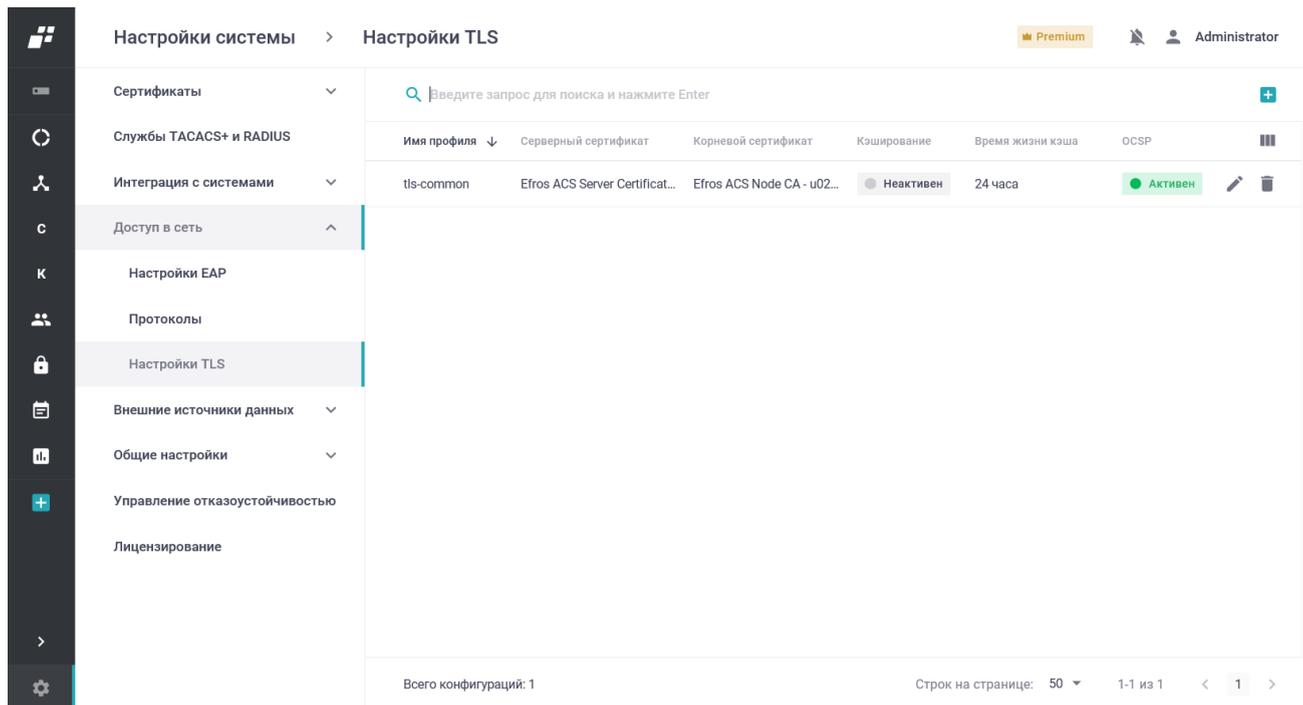


Рисунок 50 – Рисунок 51 – Страница вкладки «Настройки TLS» подраздела «Доступ в сеть»

Для создания новой конфигурации пользователю необходимо:

- 1) Нажать кнопку «Добавить настройки». Откроется страница создания новой конфигурации TLS (рис. 52). Состав и описание полей страницы приведены в таблице 13.
- 2) Заполнить поля страницы требуемыми параметрами в соответствии с таблицей 13.
- 3) Нажать кнопку «Добавить». В списке конфигураций добавится созданная конфигурации, в журнале событий «Система» будет внесено соответствующее сообщение с уровнем «Инфо», новая конфигурация будет доступна для ее выбора при настройке методов EAP на вкладке «Протоколы» (см. п.п. 3.4.5.2).

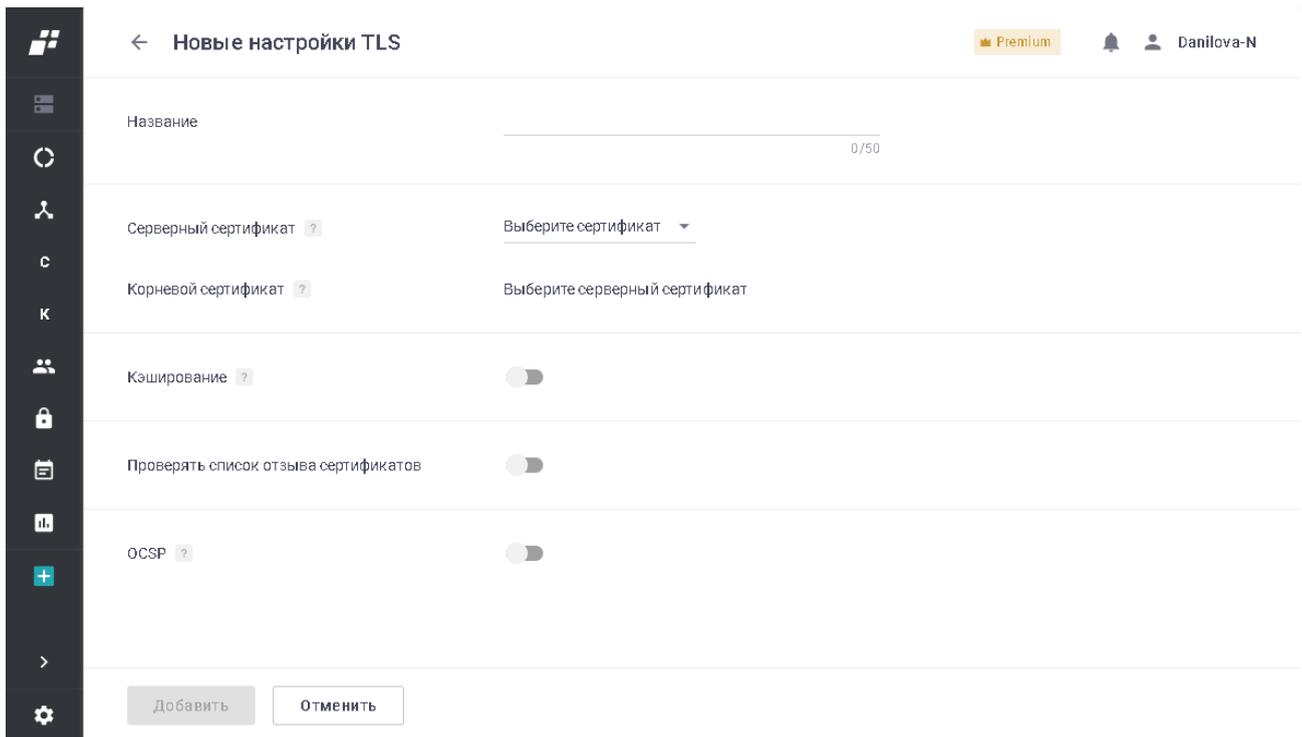


Рисунок 51 – Рисунок 52 – Страница создания новой конфигурации TLS

Таблица 13 – Состав и описание полей страницы создания новой конфигурации TLS

Поле	Описание
Название	Поле для ввода названия конфигурации. Допустимые символы: буквы латинского алфавита, цифры, «_», «-»
Серверный сертификат	Поле со списком для выбора серверного сертификата, используемого при аутентификации устройств в сети. Содержит список серверных сертификатов, включенных в список «Серверные» подраздела «Сертификаты» ПК «Efros ACS», для которых однозначно определен корневой сертификат в списке «Корневые» подраздела «Сертификаты»
Корневой сертификат	Поле заполняется автоматически после выбора серверного сертификата. Содержит название корневого сертификата, связанного с выбранным серверным сертификатом. Поле не доступно для внесения изменений в ручном режиме
Кэширование	Переключатель с двумя положениями: — «Включен» () – при восстановлении сеанса из кэша копируются атрибуты сеанса: ID сессии и имя пользователя;

Поле	Описание
	<ul style="list-style-type: none">— «Выключен» () – при восстановлении сеанса атрибуты из кэша не копируются. <p>Время хранения атрибутов сессии настраивается в поле «Время жизни кэша» (см. ниже)</p>
Время жизни кэша	<p>Поле для ввода времени хранения атрибутов сессии: ID сессии и имя пользователя (в часах).</p> <p>Допустимые значения: от 1 до 100.</p> <p>Поле отображается и доступно для редактирования только, если включен переключатель «Кэширование» (см. выше)</p>
Проверять список отзыва сертификатов	<p>Переключатель с двумя положениями:</p> <ul style="list-style-type: none">— «Включен» () – клиентские сертификаты проверяются в ПК «Efros ACS» на их наличие в списке отозванных сертификатов (CRL);— «Выключен» () – проверка не выполняется
OCSP	<p>Переключатель с двумя положениями:</p> <ul style="list-style-type: none">— «Включен» () – клиентские сертификаты проверяются в ПК «Efros ACS» с использованием протокола OCSP;— «Выключен» () – проверка не выполняется
Поля, добавляемы на страницу при включении переключателя OCSP	
Подменять URL-адреса ответчика	<p>Переключатель с двумя положениями:</p> <ul style="list-style-type: none">— «Включен» () – URL-адрес ответчика будет заменяться на значение из поля «URL-адреса ответчика OCSP» (см. ниже);— «Выключен» () – URL-адрес ответчика будет заменяться
URL-адреса ответчика OCSP	<p>Поле для ввода URL-адреса ответчика OCSP, которым должен заменяться URL-адрес ответчика.</p> <p>Поле отображается и доступно для редактирования только, если включен переключатель «Подменять URL-адреса ответчика» (см. выше)</p>
Время ожидания ответа	<p>Поле для ввода времени ожидания ответа OCSP-ответчика (в секундах)</p>

Поле	Описание
	Допустимые значения: от 0 до 100
Игнорировать ошибки	Переключатель с двумя положениями: — «Включен» () – клиенты с отозванными сертификатами смогут подключиться при недоступном ответчике OCSP; — «Выключен» () – при недоступном ответчике OCSP клиенты с отозванными сертификатами не смогут подключиться

Для редактирования конфигурации пользователю необходимо:

- 1) Нажать в блоке требуемой конфигурации кнопку «Редактировать» (). Откроется страница редактирования параметров конфигурации TLS, состав полей которой соответствует странице создания новой конфигурации (см. рис. 52).
- 2) Внести требуемые изменения в поля страницы в соответствии с таблицей 13.
- 3) Нажать кнопку «Сохранить». Внесенные изменения будут сохранены и применены, в журнале событий «Система» будет внесено соответствующее сообщение с уровнем «Инфо».

Для удаления конфигурации пользователю необходимо:

- 1) Нажать в блоке удаляемой конфигурации кнопку «Удалить» ().
- 2) Нажать в открывшемся окне подтверждения кнопку «Удалить». Конфигурация будет удалена, в журнале событий «Система» будет внесено соответствующее сообщение с уровнем «Инфо».

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

3.4.6. Настройка подключения к внешним источникам данных

3.4.6.1. Настройка подключения к LDAP-серверам

Для выполнения настройки подключения к LDAP-серверам администратору необходимо выбрать на странице «Настройки системы» в подразделе «Внешние источники данных» вкладку «LDAP». Откроется страница вкладки «LDAP» (рис. 53) со списком LDAP-серверов, подключение к которым настроено ранее.

-  После установки ПК «Efros ACS» список подключений к LDAP-серверам пуст, на странице отображается сообщение «В системе нет LDAP-серверов» и кнопка «Добавить» () для перехода на страницу добавления нового подключения к LDAP-серверу.

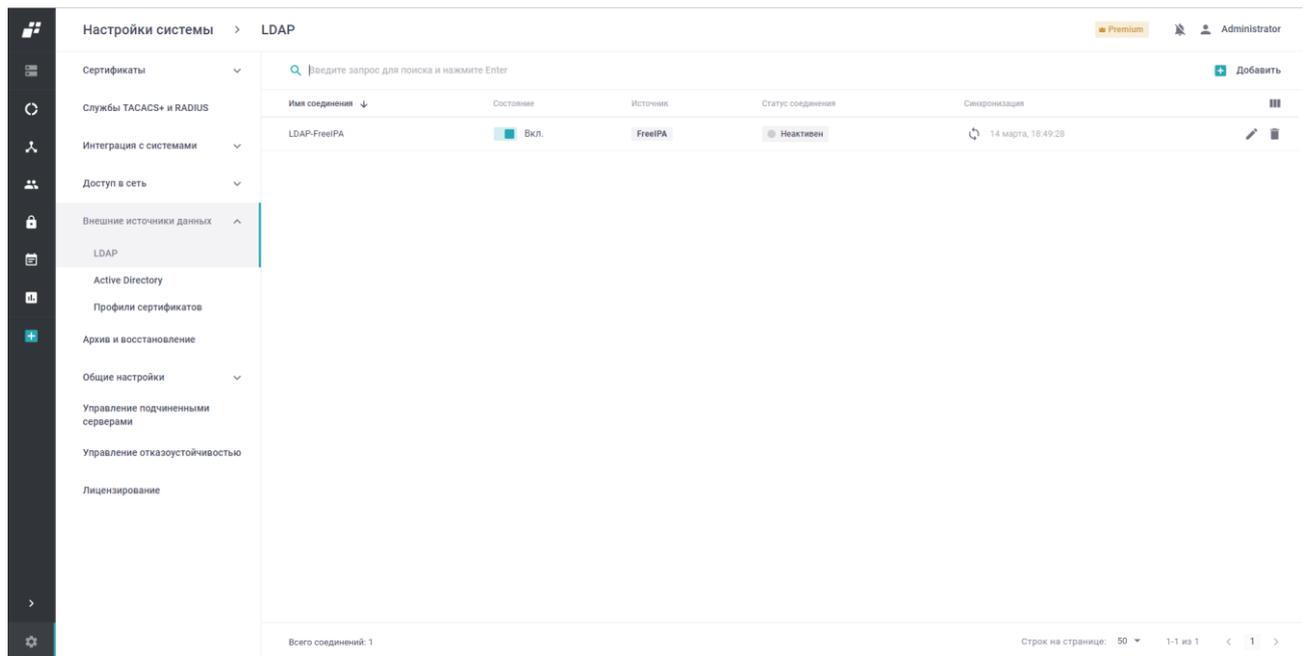


Рисунок 52 – Рисунок 53 – Страница вкладки «LDAP»

Для администраторов ACS на странице для настройки подключения к LDAP-серверам присутствуют следующие кнопки:

- «Добавить» (+) – для добавления нового подключения;
- «Изменить» (✎) – для перехода на страницу редактирования записи списка;
- «Удалить» (🗑) – для удаления соответствующей записи списка.

Для каждой записи списка отображаются данные:

- имя соединения, присвоенное при создании подключения к LDAP-серверу;
- состояние – текущее состояние подключения: «Вкл» (подключение включено) / «Выкл.» (подключение выключено). Слева расположена кнопка смены состояния подключения – в зависимости от текущего состояния кнопка имеет вид: «» (по нажатию состояние изменяется на «Выкл.»), «» (по нажатию состояние изменяется на «Вкл.»);
- источник – тип LDAP-сервера;
- статус соединения – текущий статус соединения с LDAP-сервером «Активен»/«Неактивен» (проверка соединения выполняется автоматически с периодичностью раз в три минуты);
- синхронизация – дата и время выполнения последней синхронизации данных групп пользователей и пользователей (выполняется автоматически с заданной в

форме редактирования соединения периодичностью) и кнопка запуска синхронизации вручную «↻».

Над таблицей располагается поле поиска (🔍) – для ввода последовательности символов из искомой записи. Процесс поиска запускается после ввода символов нажатием клавиши ENTER клавиатуры.

Для добавления нового соединения с LDAP-сервером администратору необходимо:

- 1) Нажать над таблицей соединений кнопку «Добавить» (+). Откроется страница добавления нового соединения, приведенная на рис. 54. Состав и описание элементов страницы приведены в таблице 14.

← Новое соединение Premium Danilova-N

Имя соединения ? Статус ?
Вкл. Выкл.

Основные настройки

Тип источника ? Домен или IP-адрес ?
Active Directory FreeIPA

База пользователей ? База групп ? SSL ?
Вкл. Выкл.

Частота обновлен... ?
48

Авторизация

Логин ? Пароль ?

Проверить соединение

Схема атрибутов

Схема ?
Active Directory Показать настройки

Добавить Отменить

Рисунок 53 – Рисунок 54 – Страница добавления нового соединения с LDAP-сервером

Таблица 14 – Состав и описание элементов страницы добавления нового соединения с LDAP-сервером

Элемент	Описание
*Поле «Имя соединения»	Текстовое поле для ввода наименования соединения с LDAP-сервером в ПК «Efros ACS» (до 50 символов) Допустимые символы: латинские буквы, цифры и символы "_", "-"
*Поле «Статус соединения»	Содержит кнопки: — «Вкл» – для включения соединения; — «Выкл.» – для выключения соединения. По умолчанию нажата кнопка «Вкл» – после нажатия кнопки «Добавить» соединение с заданными параметрами будет включено
Группа полей «Основные настройки»	
* Поле «Тип источника»	Содержит кнопки выбора типа подключаемого LDAP-сервера: — «Active Directory»; — «FreeIPA». По умолчанию выбран тип «Active Directory»
*Поле «Домен или IP»	Поле для ввода имени или IP-адреса домена установки LDAP-сервера, с которым настраивается соединение
*Поле «База пользователей»	Поля для ввода фильтра запрашиваемых данных в БД LDAP-сервера (пользователей и групп пользователей).
*Поле «База групп»	По умолчанию поля не заполнено и поиск данных выполняется в полной базе LDAP-сервера
*Поле «SSL»	Содержит кнопки: — «Вкл» – подключение к LDAP-серверу выполняется с использованием протокола SSL; — «Выкл.» – подключение к LDAP-серверу выполняется без использования протокола SSL По умолчанию протокол SSL для подключения LDAP-серверу не используется, нажата кнопка «Выкл.».

Элемент	Описание
*Поле «Сертификат»	Поле со списком для выбора сертификата, который должен использоваться при подключении к LDAP-серверу по SSL. Список содержит наименования корневых сертификатов из списка «Корневые» подраздела «Сертификаты» ПК «Efros ACS». Поле отображается на странице только после нажатия в поле «SSL» кнопки «Вкл»
*Поле «Частота обновления, час»	Числовое поле для ввода интервала запроса из ПК «Efros ACS» на обновление данных из LDAP-сервера (в часах). По умолчанию содержит значение 48 и с периодичностью в 48 часов выполняется автоматическое обновление данных
Группа полей «Авторизация»	
*Поле «Логин»	Поле для ввода имени пользователя, под которым выполняется подключение к LDAP-серверу. Допустимый формат ввода для пользователя с именем «acs», зарегистрированного на сервере TOR: TOR\acs
*Поле «Пароль»	Поле для ввода пароля пользователя, под которым выполняется подключение к LDAP-серверу. При вводе символы пароля заменяются знаком «●». Для просмотра введенного значения необходимо нажать в поле ввода кнопку «Просмотреть» (👁)
Кнопка «Проверка соединения»	По нажатию кнопки выполняется проверка успешности установления соединения с введенными параметрами к LDAP-серверу. После завершения проверки в верхней части страницы отображается сообщение «Соединение с Active Directory активно». Если проверка завершилась с ошибкой, то сообщение «Соединение с Active Directory неактивно»; информацию о последней проведенной проверке подключения: дата и время проверки и статус проверки («Активно» или «Неактивно»)
Группа полей «Схема атрибутов».	
Предназначена для сопоставления атрибутов из LDAP с соответствующими полями в ПК «Efros ACS».	
В подзаголовке группы отображается выбранный ранее в поле «Тип источника» тип LDAP-сервера: «Active Directory» или «FreeIPA»	

Элемент	Описание
Поля атрибутов	<p>Поля отображаются на странице после нажатия в подзаголовке группы ссылки «Показать настройки». Поля содержат значения по умолчанию, при подключении нового LDAP-сервера администратору необходимо проверить их соответствие атрибутам подключаемого LDAP-сервера.</p> <p>Атрибуты пользователей:</p> <ul style="list-style-type: none"> — Идентификатор объекта; — Отображаемое имя; — Имя аккаунта; — Группы пользователя; — Сертификат. <p>Атрибуты групп:</p> <ul style="list-style-type: none"> — Идентификатор объекта; — Отображаемое имя; — Имя аккаунта; — Пользователи в группе
<p>* – Справа от поля расположен знак «», при наведении на который курсора открывается всплывающая подсказка с правилами заполнения поля</p>	

- 2) Ввести в поля страницы требуемые значения.
- 3) Включить, при необходимости, использование протокола SSL при подключении к LDAP-серверу и выбрать сертификат для подключения.
- 4) Проверить и, при необходимости, скорректировать наименования используемых в LDAP-сервере атрибутов пользователей и групп пользователей. Поля с наименованиями атрибутов раскрываются при нажатии ссылки «Показать настройки» в группе полей «Схема атрибутов».
- 5) Проверить успешность подключения к указанному LDAP-серверу, нажав кнопку «Проверить соединение».

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

6) После получения сообщения об успешном подключении, нажать кнопку «СОХРАНИТЬ».

7) После чего:

- введенные параметры будут сохранены в БД ПК «Efros ACS»;
- будет запущен процесс синхронизации с БД LDAP-сервера.

В процессе синхронизации выполняется получение данных из БД LDAP-сервера, корректировка списков пользователей и групп пользователей ПК «Efros ACS». Все действия фиксируются в журнале событий в соответствии с таблицей 15.

Таблица 15 – Сообщения по результатам обновления параметров работы ПК «Efros ACS» с LDAP-сервером

Объект настройки	Тип события	Сообщение	Описание
LDAP-СЕРВЕР	Инфо	Начинается получение списка пользователей	Сервис интеграции с LDAP-сервером подключился к серверу и начал загрузку пользователей в ПК «Efros ACS»
		Получено и синхронизировано {n} пользователей LDAP-сервера	Сервис интеграции успешно синхронизировал данные о пользователях LDAP-сервера и внес изменения в ПК «Efros ACS»
		Начинается получение списка групп пользователей	Сервис интеграции с LDAP-сервером подключился к серверу и начал загрузку информации о группах пользователей LDAP-сервера в ПК «Efros ACS»
		Получено и синхронизировано N групп пользователей LDAP-сервера	Сервис интеграции успешно синхронизировал данные о группах пользователей LDAP-сервера и внес изменения в ПК «Efros ACS»
		Затраченное на синхронизацию время: 00:00:01	Отображает время, затраченное сервисом интеграции с LDAP-сервером на синхронизацию

Объект настройки	Тип события	Сообщение	Описание
		(часы:минуты: секунды)	
		Начинается связывание групп пользователей LDAP-сервера и пользователей LDAP-сервера	Связывание групп пользователей и пользователей, полученных из LDAP-сервера
		LDAP service: disconnected	Сервис интеграции с LDAP-сервером разорвал соединение с LDAP-сервером
	Предупреждение	Не удалось установить связи групп LDAP-сервера с пользователями	Сервису интеграции с LDAP-сервером не удалось связать пользователей и группы пользователей, полученные из LDAP-сервера
		Host not found for connect to LDAP	Сервису интеграции с LDAP-сервером не удалось подключиться к LDAP-серверу
	Ошибка	Произошла ошибка при синхронизации: {текст_ошибки}	При попытке синхронизации с LDAP-сервером произошла неизвестная ошибка. Ее описание указывается в {текст_ошибки}
		Не удалось обновить конфигурацию протоколов: {текст_ошибки}	После синхронизации данных с LDAP-сервером сервису интеграции не удалось обновить конфигурации протоколов
		Не удалось актуализировать группы пользователей: {текст_ошибки}	При синхронизации групп LDAP-сервера произошла ошибка, в результате которой не удалось синхронизировать существующие в системе группы, связанные с LDAP-сервером

Объект настройки	Тип события	Сообщение	Описание
		Не удалось удалить отсутствующие в LDAP-сервере группы пользователей	После синхронизации в системе были обнаружены группы, отсутствующие в LDAP-сервере. При попытке их удаления произошла ошибка
		Не удалось актуализировать пользователей: {текст_ошибки}	При синхронизации пользователей LDAP-сервера произошла ошибка, в результате которой не удалось синхронизировать существующих в системе пользователей, связанных с LDAP-сервером

Для отмены подключения к LDAP-серверу необходимо:

- 1) Выбрать на странице «Настройки системы» в подразделе «Внешние источники данных» вкладку «LDAP».
- 2) Установить переключатель в поле «Состояние» в положение «Выкл.».
- 3) После чего подключение к LDAP-серверу будет выключено. При этом параметры подключения, установленные ранее, не удаляются и при активировании подключения к LDAP-серверу будут применены для установки соединения.

3.4.6.2. Настройка подключения к серверам аутентификации

Для выполнения настройки подключения к серверам аутентификации (доменам AD) администратору необходимо выбрать на странице «Настройки системы» в подразделе «Внешние источники данных» вкладку «Active Directory». Откроется страница вкладки «Active Directory» (рис. 55) со списком доменов AD, подключение к которым настроено ранее.

Примечание. После установки ПК «Efros ACS» список подключений к доменам AD пуст, на странице отображается сообщение «В системе нет AD» и кнопка «Добавить» () для перехода на страницу добавления нового подключения к домену AD.

Для администраторов ACS на странице для настройки подключения к доменам AD присутствуют следующие кнопки:

- «Добавить» () – для добавления нового подключения;

- «Изменить» (✎) – для перехода на страницу редактирования записи списка;
- «Удалить» (🗑) – для удаления соответствующей записи списка.

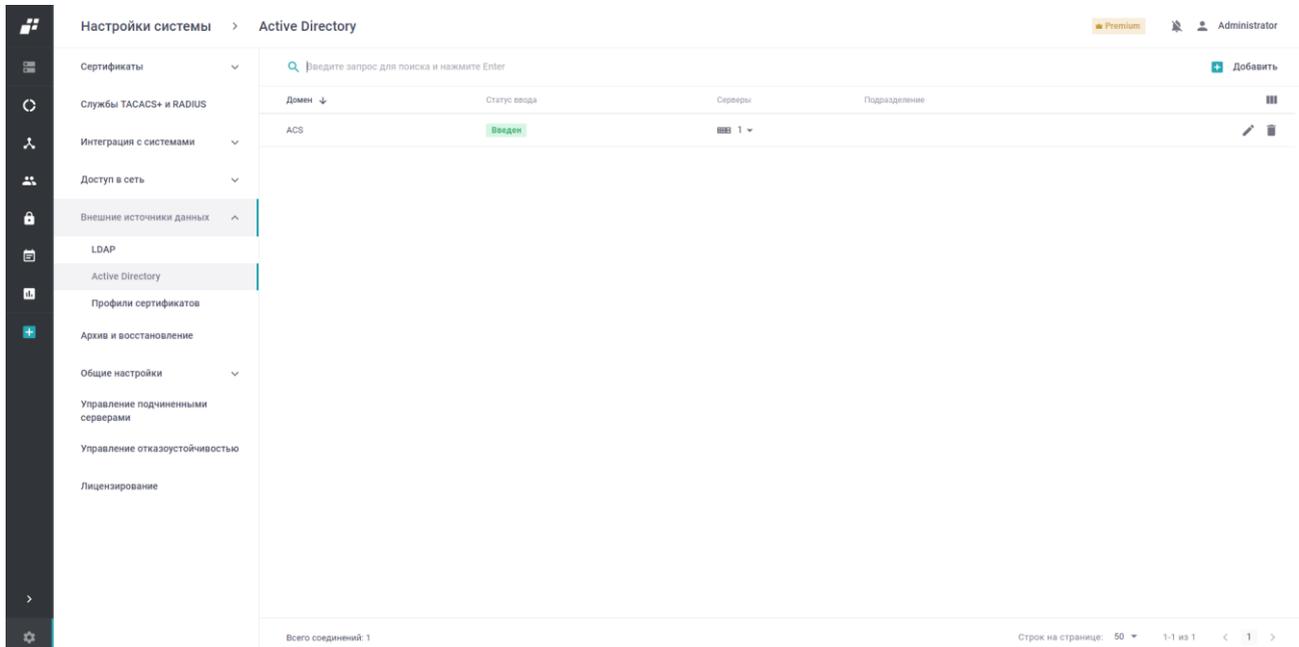


Рисунок 54 – Рисунок 55 – Страница вкладки «Active Directory»

Для каждой записи списка отображаются данные:

- домен – имя соединения, присвоенное при создании подключения к домену AD;
- статус ввода – статус ввода ПК «Efros ACS» в домен («Введен» или «Не введен»);
- серверы – количество серверов аутентификации в домене. Является ссылкой, при выборе которой открывается окно просмотра наименований серверов (см. рис. 54);
- подразделение – учетная запись сервера ПК «Efros ACS» в определенном подразделении.

Над таблицей располагается поле поиска (🔍) – для ввода последовательности символов из искомой записи. Процесс поиска запускается после ввода символов нажатием клавиши ENTER клавиатуры.

Для выполнения настройки подключения к домену AD администратору необходимо:

- 1) Нажать над таблицей соединений кнопку «Добавить» (+). Откроется страница добавления нового соединения, приведенная на рис. 56. Состав и описание элементов страницы приведены в таблице 16.

Рисунок 55 – Рисунок 56 – Страница добавления соединения с доменом AD

Таблица 16 – Состав и описание элементов страницы соединения с доменом AD

Элемент	Описание
Группа полей «Основные настройки»	
Поле «Имя соединения»	Текстовое поле для ввода наименования соединения с доменом AD в ПК «Efros ACS» (до 50 символов) Допустимые символы: латинские буквы, цифры и символы " ", "_"
Поле «Домен или IP»	Поле для ввода имени или IP-адреса домена, к которому подключается сервер ПК «Efros ACS»
Поле «Подразделение (OU)»	Поле для ввода учетной записи сервера ПК «Efros ACS» в определенном подразделении. Строка OU читается сверху вниз без относительных уникальных имён и разделяется символом «/». Например, «Computers/Servers/Unix»
Поле «Серверы аутентификации»	Поле для ввода данных (имени или IP-адреса) одного или нескольких серверов, являющихся серверами аутентификации в домене

Элемент	Описание
	По умолчанию содержит одну строку для ввода данных одного сервера. Для добавления новой строки в поле необходимо нажать кнопку «Добавить» (+)
<p>Группа полей «Ввод в домен».</p> <p>Поля группы активны только после успешного создания подключения (после сохранения введенных выше параметров по нажатию кнопки «СОХРАНИТЬ» без появления сообщений об ошибках).</p> <p>Справа от заголовка группы отображается текущий статус ввода ПК «Efros ACS» в домен:</p> <ul style="list-style-type: none">— «Не введен» – до ввода сервера ПК «Efros ACS» в домен;— «Введен» – после успешного ввода в домен;— «В процессе ввода» – в процессе ввода сервера ПК «Efros ACS» в домен (после нажатия кнопки «Вести в домен» (см. ниже))	
Поле «Логин»	Поле для ввода имени пользователя, под которым выполняется подключение к домену. Допустимый формат ввода для пользователя с именем «acs», зарегистрированного на сервере TOR: TOR\acs
Поле «Пароль»	Поле для ввода пароля пользователя, под которым выполняется подключение к домену. При вводе символы пароля заменяются знаком «●». Для просмотра введенного значения необходимо нажать в поле ввода кнопку «Просмотреть» (👁)
Кнопка «Ввести в домен»/ «Вывести из домена»	Если сервер ПК «Efros ACS» не введен в домен отображается кнопка «Ввести в домен». Если сервер ПК «Efros ACS» введен в домен – кнопка «Вывести из домена»
Поле «Группы доменов»	Поле со списком для выбора групп домена, которые могут быть использованы при настройке правил авторизации в подразделе «Наборы политик» раздела «Политики доступа» ПК «Efros ACS» (будут доступны для выбора в списке значения атрибута «AdDomainGroups->Name»). <p>По умолчанию в списке не выбрана ни одна группа</p>

- 2) Ввести в поля вкладки требуемые значения в соответствии с правилами, приведенными в таблице 16.
- 3) Нажать кнопку «Добавить». По нажатию кнопки выполняется проверка успешности установления соединения с введенными параметрами к указанному домену и серверам аутентификации.

4)

 Если проверка завершилась сообщением об ошибке, внести, при необходимости, поправки в введенные параметры и вновь проверить успешность установления соединения.

5) После получения сообщения об успешном завершении проверки станут активны поля группы «Ввод в домен, кнопка «Добавить» заменится кнопкой «Сохранить».

6) Далее для:

- выхода из режима создания соединения без ввода ПК «Efros ACS» в домен – нажать кнопку «Отменить». Откроется страница вкладки «Active Directory», в списке соединений с доменами AD добавится запись с данными, введенными на шаге 2;
- ввода ПК «Efros ACS» в домен – ввести в соответствующие поля группы полей «Ввод в домен» логин и пароль пользователя, под которым запущен ПК «Efros ACS», сохранить или отменить установкой флага в поле «Сохранить учетные данные» и нажать кнопку «Ввести в домен». Будет запущен процесс ввода сервера в домен, в заголовке группы полей будет отображаться текст «В процессе ввода»

7) После получения сообщения об успешном завершении ввода сервера в домен:

- все параметры подключения к серверу аутентификации станут не доступны для внесения изменений;
- в заголовке группы полей «Ввод в домен» 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». При этом параметры подключения, установленные ранее, не удаляются и могут быть применены для повторного ввода сервера в домен или изменены.

Все действия пользователей фиксируются в журнале событий.

3.4.6.3. Ведение списка профилей сертификатов

Для ведения списка профилей сертификатов администратору необходимо выбрать на странице «Настройки системы» в подразделе «Внешние источники данных» вкладку «Профили сертификатов». Откроется страница вкладки «Профили сертификатов» (рис. 57) со списком созданных ранее профилей.

 После установки ПК «Efros ACS» список профилей сертификатов пуст, на странице отображается сообщение «В системе нет профилей сертификатов» и кнопка «Добавить» () для перехода на страницу добавления нового профиля сертификата.

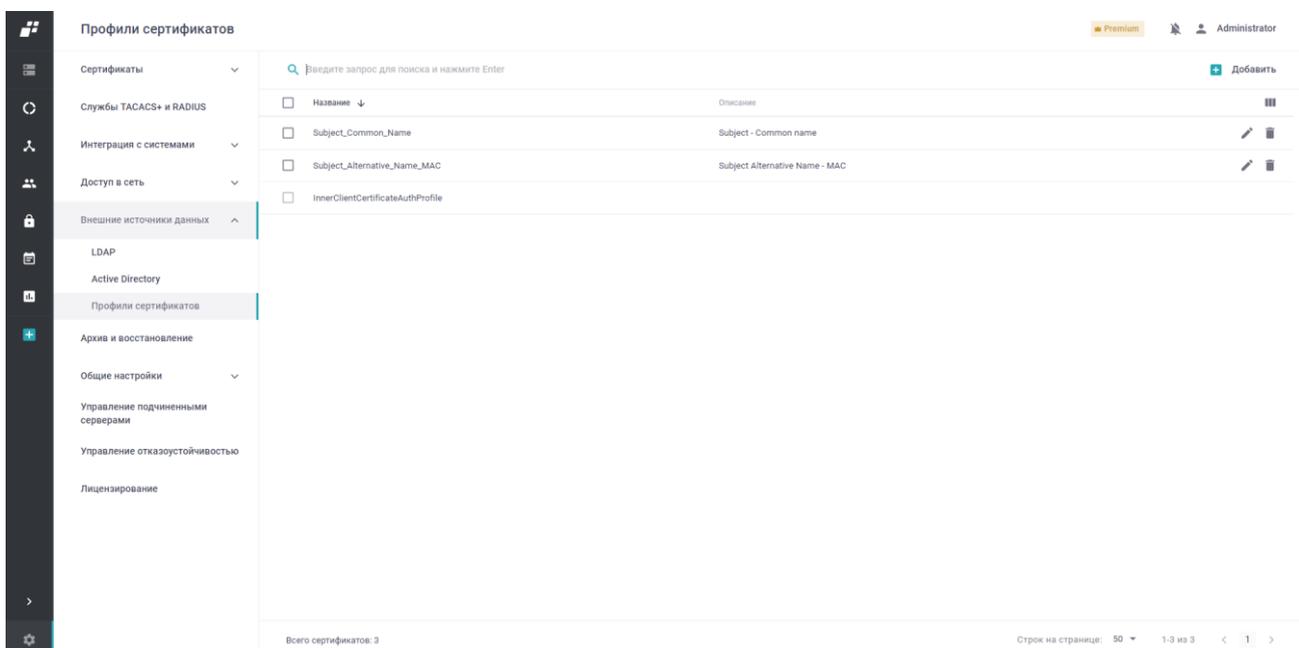


Рисунок 56 – Рисунок 57 – Страница вкладки «Профили сертификатов»

Для администраторов ACS на странице доступны кнопки:

- «Добавить» () – для добавления нового профиля сертификатов;
- «Изменить» () – для перехода на страницу редактирования записи списка;
- «Удалить» () – для удаления соответствующей записи списка.

Для каждой записи списка отображаются название и описание.

Над таблицей располагается поле поиска () – для ввода последовательности символов из искомой записи. Процесс поиска запускается после ввода символов нажатием клавиши ENTER клавиатуры.

Для добавления в список нового профиля сертификатов администратору необходимо:

- 1) Нажать над таблицей профилей кнопку «Добавить» (+). Откроется страница добавления нового профиля сертификатов, приведенная на рис. 58. Состав и описание элементов страницы приведены в таблице 17.

Рисунок 57 – Рисунок 58 – Страница добавления профиля сертификата

Таблица 17 – Состав и описание элементов страницы добавления профиля сертификата

Элемент	Описание
Поле «Название»	Текстовое поле для ввода названия профиля сертификата в ПК «Efros ACS» (до 50 символов) Допустимые символы: латинские буквы, цифры и символы "_", "-"
Кнопка «Добавить описание»	По нажатию кнопки на странице дополнительно отображается поле «Описание» – текстовое поле для ввода описания профиля сертификата в ПК «Efros ACS» (до 250 символов). Под полем отображается кнопка «Удалить описание», по нажатию которой поле «Описание» очищается и удаляется
Группа полей «Основные настройки»	

Элемент	Описание
Поле «Источник данных»	Поле со списком для выбора протокола аутентификации. Список доступных для выбора протоколов зависит от текущих настроек комплекса (наличие подключения внешних источников данных)
Поле «Данные из атрибута сертификата»	Поле со списком атрибутов выбранного источника данных для выбора атрибута, значение которого будет использовано в качестве имени пользователя для поиска в протоколе аутентификации

2) Ввести в поля вкладки требуемые значения в соответствии с правилами, приведенными в таблице 17.

3) Нажать кнопку «Добавить».

Будет запущен процесс проверки заполненности всех обязательных полей и уникальности добавляемого профиля по наименованию.

При обнаружении незаполненных обязательных полей рядом с первым из таких полей отобразится всплывающая подсказка «Обязательное поле», в случае обнаружения в списке дубликата профиля сертификатов в верхней части страницы отобразится соответствующее сообщение. Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Добавить».

Если проверки завершились без обнаружения ошибок, то открывается страница вкладки «Профили сертификатов», в списке профилей добавляется новый профиль, профиль становится доступен для выбора при создании/редактировании правил аутентификации наборов политик.

Далее администратор имеет возможность:

- просмотреть и отредактировать параметры профиля сертификатов, для чего необходимо нажать в строке профиля кнопку «Редактировать» () , внести требуемые изменения в поля страницы редактирования и нажать кнопку «Изменить»;
- удалить профиль – в соответствии с п. 3.2.6.

Сообщения о выполненных с профилями сертификатов действиях будут внесены в журнал событий ПК «Efros ACS».

3.4.7. Выполнение общих настроек

3.4.7.1. Настройка парольной политики

Для выполнения настройки парольной политики ПК «Efros ACS» необходимо:

- 1) Выбрать на странице «Настройки системы» в разделе «Общие настройки» подраздел «Парольные политики». Откроется страница подраздела «Парольные политики» с активной вкладкой «Администраторы» (рис. 59). Состав и описание элементов вкладок страницы приведены в таблице 18.
- 2) Ввести в поля вкладки требуемые количественные и временные параметры паролей.
- 3) Перейти, при необходимости, на вкладку «Общие настройки», изменить минимальную требуемую длину пароля и нажатием кнопок задать требуемый уровень сложности пароля.
- 4) Нажать кнопку «Сохранить». После чего введенные параметры будут сохранены в БД ПК «Efras ACS» и будут применяться при авторизации пользователей и при смене пароля.

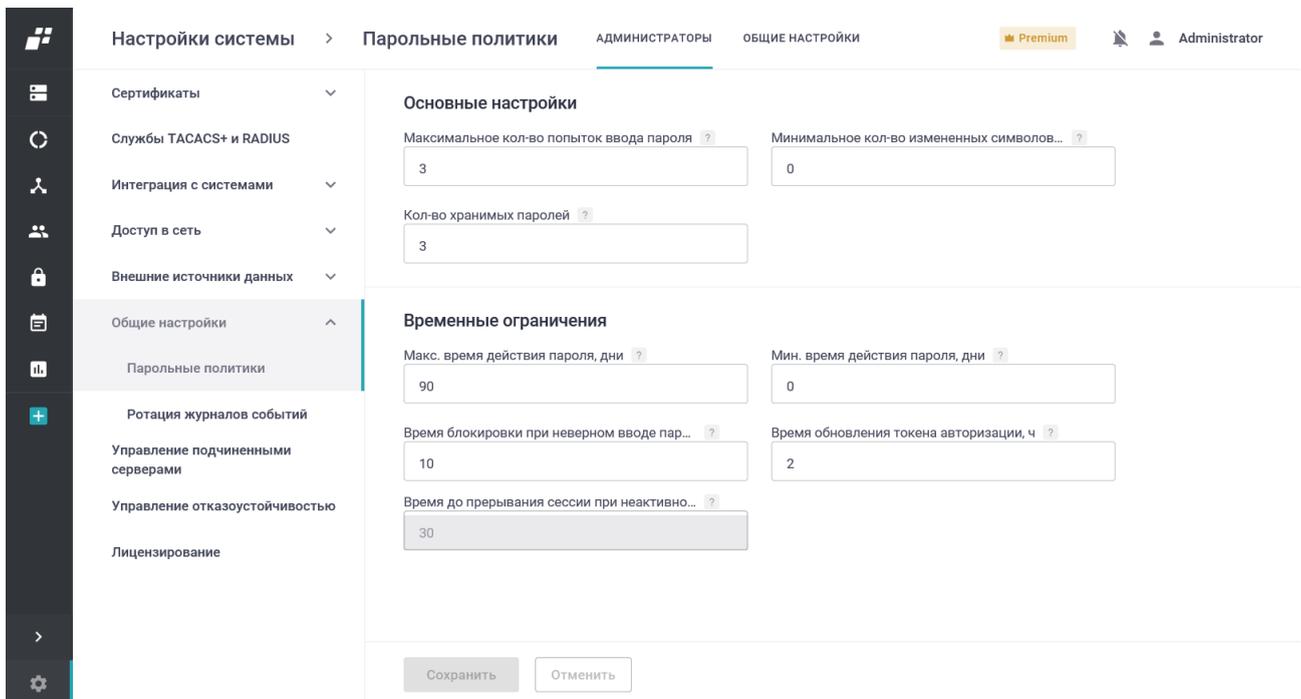


Рисунок 58 – Рисунок 59 – Страница подраздела «Парольные политики». Вкладка «Администраторы»

Таблица 18 – Состав и описание элементов страницы подраздела «Парольные политики»

Элемент	Описание
Вкладка «Администраторы»	
Группа полей «Основные настройки»	

Элемент	Описание
Поле «Максимальное кол-во попыток ввода пароля»	Числовое поле для ввода количества неуспешных попыток ввода пароля. После превышения указанного количества неуспешных попыток авторизации пользователь блокируется на время, указанное в параметре «Временные ограничения. Время блокировки при неверном вводе пароля» (см. ниже в таблице). Допустимые значения: от 3 до 8. Значение по умолчанию – 3
Поле «Кол-во хранимых паролей»	Числовое поле для ввода количества последних использовавшихся пользователем паролей. При смене пароля не допускается использование в качестве нового пароля значения, совпадающего с хранящимся в БД ПК «Efros ACS». Допустимые значения: от 0. Значение по умолчанию: 3
Поле «Минимальное кол-во измененных символов при редактировании пароля»	Числовое поле для ввода минимального количества символов, которые пользователь должен изменить в старом пароле при замене его на новый. Допустимые значения: от 0. Значение по умолчанию: 0
Группа полей «Временные ограничения»	
Поле «Максимальное время действия пароля, дн.»	Числовое поле для ввода времени (в днях) действия пароля пользователя (второго и последующих). После истечения указанного времени пароль необходимо изменить (пользователю при попытке запуска веб-приложения будет выведено соответствующее сообщение). Допустимые значения: от 0. Значение по умолчанию – 90
Поле «Минимальное время действия пароля, дн.»	Числовое поле для ввода времени (в днях) действия первого пароля пользователя (используемого им при первой авторизации в ПК «Efros ACS»). После истечения указанного времени пароль необходимо изменить (пользователю при попытке запуска веб-приложения будет выведено соответствующее сообщение). Допустимые значения: от 0. Значение по умолчанию – 0 (первый пароль пользователя должен быть изменен при первом запуске веб-приложения)
Поле «Время блокировки при»	Числовое поле для ввода интервала времени (в минутах), на который блокируется учетная запись пользователя после

Элемент	Описание
неверном вводе пароля, мин.»	превышения разрешенного количества неуспешных попыток авторизации (см. выше параметр «Основные настройки. Максимальное кол-во попыток ввода пароля»). Допустимые значения: от 10. Значение по умолчанию: 10
*Поле «Время обновления токена авторизации, час»	Числовое поле для ввода времени обновления токена авторизации (в часах). Интервал времени отсчитывается от времени закрытия веб-интерфейса ПК «Efros ACS». По истечении заданного интервала времени сессия пользователя прерывается, для продолжения работы необходимо вновь выполнить запуск веб-приложения ПК «Efros ACS» (см. п. 3.1.1). Допустимые значения: от 1 до 24. Значение по умолчанию: 10
Время до прерывания сессии при неактивности, мин	Не редактируемое поле с установленным значением в 30 минут Если в течение 30 минут пользователь будет неактивен в ПК «Efros ACS», то есть не будет взаимодействовать с веб-интерфейсом, то сессия пользователя будет заблокирована до его повторной авторизации
Вкладка «Общие настройки»	
Группа полей «Основные настройки»	
Поле «Минимальная длина пароля»	Числовое поле для ввода минимально допустимой длины пароля. Допустимые значения: от 6 до 30. Значение по умолчанию – 6
Группа кнопок «Сложность пароля»	
«Цифры»	Кнопка нажата (<input checked="" type="checkbox"/> Цифры) – пароль должен содержать хотя бы одну цифру, не нажата (<input type="checkbox"/> Цифры) – наличие в пароле цифр необязательно. По умолчанию кнопка нажата
«Буквы верхнего регистра»	Кнопка нажата – пароль должен содержать хотя бы одну букву верхнего регистра латинского алфавита; не нажата – наличие в пароле букв верхнего регистра необязательно. По умолчанию кнопка нажата
«Буквы нижнего регистра»	Кнопка нажата – пароль должен содержать хотя бы одну букву нижнего регистра латинского алфавита, не нажата – наличие в пароле букв нижнего регистра необязательно.

Элемент	Описание
	По умолчанию кнопка нажата
«Не буквенно-цифровые символы»	Кнопка нажата – пароль должен содержать хотя бы один не буквенно-цифровой символ, не нажата – наличие в пароле не буквенно-цифровых символов необязательно. По умолчанию кнопка не нажата
Примечание – Справа от полей страницы расположен знак «?», при наведении на который курсора открывается всплывающая подсказка с правилами заполнения поля	

3.4.7.2. Настройка ротации журналов событий

В ПК «Efros ACS» выполняется архивирование данных журналов событий. Данные сохраняются в каталог в файловой системе «../efros-acs_logs/_data», название файла архива формируется в формате: serverAPI.log_{dd.мм.yyyy}.zip, где «dd.мм.yyyy» – дата формирования файла архива. Файлы доступны для просмотра и анализа архивных данных. Время хранения архивных файлов ограничено.

Архивирование и удаление архивных файлов из БД ПК «Efros ACS» (далее – ротация) проводятся автоматически с заданной в настройках ПК «Efros ACS» периодичностью.

Для выполнения настройки ротации журналов событий ПК «Efros ACS» необходимо:

- 1) Выбрать на странице «Настройки системы» в разделе «Общие настройки» подраздел «Ротация журналов событий». Откроется страница подраздела «Ротация журналов событий» (рис. 60). Состав и описание элементов страницы приведены в таблице 19.
- 2) Ввести в поля страницы требуемые значения.
- 3) Нажать кнопку «Сохранить». После чего введенные параметры будут сохранены в БД ПК «Efros ACS» и будут применяться при ротации журналов событий.

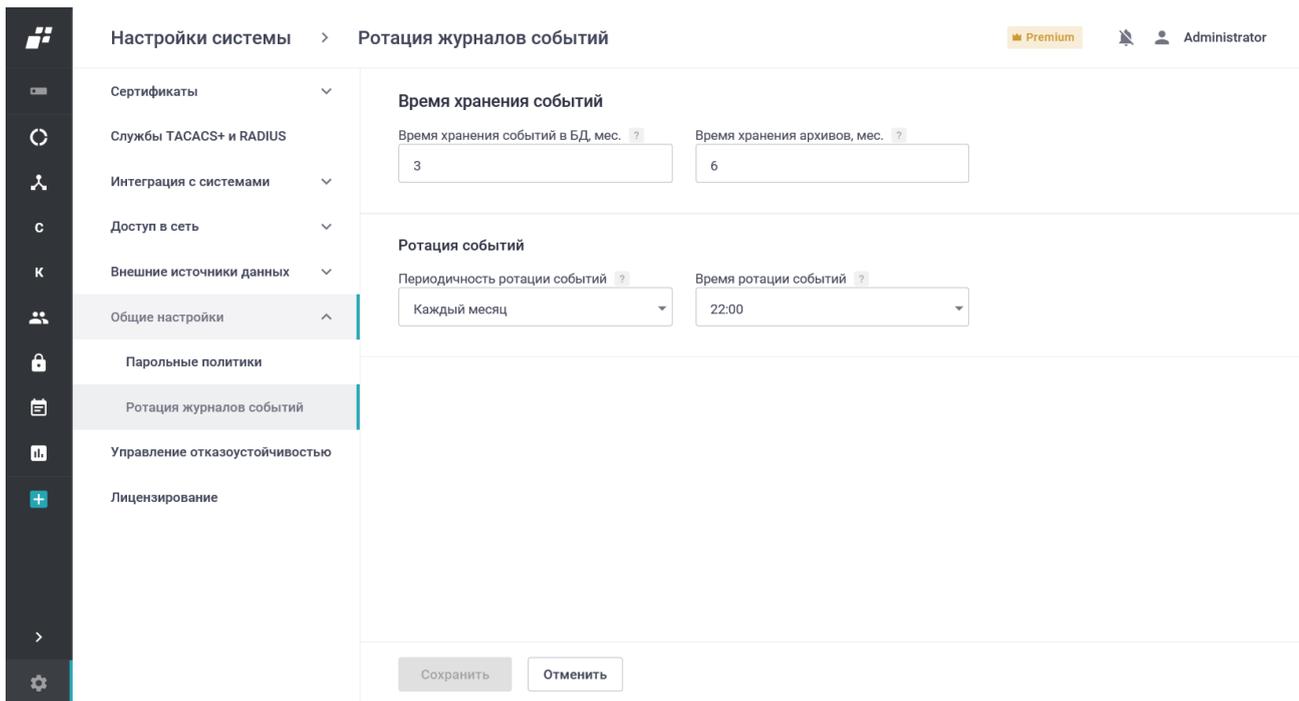


Рисунок 59 – Рисунок 60 – Страница подраздела «Ротация журналов событий»

Таблица 19 – Состав и описание элементов страницы подраздела «Парольные политики»

Элемент	Описание
Группа полей «Время хранения событий»	
Поле «Время хранения событий в БД, мес»	Числовое поле для ввода интервала времени хранения записей журналов событий в БД ПК «Efros ACS» до их архивации (в месяцах). Допустимые значения: от 1 до 12. Значение по умолчанию – 3
Поле «Время хранения архивов, мес»	Числовое поле для ввода интервала времени хранения заархивированных данных журналов событий до их удаления. Допустимые значения: от 3 до 24. Значение по умолчанию – 6
Группа полей «Ротация событий»	
Поле «Периодичность ротации событий»	Поле со списком для выбора периодичности ротации журналов событий: каждый день, каждую неделю или каждый месяц. Значение по умолчанию – «Каждый месяц»
Поле «Время ротации событий»	Поле со списком для выбора времени суток для начала ротации журналов событий. Список содержит значения от 00:00 до 23:00 с разницей в один час.

Элемент	Описание
	Значение по умолчанию – 19:00

3.4.8. Управление подчиненными серверами

Для перехода к списку подчиненных серверов текущего сервера ПК «Efros ACS» необходимо выбрать на странице «Настройки системы» раздел «Управление подчиненными серверами». Откроется страница раздела «Управление подчиненными серверами»⁹ (рис. 61).

Список серверов содержит данные главного в иерархии (основного) сервера и подчиненных серверов. Главный сервер добавляется в список автоматически после установки ПК «Efros ACS», подчиненные серверы – вручную администратором.

Для каждого сервера отображаются данные:

- название;
- статус соединения – «Активно»/«Неактивно». Статус определяется автоматически по наличию/отсутствию связи между главным сервером и соответствующим подчиненным сервером (обновление статуса выполняется автоматически с периодичностью в 15 минут);
- иерархический статус – главный или подчиненный;
- домен или IP-адрес сервера;
- описание.

Для администраторов ACS на странице доступны следующие кнопки:

- «Добавить» () – для добавления нового подчиненного сервера;
- «Изменить» () – для перехода на страницу редактирования записи списка;
- «Удалить» () – для удаления соответствующей записи списка.

 Кнопки «Изменить» и «Удалить» доступны только для подчиненных серверов.

Над таблицей располагается поле поиска () – для ввода последовательности символов из искомой записи. Процесс поиска запускается после ввода символов нажатием клавиши ENTER клавиатуры.

⁹ Данная вкладка отображается только при нахождении на главном сервере

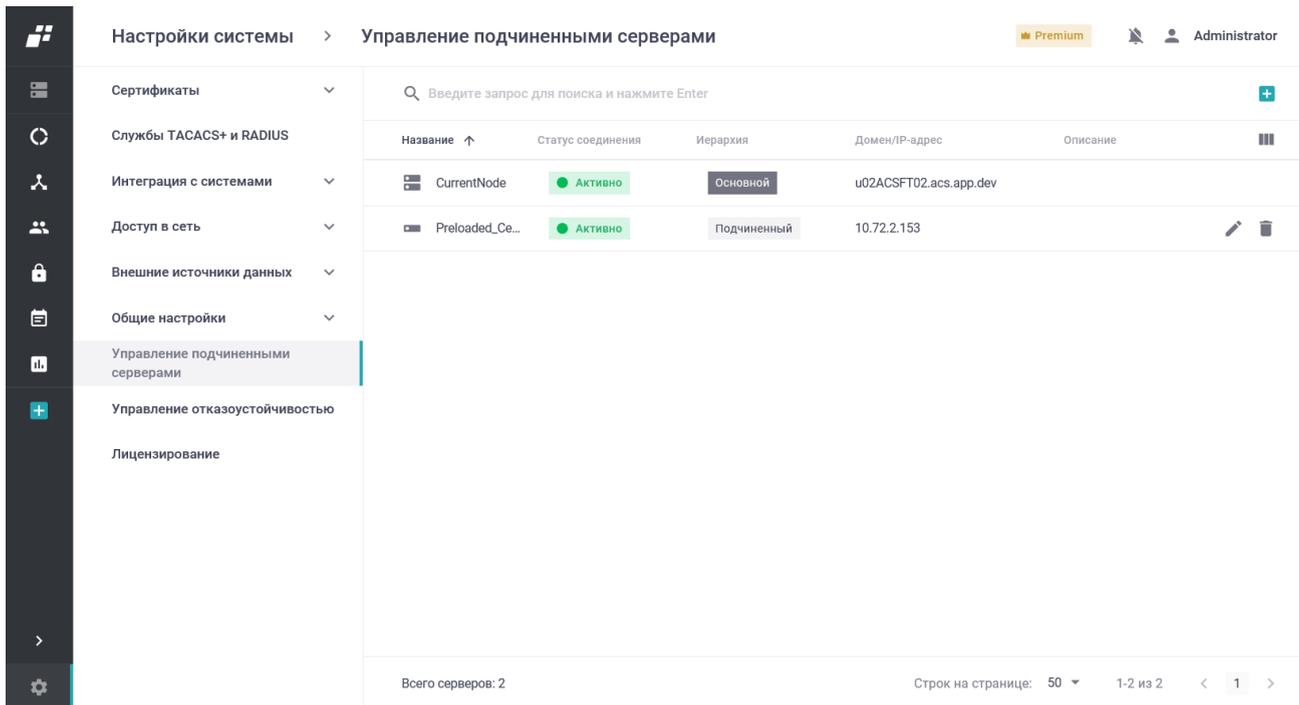


Рисунок 60 – Рисунок 61 – Страница раздела «Управление подчиненными серверами»

Для добавления нового подчиненного сервера администратору необходимо:

- 1) Нажать кнопку «Добавить» (+) над таблицей серверов. Откроется страница добавления подчиненного сервера (рис. 62). Состав и описание элементов страницы приведены в таблице 20.
- 2) Ввести в поля страницы требуемые значения.
- 3) Нажать кнопку «Сохранить». После чего введенные параметры будут сохранены в БД ПК «Efros ACS», пользователи которым назначен доступ к серверу смогут выбрать его в панели главного меню и получить доступ к настройкам сервера в соответствии с назначенным уровнем доступа.

Рисунок 61 – Рисунок 62 – Страница добавления подчиненного сервера

Таблица 20 – Состав и описание элементов страницы добавления подчиненного сервера

Элемент	Описание
*Поле «Название»	Текстовое поле для ввода названия сервера (до 50 символов)
Кнопка «Добавить описание»	По нажатию кнопки на странице дополнительно отображается поле «Описание» – текстовое поле для ввода описания сервера (до 250 символов). Под полем отображается кнопка «Удалить описание», по нажатию которой поле «Описание» очищается и удаляется
Группа полей «Основные настройки» / Поле «Домен/IP-адрес»	Поле для ввода DNS-имени или IP-адреса домена установки подчиненного сервера
Группа полей «Доступы»	Содержит поля со списком: <ul style="list-style-type: none"> — «Администратор» – для выбора из списка администраторов ПК «Efros ACS» учетной записи пользователя, которому назначается доступ к подчиненному серверу; — «Уровень доступа» – для выбора из списка возможных уровней доступа «Полный доступ» и

Элемент	Описание
	<p>«Только просмотр» уровень доступа пользователя к подчиненному серверу.</p> <p>Добавление новых пользователей в список имеющих доступ к серверу выполняется по нажатию кнопки «Добавить» (+) в строке предыдущего пользователя. Удаление неактуальных записей в списке выполняется по нажатию кнопки «Удалить» (-) в строке удаляемого пользователя.</p> <p> Доступ пользователя к подчиненному серверу может быть назначен также в карточке пользователя (см. п.п.3.9.4.2)</p>

3.4.9. Управление отказоустойчивостью

 Данный раздел доступен только при активации лицензии Premium.

 Для штатного функционирования ПК «Efras ACS» требуется полная настройка сети. Также необходимо разрешить имена серверов на контролере домена. Пример настройки DNS-сервера приведен на рис 63, 64. Создание кластера выполняется перед вводом ПК «Efras ACS» в домен.

```
Astra Linux SE 1.6 (smolensk)
tty1
vm1 login: administrator
Password:
Integrity level:
Last login: Wed Jun  1 11:07:30 MSK 2022 on tty1
administrator@vm1:~$ hostname -f
vm1.eacs.app.dev
administrator@vm1:~$ _
```

Рисунок 62 – Рисунок 63 – Пример настройки DNS-сервера для виртуальной машины vm1

Рисунок 63 –

```
Astra Linux SE 1.6 (smolensk)
tty1
vm2 login: administrator
Password:
Integrity level:
Last login: Wed Jun  1 10:55:35 MSK 2022 on tty1
administrator@vm2:~$ hostname -f
vm2.eacs.app.dev
administrator@vm2:~$ _
```

Рисунок 64 –

Рисунок 65 – Рисунок 64 - Пример настройки DNS-сервера для виртуальной машины vm2

Для создания кластеров и управления отказоустойчивостью ПК «Efros ACS» необходимо выбрать на странице «Настройки системы» раздел «Управление отказоустойчивостью». Откроется страница раздела «Управление отказоустойчивостью» (рис. 65).

The screenshot displays the 'Management of High Availability' (Управление отказоустойчивостью) settings page. The left sidebar contains a navigation menu with options like 'Certificates', 'TACACS+ and RADIUS services', 'Integration with systems', 'Network access', 'External data sources', 'General settings', 'High Availability management', and 'Licensing'. The main content area is titled 'Cluster settings' (Настройки кластера) and includes two sections: 'Cluster settings' and 'Additional node' (Дополнительный узел). Each section has input fields for 'Virtual IP address of the cluster' (Виртуальный IP-адрес кластера) and 'Domain name' (Доменное имя). The 'Cluster settings' section shows a virtual IP of 192.168.0.1/0 and a domain name field with the placeholder 'Введите доменное имя'. The 'Additional node' section shows an IP address of 192.168.0.1 and a domain name field with the placeholder 'Введите доменное имя'. At the bottom, there are two buttons: 'Build cluster' (Построить кластер) and 'Cancel' (Отменить).

Рисунок 66 – Рисунок 65 – Страница раздела «Управление отказоустойчивостью»

Кластеры создаются или удаляются в ПК «Efros ACS» вручную администраторами ACS.

- ❗ Кластер организуется из двух узлов и работает в режиме active-standby.
- ❗ На узлы предварительно должен быть установлен ПК «Efros ACS» в версии «без базы данных».
- ❗ После создания кластера необходимо выполнить настройку протоколов TACACS+ и RADIUS непосредственно на АСО.

Для создания кластера администратору необходимо:

- 1) Заполнить на странице требуемые значения (см. рис. 65). Состав и описание элементов страницы приведены в таблице 21.
- 2)
- 3)
- 4) Нажать кнопку «Построить кластер» (все введенные параметры будут сохранены в БД ПК «Efros ACS») (рис. 66).

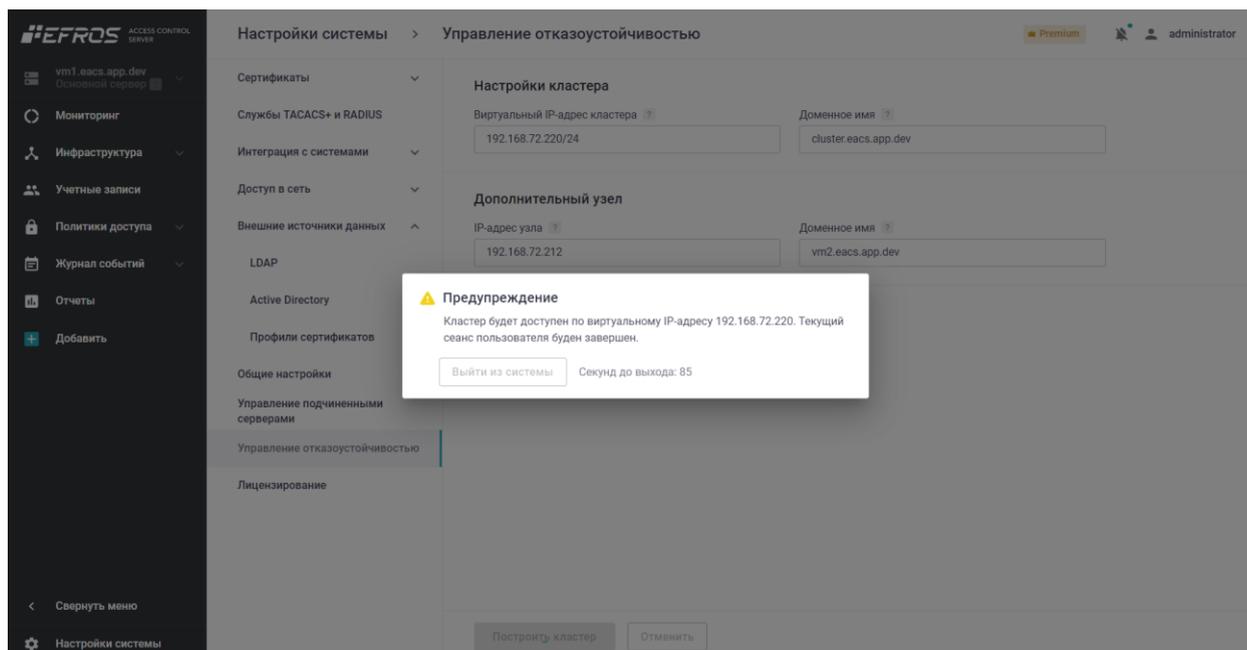


Рисунок 67 – Рисунок 66 – Создание кластера

- 5)
- 6) Появится окно с предупреждением о выходе из системы. Если пользователь не захочет ждать положенные 90 сек. Для выхода из системы пользователь может воспользоваться кнопкой «Выйти из системы».
- 7) В окне предупреждения содержится информация об IP-адресе, по которому будет доступен кластер. Пользователь автоматически перенаправляется на виртуальную машину с указанным в окне предупреждения IP-адресом.
- 8) Далее пользователю необходимо повторить процедуру аутентификации в ПК «Efros ACS».
- 9) Чтобы посмотреть, как выглядит построенный кластер, пользователю необходимо перейти в раздел «Настройки системы», далее в раздел «Управление отказоустойчивостью». (рис. 67)

Таблица 21 – Состав и описание элементов страницы создания кластера

Элемент	Описание
Группа полей «Настройка кластера»	
Поле «*Виртуальный IP кластера»	IP-адрес кластера, используемый для взаимодействия с комплексом в режиме отказоустойчивости. Используйте любой свободный IP-адрес
Поле «Домен»	Доменное имя сервера
Группа полей «Дополнительный сервер»	
Поле «IP сервера»	IP-адрес второго сервера, на котором установлен ПК «Efros ACS»
Поле «Домен»	Доменное имя сервера
*Необходимо использовать этот адрес при настройке ACO для протоколов RADIUS и TACACS+	

The screenshot displays the 'Efros ACS' management interface. On the left is a dark sidebar with navigation options: 'u02ACSFT02.acs.app.dev' (Основной сервер), 'Мониторинг', 'Инфраструктура', 'Учетные записи', 'Политики доступа', 'Журнал событий', 'Отчеты', 'Добавить', 'Свернуть меню', and 'Настройки системы'. The main content area is titled 'Настройки системы > Управление отказоустойчивостью'. A central menu lists various system settings, with 'Управление отказоустойчивостью' highlighted. The right-hand side shows the 'Кластер' configuration page, which includes:

- Кластер:** 'EfrosACScluster' (Активен), IP-адрес: 10.72.2.194, Доменное имя: testers-cluster.acs.app.dev.
- Узлы кластера:**
 - 'u02ACSFT02.acs.app.dev' (Активен), IP-адрес: 10.72.2.152.
 - 'u02ACSFT03.acs.app.dev' (Активен), IP-адрес: 10.72.2.153.
- Состояние кластера:**
 - 'Виртуальный IP-адрес кластера' (Активен), Узел: u02ACSFT02.acs.app.dev.
 - 'Службы EfrosACS' (Активен), Узел: u02ACSFT02.acs.app.dev.

 At the bottom right, there is a red button labeled 'Разрушить кластер'.

Рисунок 68 – Рисунок 67 – Построенный кластер

Для разрушения кластера необходимо сделать следующие шаги:

- 1) Нажать кнопку «Разрушить кластер».
- 2) Появится окно с предупреждением о том, что разрушение кластера займет некоторое время. Виртуальный IP-адрес станет недоступным. Узлы вернуться в состояние до построения кластера.
- 3) Далее нажать кнопку «Продолжить». Кластер будет разрушен

3.4.10. Лицензирование

Для использования функциональных возможностей программного комплекса после установки комплекса должна быть активирована лицензия на право использования продукта. ПК «Efros ACS» поддерживает два типа лицензии Standard и Premium. От выбранной лицензии зависит состав доступных пользователям функций комплекса. При использовании лицензии Standard к комплексу может быть подключено не более 1000 устройств, поддерживается только один внешний источник данных (LDAP-сервер или MS AD), не доступна функциональность формирования отчетов (раздел «Отчеты») и выпуска клиентских сертификатов (в разделе «Сертификаты» подраздел «Клиентские»).

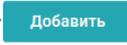
Первичная активация лицензии выполняется с правами встроенной учетной записи с ролью «ACS Администратор». Для осуществления операций по активации лицензии, переносу ключа лицензии, сброса лицензии и просмотра данных по текущей лицензии необходимо перейти на страницу раздела «Настройки системы» подраздел «Лицензирование». Подробно данные операции рассмотрены в документе «ПК «Efros ACS». Руководство администратора» в разделе 3.3. «Лицензирование».

3.5 Просмотр и ведение списка контролируемого АСО

3.5.1. Просмотр списка АСО

Для просмотра списка АСО пользователю необходимо перейти на страницу раздела «Инфраструктура» подраздел «Сетевое оборудование», выбрав в панели главного меню ссылку «Сетевое оборудование» или, если панель свернута, – пиктограмму «» и далее пиктограмму «».

Страница подраздела содержит отдельные вкладки списков АСО и групп АСО. По умолчанию активной является вкладка «Устройства», содержащая список всех АСО, контролируемых ПК «Efros ACS». АСО добавляются, редактируются или удаляются в списке вручную администраторами ACS либо в результате импорта данных из внешних систем: ПК «Efros Config Inspector» (см пункт 3.4.4).

 После установки ПК «Efros ACS» список АСО пуст, на странице отображается сообщение «В системе нет устройств» и кнопка «Добавить» () для перехода на страницу добавления нового АСО.

На рис. 68 приведена страница с вкладкой «Устройства» для администраторов RO. На рис. 69 приведена страница с вкладкой «Устройства» для администраторов ACS.

Название	IP-адрес	Тип протокола	Группы	Описание	Последние изменения ↓
st01	10.72.2.161	RADIUS	0		30 марта, 09:07:41
testnn	123.0.1.12	TACACS+ RADIUS	3		18 марта, 05:49:35
test2	120.1.1.11	TACACS+ RADIUS	2		11 марта, 09:06:46
Cisco123	123.0.0.11	RADIUS	1		11 марта, 08:18:50

Всего устройств: 4 Строк на странице: 50 1-4 из 4 1

Рисунок 69 – Рисунок 68 – Страница списка АСО для администратора RO

Название	IP-адрес	Тип протокола	Группы	Описание	Последние изменения ↓
st01	10.72.2.161	RADIUS	0		30 марта, 09:07:41
testnn	123.0.1.12	TACACS+ RADIUS	3		18 марта, 05:49:35
test2	120.1.1.11	TACACS+ RADIUS	2		11 марта, 09:06:46
Cisco123	123.0.0.11	RADIUS	1		11 марта, 08:18:50

Всего устройств: 4 Строк на странице: 50 1-4 из 4 1

Рисунок 70 – Рисунок 69 – Страница списка АСО для администратора ACS

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

- наименование;
- сетевой адрес;

- типы протоколов, по которым работает устройство;
- количество групп, в которые входит устройство. Является ссылкой, при выборе которой раскрывается список с наименованиями групп. При выборе наименования группы открывается страница просмотра/редактирования параметров группы АСО;
- описание устройства;
- дата и время последних изменений, внесенных в данные устройства.

Над таблицей располагаются:

- поле поиска (🔍 Введите запрос для поиска и нажмите Enter). Правила поиска приведены в п. 3.2.2;
- кнопка «Добавить» (+) – для перехода на страницу добавления АСО (см. п.п.3.5.3.1);
- кнопка «Добавить фильтр» (☰) – для перехода в окно фильтрации. Правила фильтрации приведены в п. 3.5.2;
- кнопка «Выбрать период» (📅) – Правила выбора периода внесения последних изменений в данные устройств приведены в п. 3.2.3.

Для пользователей-администраторов ACS дополнительно при наведении курсора на название устройства справа от названия отображается кнопка «Изменить название» (✎), предназначенная для перехода в окно изменения названия устройства.

3.5.2. Фильтрация данных в таблице АСО

Для фильтрации данных в таблице АСО необходимо нажать кнопку «Добавить фильтр» (☰). Откроется окно фильтрации, приведенное на рис. 70. Состав элементов окна и правила их заполнения приведены в таблице 22.

Далее необходимо:

- выбрать установкой переключателя тип протокола, по которому работают искомые устройства;
- заполнить, при необходимости, полностью или частично поле «IP-адрес»;
- нажать кнопку «Применить».

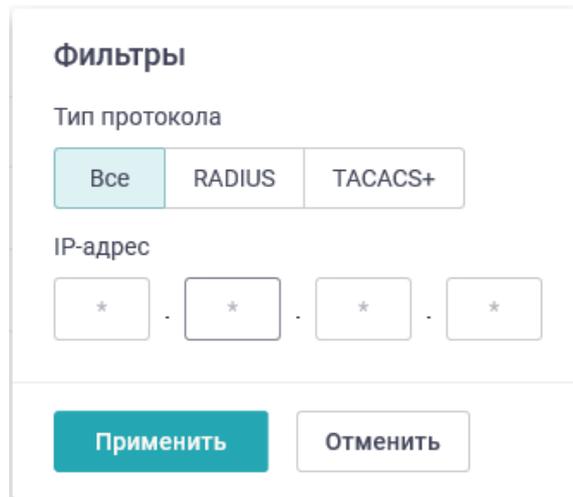


Рисунок 71 – Рисунок 70 – Окно фильтрации списка АСО

Таблица 22 – Состав и описание элементов окна фильтрации списка АСО

Элемент	Описание
Поле «Тип протокола»	<p>Поле-переключатель с тремя положениями:</p> <ul style="list-style-type: none"> — «Все» – в таблице содержатся записи устройств, работающих по обоим протоколам TACACS+ и RADIUS; — «RADIUS» – в таблице содержатся записи устройств, работающих только по протоколу RADIUS; — «TACACS+» – в таблице содержатся записи устройств, работающих только по протоколу TACACS+. <p>По умолчанию переключатель установлен в поле «Все»</p>
Поле «IP-адрес»	<p>Поле из четырех блоков для ввода полного или частичного значения IP-адреса искомых устройств.</p> <p>Справа расположена кнопка «Очистить» (🗑️), предназначенная для удаления введенных в поле значений</p>
Кнопки управления	
Применить	По нажатию кнопки окно фильтрации закрывается, введенные настройки фильтрации применяются
Отменить	По нажатию кнопки окно фильтрации закрывается без применения введенных настроек

После чего:

- окно фильтрации закрывается;

- в таблице отобразятся записи устройств, соответствующие заданным параметрам фильтрации;
- слева над таблицей в соответствии с рис. 71 отобразятся поля с заданными параметрам фильтрации.



Рисунок 72 – Рисунок 71 – Отображение параметров фильтрации записей списка

Для отмены заданных правил фильтрации и отображения в таблице всех записей необходимо нажать кнопку «Очистить» (X) в каждом поле отдельно.

3.5.3. Ведение списка АСО

3.5.3.1. Добавление АСО

Добавление нового АСО выполняется пользователем вручную средствами веб-приложения ПК «Efros ACS» либо автоматически при импорте данных из внешних систем (см. п. 3.4.4).

! Перед заведением нового АСО необходимо добавить профиль оборудования (см. подробнее в п. 3.10.2)!

Для добавления в список нового АСО вручную пользователю необходимо:

- 1) Нажать на странице списка АСО (см. рис. 69) над таблицей кнопку «Добавить» или в панели главного меню нажать кнопку «Добавить» и выбрать в открывшемся меню пункты «Инфраструктура» → «Устройство». Откроется страница добавления АСО, приведенная на рис. 72. Состав и описание элементов страницы приведены в таблице 23.
- 2) Заполнить поля страницы «Название», «Описание» и «IP-адрес или список подсетей» соответствующими данными добавляемого устройства.
- 3) Выбрать в поле «Профиль сетевого оборудования» из предлагаемого списка профиль устройства.

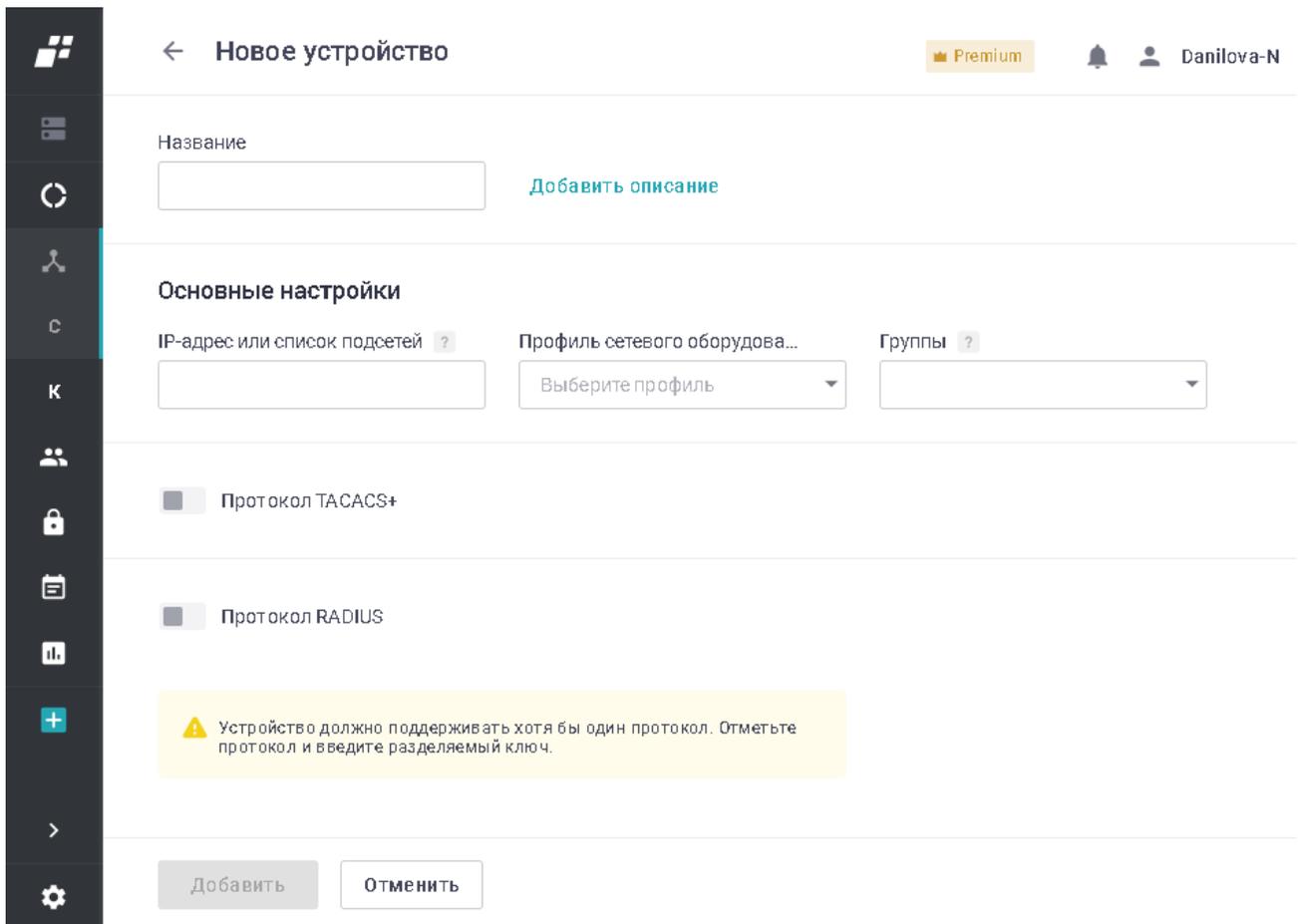


Рисунок 73 – Рисунок 72 – Страница добавления АСО

Таблица 23 – Состав и описание элементов страницы добавления АСО

Элемент	Описание
Поле «Название»	Текстовое поле для ввода названия устройства (до 50 символов)
Кнопка «Добавить описание»	По нажатию кнопки на странице дополнительно отображается поле «Описание» – текстовое поле для ввода описания устройства (до 250 символов). Под полем отображается кнопка «Удалить описание», по нажатию которой поле «Описание» очищается и удаляется
Группа полей «Основные настройки»	
*Поле «IP-адрес или список подсетей»	Текстовое поле для ввода IP-адреса или диапазона IP-адресов устройства

Элемент	Описание
*Поле «Профиль сетевого оборудования»	Поле со списком для выбора профиля сетевого оборудования из перечня заранее заведенных в разделе «Профили оборудования» (см . п. 3.10.2)
Поле «Группы»	Поле со списком для выбора одной или нескольких групп, в которые входит устройство. Список содержит названия групп, имеющихся в списке «Инфраструктура – Сетевое оборудование – Группы» ПК «Efros ACS». После выбора групп в поле отображается их общее количество
Поле «Протокол TACACS+»	Поля содержат переключатель с двумя положениями «  » (выключено) или «  » (включено) и наименование соответствующего протокола. При включенном переключателе – устройство работает по соответствующему протоколу. После включения переключателя на странице дополнительно отображается поле *«Разделяемый ключ» для ввода разделяемого ключа (ключ для защиты соединения между устройством и сервером авторизации (shared secret)) для соответствующего протокола. При вводе символы ключа заменяются знаком «●». Для просмотра введенного значения необходимо нажать в поле ввода кнопку «Просмотреть» ()
Поле «Протокол RADIUS»	
Кнопки управления	
Добавить	По нажатию кнопки выполняется переход на страницу списка устройств с сохранением внесенных данных
Отменить	По нажатию кнопки выполняется переход на страницу списка устройств без сохранения внесенных данных
* – Справа от поля расположен знак «  », при наведении на который курсора открывается всплывающая подсказка с правилами заполнения поля	

4) Выбрать, при необходимости, группы устройств, в которые входит АСО, для чего:

- установить курсор в поле «Группы»;
- в раскрывшемся списке групп устройств ПК «Efros ACS» (рис. 73) найти, при необходимости, требуемую группу или группы устройств, для чего ввести в поле поиска последовательность символов из наименования группы;

- установить флаг в строках групп, в которые должно входить устройство;
 - выбор будет сохранен после установки курсора вне поля, в поле отобразится либо наименование выбранной группы, либо общее количество выбранных групп (если их выбрано две и более).
- 5) Перевести переключатель в полях «Протокол TACACS+» и/или «Протокол RADIUS» в положение «включен» для включения соответственно режимов работы устройства по протоколам.
 - 6) Ввести для выбранного протокола (или протоколов) разделяемый ключ.
 - 7) Нажать кнопку «Добавить».

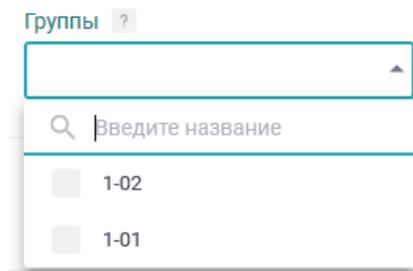


Рисунок 74 – Рисунок 73 – Поле «Группы»

Будет запущен процесс проверки заполненности всех обязательных полей и уникальности добавляемого АСО по названию и IP-адресу.

При обнаружении незаполненных обязательных полей рядом с первым из таких полей отобразится всплывающая подсказка «Обязательное поле», в случае обнаружения в списке дубликата устройства в верхней части страницы отобразится соответствующее сообщение. Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Добавить».

Если проверки завершились без обнаружения ошибок, то окно добавления закрывается, АСО добавляется в список устройств, перезапускаются службы протоколов TACACS+ и RADIUS для применения новых настроек. Контроль устройства посредством ПК «Efros ACS» будет осуществляться после успешного перезапуска служб.

В журнал событий ПК «Efros ACS» будет внесено сообщение:

- при успешном завершении – сообщение типа «Инфо» в формате: «Администратор {имя_выполняющего_операцию_администратора}: Устройство {название_устройства} успешно создано»;
- при обнаружении ошибки – сообщение типа «Ошибка» в формате: «Администратор {имя_выполняющего_операцию_администратора}: Ошибка создания устройства {название_устройства} - {текст_ошибки}».

3.5.3.2. Добавление АСО путем копирования записи имеющегося устройства

Для добавления нового устройства путем копирования записи имеющегося устройства пользователю необходимо:

- 1) Выбрать установкой флага в левой крайней графе таблицы списка устройств исходное устройство. В верхней части таблицы отобразится строка выбора операций в соответствии с рис. 74.

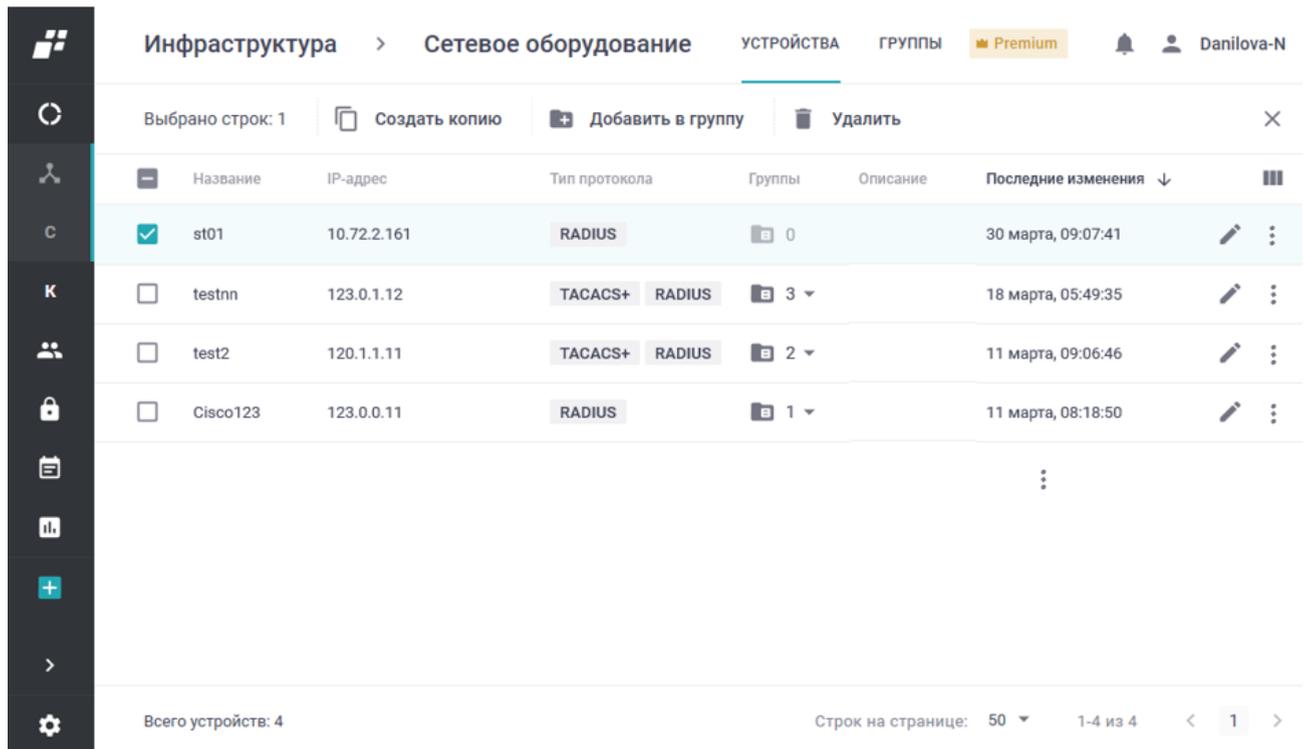


Рисунок 75 – Рисунок 74 – Страница списка АСО со строкой выбора операций

- 2) Нажать в строке кнопку «Создать копию» (📄). Откроется страница добавления нового устройства, аналогичная приведенной на рис. 72. Все поля страницы будут заполнены данными исходного АСО, кроме полей «Название» и «IP-адрес или список подсетей».
- 3) Далее пользователю необходимо внести требуемые изменения и нажать кнопку «Добавить».

Правила заполнения полей страницы, проверки корректности данных и действий ПК «Efros ACS» при успешном и неуспешном завершении проверок аналогичны правилам добавления АСО (см. п.п. 3.5.3.1).

3.5.3.3. Добавление АСО в группу устройств

Добавление АСО в группу устройств выполняется либо при его добавлении в список устройств (см. п.п. 3.5.3.1 и 3.5.3.2), либо при редактировании учетной записи АСО (см.

п.п. 3.5.3.4) в поле «Группы» страницы создания/редактирования устройства. Кроме того, АСО может быть добавлено в группу устройств непосредственно из списка устройств.

Для добавления АСО в группу устройств из списка пользователю необходимо:

- 1) Выбрать установкой флага в левой крайней графе таблицы списка устройств добавляемое АСО. В верхней части таблицы отобразится строка выбора операций (см. рис. 74).
- 2) Нажать в строке кнопку «Добавить в группу» (+). Откроется окно выбора группы устройств, приведенное на рис. 75.
- 3) Выбрать в раскрывающемся списке групп устройств окна наименование требуемой группы.
- 4) Нажать кнопку «Добавить». Окно закроется. В указанную группу будет добавлено выбранное на шаге 1 АСО.

Будет запущен процесс проверки корректности данных группы и уникальности АСО по названию и IP-адресу.

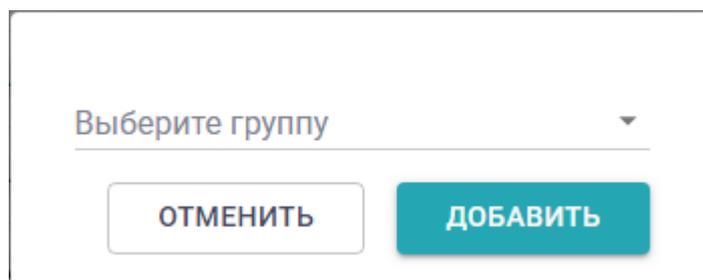


Рисунок 76 – Рисунок 75 – Окно выбора группы устройств

Если проверки завершились без обнаружения ошибок, то АСО добавляется в группу, перезапускаются службы протоколов TACACS+ и RADIUS для применения новых настроек. Контроль АСО с новыми настройками посредством ПК «Efros ACS» будет осуществляться после успешного перезапуска служб.

В журнал событий ПК «Efros ACS» будут внесены сообщения:

- 1) При успешном завершении – сообщения типа «Инфо» в формате:
 - «Администратор{имя_выполняющего_операцию_администратора}: Устройство {название_устройства} успешно обновлено»;
 - «Администратор {имя_выполняющего_операцию_администратора}: Группа устройств {название_группы_устройств} успешно обновлена».
- 2) При обнаружении ошибки – сообщения типа «Ошибка» в формате:

- «Администратор {имя_выполняющего_операцию_администратора}: Ошибка обновления устройства {название_устройства} - {текст_ошибки}»;
- «Администратор {имя_выполняющего_операцию_администратора}: Ошибка обновления группы устройств - {текст_ошибки}».

3.5.3.4. Редактирование АСО

Редактирование данных АСО выполняется пользователем вручную средствами веб-приложения ПК «Efros ACS» либо автоматически при импорте данных из внешних систем (см. пункты 3.4.4). При редактировании вручную для внесения изменений доступны все данные АСО.

Для редактирования названия АСО пользователю необходимо:

- 1) Навести в списке устройств курсор на название требуемого АСО.
- 2) Нажать справа от названия кнопку «Изменить название» (✎). Откроется окно, приведенное на рис. 76.
- 3) Внести изменения в название устройства и нажать ставшую активной кнопку «Сохранить».

Рисунок 77 – Рисунок 76 – Окно изменения названия АСО

Для редактирования всех данных АСО пользователю необходимо выбрать в списке с помощью «мыши» название требуемого АСО либо нажать в строке АСО кнопку «Изменить» (✎). Откроется страница редактирования АСО. Страница содержит внесенные ранее данные. Состав элементов страницы и правила заполнения полей страницы аналогичны составу страницы добавления АСО и правилам добавления АСО (см. п.п. 3.5.3.1). Далее пользователю необходимо внести требуемые изменения и нажать кнопку «Сохранить».

После нажатия кнопки «Сохранить» (после изменения названия АСО или всех данных АСО) будет запущен процесс проверки заполненности всех обязательных полей и уникальности редактируемого АСО по названию и IP-адресу.

При обнаружении незаполненных обязательных полей рядом с первым из таких полей отобразится всплывающая подсказка «Обязательное поле», в случае обнаружения в

списке дубликата АСО в верхней части страницы отобразится соответствующее сообщение. Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Сохранить».

Если проверки завершились без обнаружения ошибок, то окно редактирования закрывается, внесенные изменения сохраняются, перезапускаются службы протоколов TACACS+ и RADIUS для применения новых настроек. Внесенные изменения будут применяться при контроле АСО посредством ПК «Efros ACS» после успешного перезапуска служб.

В журнал событий ПК «Efros ACS» будет внесено сообщение:

- при успешном завершении – сообщение типа «Инфо» в формате: «Администратор {имя_выполняющего_операцию_администратора}: Устройство {название_устройства} успешно обновлено»;
- при обнаружении ошибки – сообщение типа «Ошибка» в формате: «Администратор {имя_выполняющего_операцию_администратора}: Ошибка обновления устройства {название_устройства} - {текст_ошибки}».

3.5.3.5. Просмотр данных АСО

Для просмотра данных одного АСО необходимо выбрать в таблице с помощью «мыши» название АСО, после чего:

- для пользователя-администратора RO откроется страница просмотра соответствующей записи списка (рис. 77);
- для пользователя-администратора ACS откроется страница редактирования данных соответствующей записи списка (см. п.п. 3.5.3.1). Страница содержит все данные страницы просмотра, данные доступны для редактирования.

Пользователь имеет возможность просмотреть название, описание, IP-адрес, выбранный протокол взаимодействия и список групп, в которые АСО включено. Список групп, в которые включено устройство администратор RO может просмотреть в списке устройств в соответствии с рис. 78.

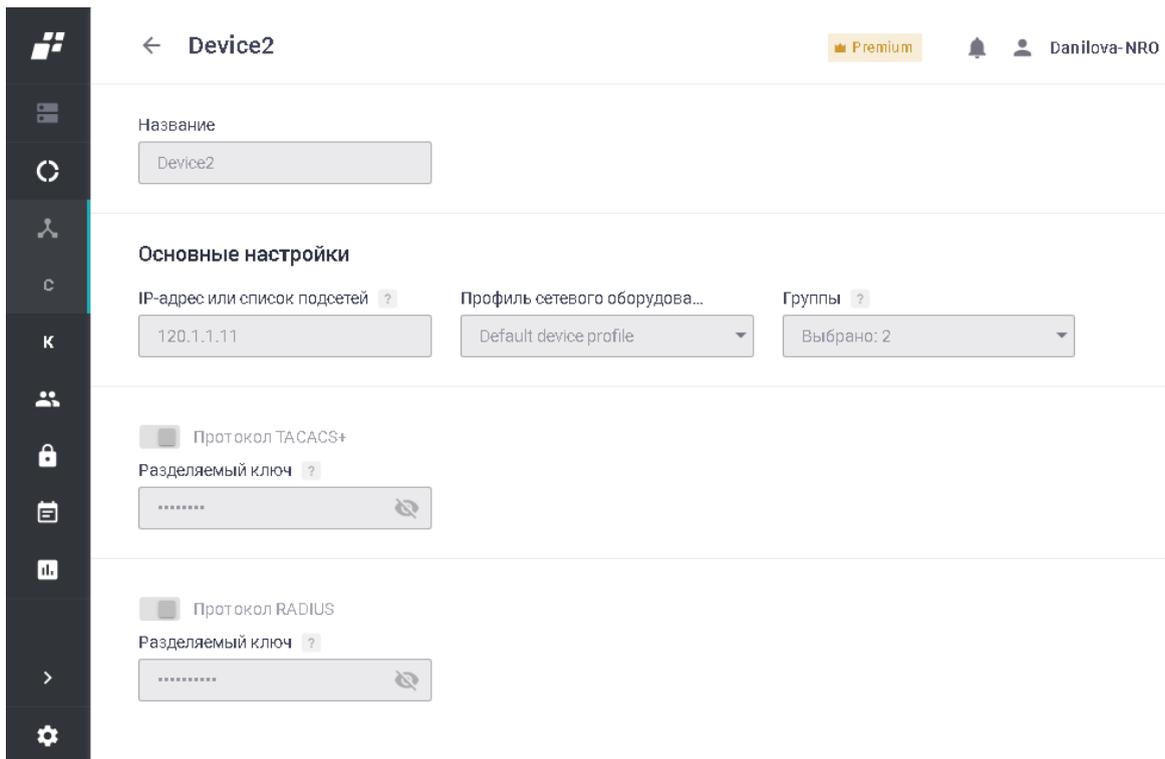


Рисунок 78 – Рисунок 77 – Страница просмотра данных устройств для администратора RO

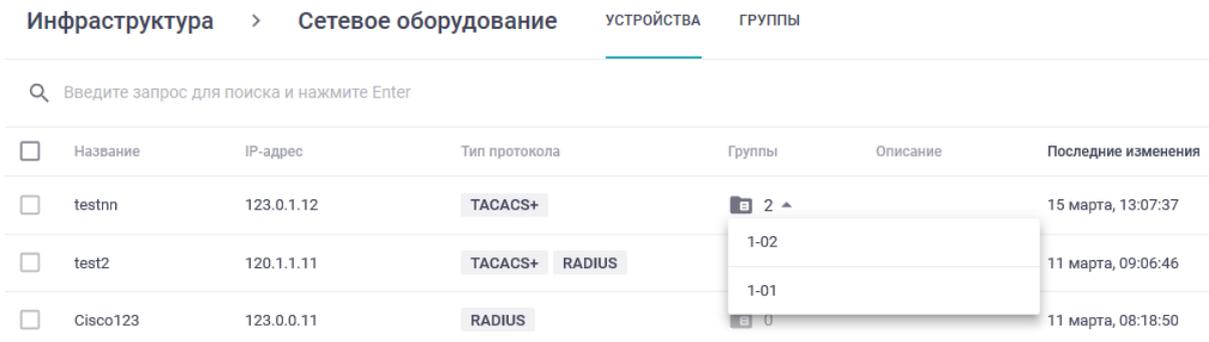


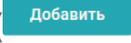
Рисунок 79 – Рисунок 78 – Окно просмотра групп, в которые включено АСО

3.6 Просмотр и ведение списка групп АСО

3.6.1. Просмотр списка групп АСО

Для просмотра списка групп АСО пользователю необходимо перейти на страницу раздела «Инфраструктура» в подраздел «Сетевое оборудование», выбрав в панели главного меню ссылку «Инфраструктура», далее ссылку «Сетевое оборудование» или, если панель свернута, – пиктограмму «» и далее пиктограмму «». Далее – перейти на вкладку «Группы». Вкладка содержит список всех групп АСО, в которые объединены контролируемые АСО в ПК «Efros ACS».

Группы АСО добавляются, редактируются или удаляются в ПК «Efros ACS» вручную администраторами ACS.

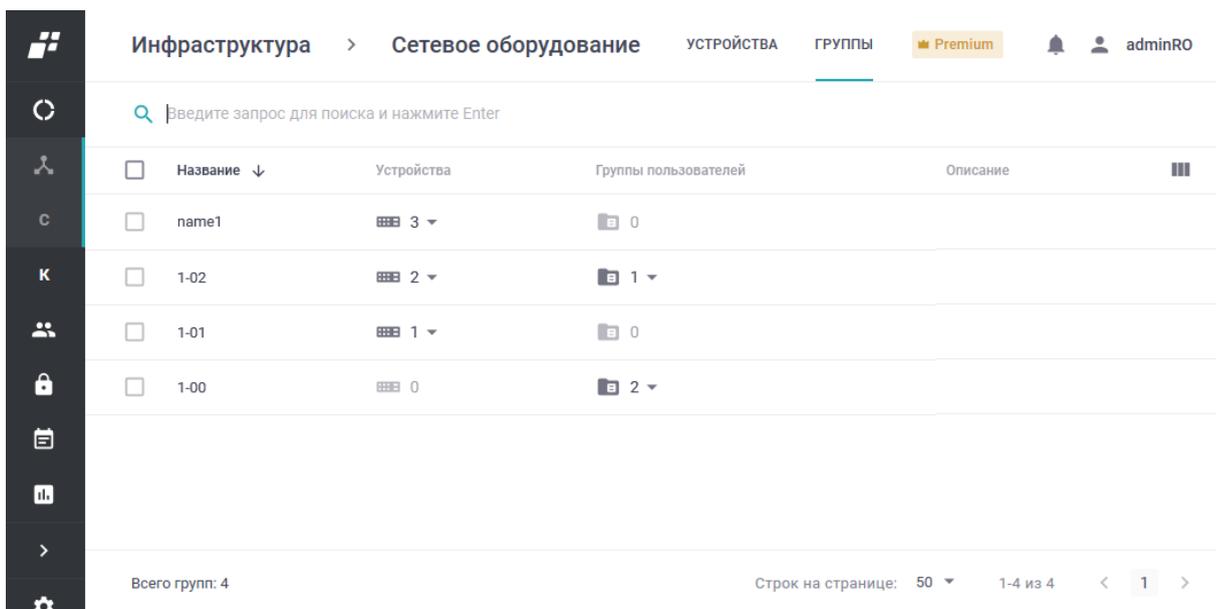
Примечание. После установки ПК «Efros ACS» список групп АСО пуст, на странице отображается сообщение «В системе нет групп устройств» и кнопка «Добавить» () для перехода на страницу добавления новой группы АСО.

На рис. 79 приведена страница с вкладкой «Группы» для пользователей с ролью «RO Администратор», все данные доступны для просмотра. На рис. 80 приведена страница с вкладкой «Группы» для пользователей с ролью «ACS Администратор».

Над таблицей располагается поле поиска. Правила поиска приведены в п. 3.2.2

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

- наименование;
- количество входящих в группу АСО. Является ссылкой, при выборе которой открывается окно просмотра данных устройств (рис. 81). При выборе наименования АСО открывается страница просмотра/редактирования данных АСО;
- количество групп пользователей, имеющих доступ к устройствам группы. Является ссылкой, при выборе которой открывается окно просмотра наименований групп пользователей, имеющих доступ к группе АСО (рис. 82). При выборе наименования группы пользователей открывается страница просмотра/редактирования данных группы;
- описание группы.



Имя	Устройства	Группы пользователей	Описание
name1	3	0	
1-02	2	1	
1-01	1	0	
1-00	0	2	

Рисунок 80 – Рисунок 79 – Страница списка групп АСО для администратора RO

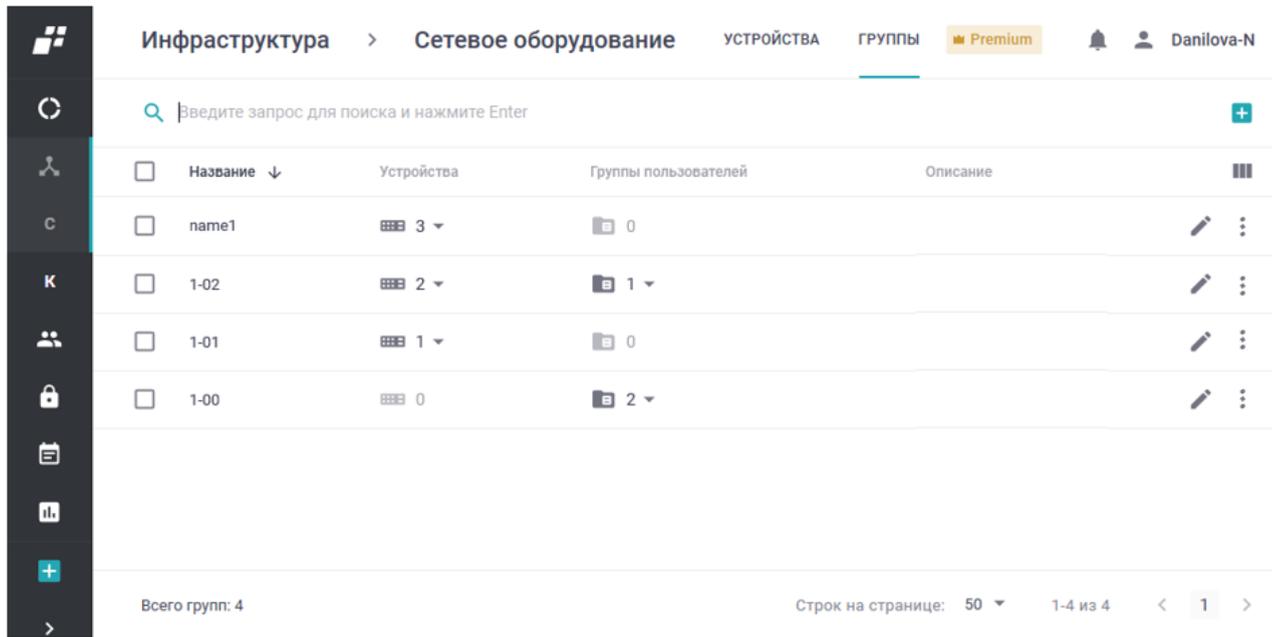


Рисунок 81 – Рисунок 80 – Страница списка групп АСО для администратора ACS

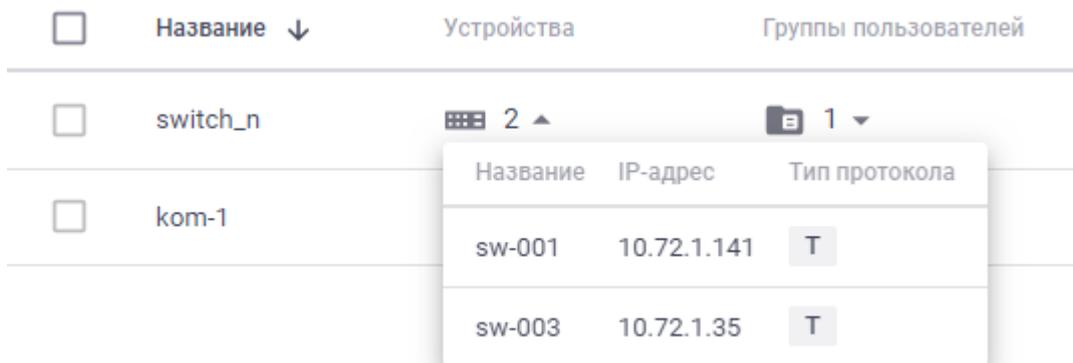


Рисунок 82 – Рисунок 81 – Окно просмотра данных АСО, включенных в группу

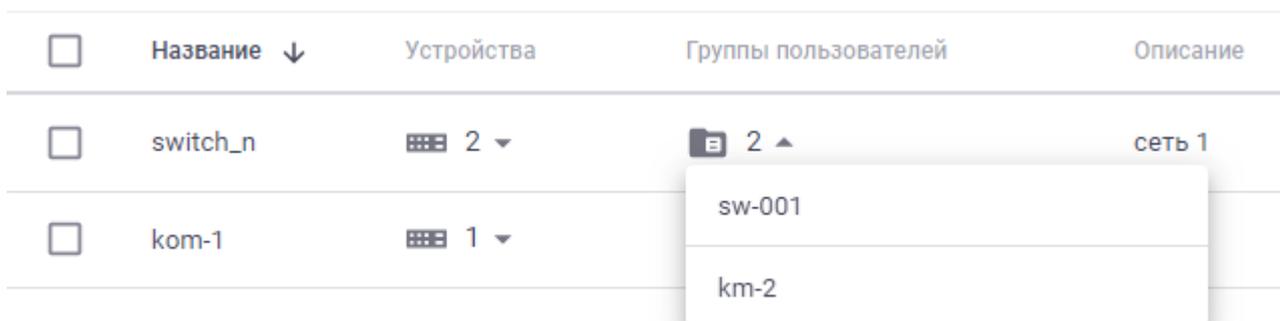


Рисунок 83 – Рисунок 82 – Окно просмотра наименований групп пользователей, имеющих доступ к группе АСО

3.6.2. Ведение списка групп АСО

3.6.2.1. Добавление группы АСО из списка АСО

Для добавления в список новой группы АСО из списка АСО пользователю необходимо:

- 1) Выбрать установкой флагов в списке устройств АСО, объединяемые в группу. В верхней части таблицы отобразится строка в соответствии с рис. 83.
- 2) Нажать в строке кнопку «Создать группу» (📁). Откроется страница добавления группы АСО, приведенная на рис. 84. Состав и описание элементов страницы приведены в таблице 24.
- 3) Заполнить поле страницы «Название».
- 4) Добавить, при необходимости, описание группы, нажав кнопку «Добавить описание» и заполнив отобразившееся поле «Описание».

Выбрано строк: 2	Создать группу	Добавить в группу	Удалить				
Название	IP-адрес	Тип протокола	Группы	Описание	Последние изменения ↓		
<input checked="" type="checkbox"/>	st01	10.72.2.161	RADIUS	0		30 марта, 09:07:41	✎ ⋮
<input type="checkbox"/>	testnn	123.0.1.12	TACACS+ RADIUS	3		18 марта, 05:49:35	✎ ⋮
<input checked="" type="checkbox"/>	test2	120.1.1.11	TACACS+ RADIUS	2		11 марта, 09:06:46	✎ ⋮
<input type="checkbox"/>	Cisco123	123.0.0.11	RADIUS	1		11 марта, 08:18:50	✎ ⋮

Всего устройств: 4

Строк на странице: 50 1-4 из 4 < 1 >

Рисунок 84 – Рисунок 83 – Страница списка АСО со строкой выбора операций

← Новая группа устройств Premium Danilova-N

Название ?

Добавить описание

Основные настройки

Устройства ?

Выбрано: 3

Добавить Отменить

Рисунок 85 – Рисунок 84 – Страница добавления группы устройств

Таблица 24 – Состав и описание элементов страницы добавления группы АСО

Элемент	Описание
*Поле «Название»	Текстовое поле для ввода названия группы устройств (до 50 символов)
Кнопка «Добавить описание»	По нажатию кнопки на странице дополнительно отображается поле «Описание» – текстовое поле для ввода описания группы (до 250 символов). Под полем отображается кнопка «Удалить описание», по нажатию которой поле «Описание» очищается и удаляется
*Группа полей «Основные настройки» / поле «Устройства»	Содержит общее количество устройств, выбранных в списке для объединения в группу. При установке в поле курсора раскрывается список АСО ПК «Efros ACS». Пользователь имеет возможность установкой/отменой установки флагов указать включаемые в группу устройства

Элемент	Описание
Кнопки управления	
Добавить	По нажатию кнопки выполняется переход на страницу списка устройств с сохранением внесенных данных
Отменить	По нажатию кнопки выполняется переход на страницу списка устройств без сохранения внесенных данных
Сбросить	По нажатию кнопки все введенные данные в окне удаляются
* – Справа от поля расположен знак «?», при наведении на который курсора открывается всплывающая подсказка с правилами заполнения поля	

- 5) Выбрать, при необходимости, дополнительные устройства, входящие в группу, для чего:
- установить курсор в поле «Устройства». Раскроется список устройств, внесенных ранее в список АСО ПК «Efros ACS» (рис. 85);
 - ввести, при необходимости, в поле поиска символы из наименования требуемого устройства (список устройств будет отфильтрован по совпадению наименований с введенными символами);
 - установить флаг в строках устройств, которые должны входить в группу АСО.
- 6) Нажать в окне добавления группы кнопку «Добавить».

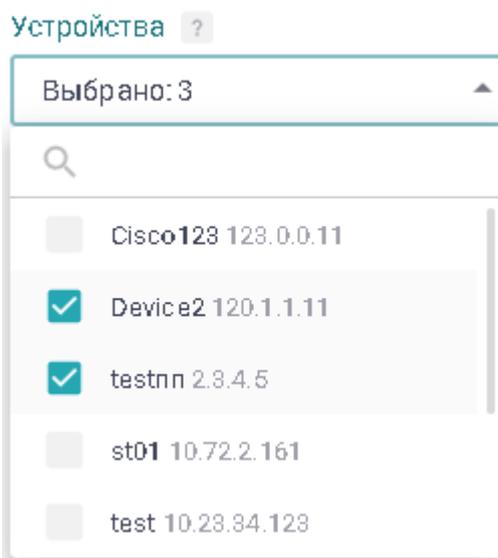


Рисунок 86 – Рисунок 85 – Поле «Устройства» с раскрытым списком АСО ПК «Efros ACS»

Будет запущен процесс проверки заполненности всех обязательных полей и уникальности добавляемой группы АСО по наименованию.

При обнаружении незаполненных обязательных полей рядом с первым из таких полей отобразится всплывающая подсказка «Обязательное поле», в случае обнаружения в списке дубликата группы устройств в верхней части страницы отобразится соответствующее сообщение. Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Добавить».

Если проверки завершились без обнаружения ошибок, то окно добавления закрывается, группа АСО добавляется в список групп АСО, группа становится доступна для выбора при создании/редактировании АСО.

В журнал событий ПК «Efros ACS» будет внесено сообщение:

- при успешном завершении – сообщение типа «Инфо» в формате: «Администратор {имя_выполняющего_операцию_администратора}: Группа устройств {название_группы_устройств} успешно создана»;
- при обнаружении ошибки – сообщение типа «Ошибка» в формате: «Администратор {имя_выполняющего_операцию_администратора}: Ошибка создания группы устройств - {текст_ошибки}».

3.6.2.2. Добавление группы АСО из списка групп АСО или из главного меню

Для добавления в список новой группы АСО из списка групп АСО или из главного меню пользователю необходимо:

- 1) Нажать на странице списка групп АСО (см. рис. 80) над таблицей кнопку «Добавить» или нажать в панели главного меню кнопку «Добавить» и выбрать в открывшемся меню пункты «Инфраструктура»→«Группа устройств». Откроется страница добавления группы пользователей, приведенная на рис. 84.
- 2) Далее – повторить действия по созданию группы, приведенные в п.п. 3.6.2.1.

В журнал событий ПК «Efros ACS» будут внесены соответствующие сообщения.

3.6.2.3. Добавление группы АСО путем копирования записи имеющейся группы АСО

Для добавления новой группы АСО путем копирования записи имеющейся группы АСО пользователю необходимо:

- 1) Выбрать установкой флага в левой крайней графе таблицы списка групп АСО исходную группу. В верхней части таблицы отобразится строка выбора операций в соответствии с рис. 86.

- 2) Нажать в строке кнопку «Создать копию» (📄). Откроется страница добавления новой группы АСО, аналогичная приведенной на рис. 86. Все поля страницы будут заполнены данными исходной группы АСО, кроме поля «Название».
- 3) Далее пользователю необходимо внести требуемые изменения и нажать кнопку «Добавить». Правила заполнения полей страницы аналогичны правилам добавления группы АСО (см. п.п. 3.6.2.1).

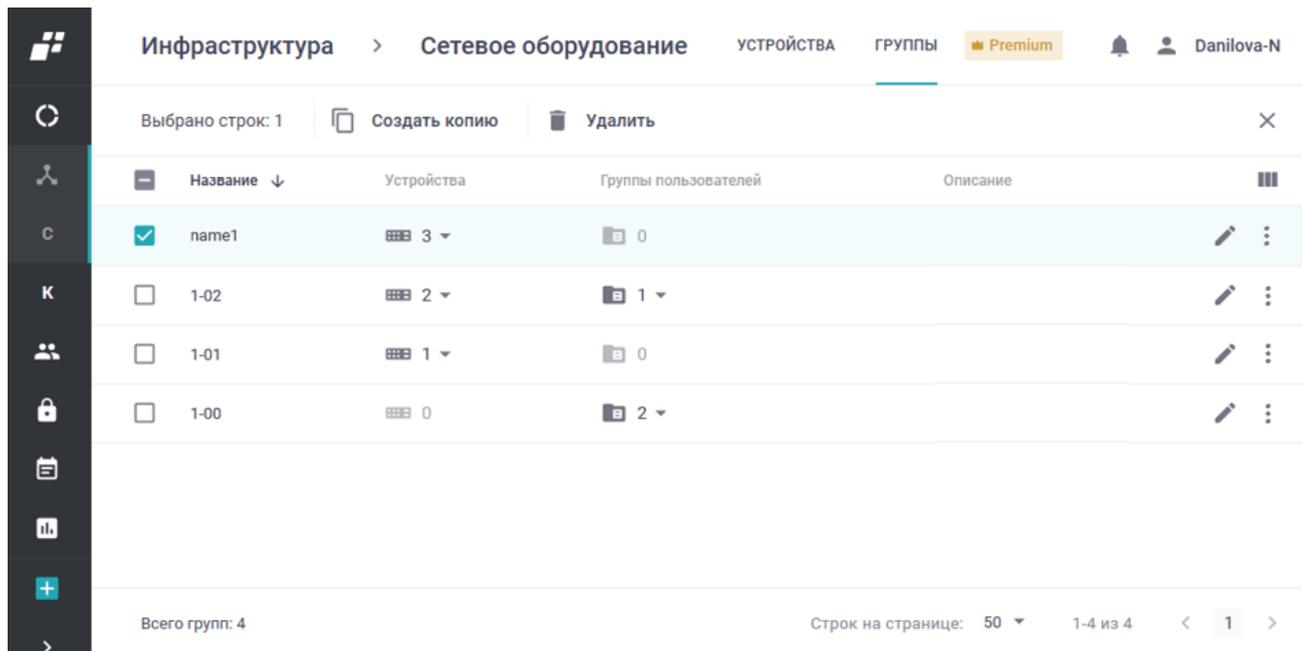


Рисунок 87 – Рисунок 86 – Страница списка групп АСО со строкой выбора операций

Будет запущен процесс проверки заполненности всех обязательных полей и уникальности добавляемой группы АСО по наименованию.

При обнаружении незаполненных обязательных полей рядом с первым из таких полей отобразится всплывающая подсказка «Обязательное поле», в случае обнаружения в списке дубликата группы устройств в верхней части страницы отобразится соответствующее сообщение. Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Добавить».

Если проверки завершились без обнаружения ошибок, то окно добавления закрывается, группа АСО добавляется в список групп АСО, группа становится доступна для выбора при создании/редактировании устройства.

В журнал событий ПК «Efros ACS» будут внесены соответствующие сообщения.

3.6.2.4. Просмотр данных группы АСО

Для просмотра данных одной группы АСО необходимо выбрать в таблице с помощью «мыши» название группы АСО, после чего:

- для пользователя-администратора RO откроется страница просмотра соответствующей записи списка (рис. 87);
- для пользователя-администратора ACS откроется страница редактирования данных соответствующей записи списка (см. п.п. 3.6.2.5). Страница содержит все данные страницы просмотра, данные доступны для редактирования. В поле «Состав группы» вместо кнопки «Просмотр» отображается кнопка «Изменить».

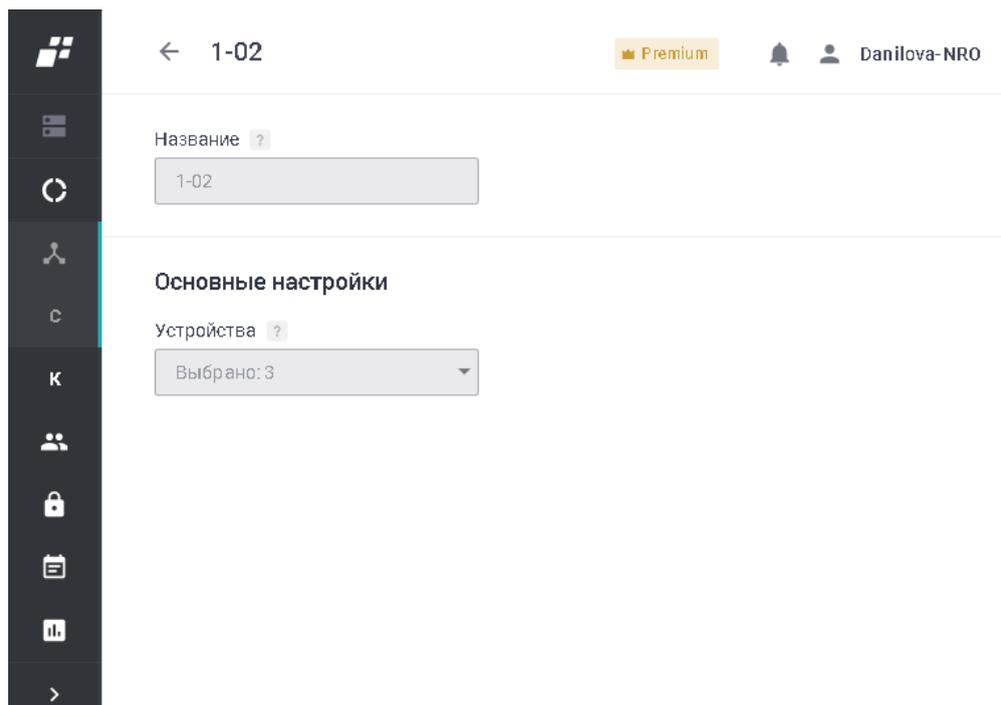


Рисунок 88 – Рисунок 87 – Страница просмотра данных группы АСО для администратора RO

Пользователь имеет возможность просмотреть название, описание (при его наличии) группы и список АСО, включенных в группу.

Список устройств, включенных в группу администратор RO может просмотреть в списке групп АСО в соответствии с рис. 88.

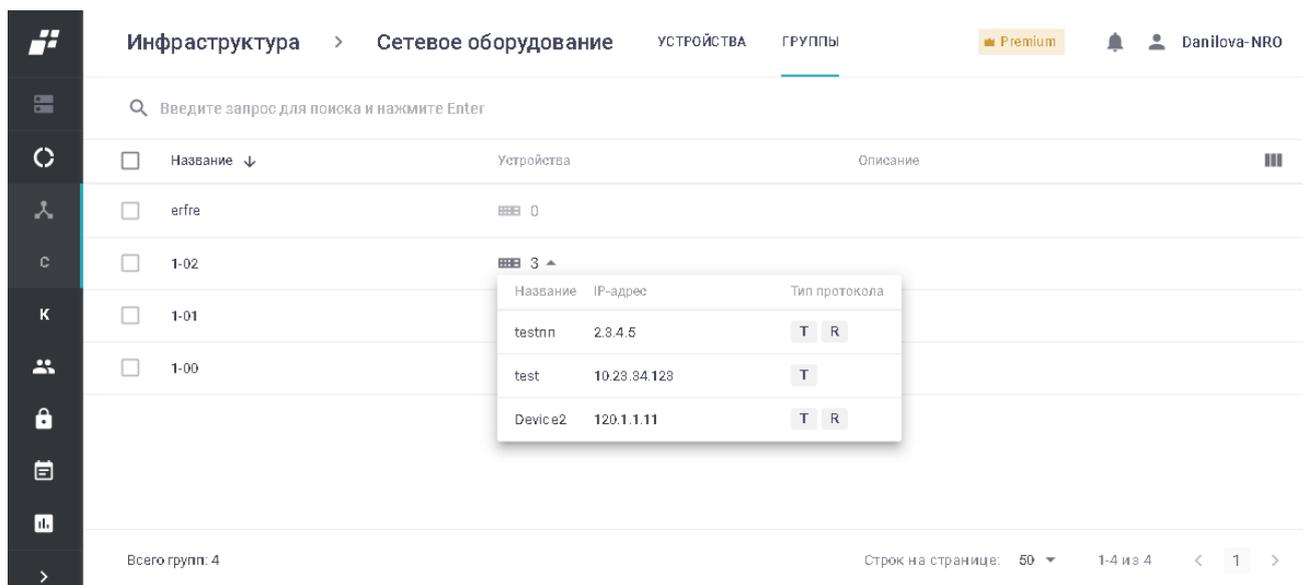


Рисунок 89 – Рисунок 88 – Просмотр списка АСО, включенных в группу, из списка групп

3.6.2.5. Редактирование группы АСО

Редактирование данных группы АСО выполняется пользователем вручную средствами веб-приложения ПК «Efros ACS». При редактировании для внесения изменений доступны все данные группы АСО.

Для редактирования пользователю необходимо выбрать в списке с помощью «мыши» название требуемой группы либо нажать в строке группы кнопку «Изменить» (✎). Откроется страница редактирования группы АСО. Страница содержит внесенные ранее данные. Состав элементов страницы и правила заполнения полей страницы аналогичны составу страницы добавления группы АСО и правилам добавления группы (см. п.п. 3.6.2.1). Далее пользователю необходимо внести требуемые изменения и нажать кнопку «Сохранить».

Будет запущен процесс проверки заполненности всех обязательных полей и уникальности редактируемой группы АСО по наименованию.

При обнаружении незаполненных обязательных полей рядом с первым из таких полей отобразится всплывающая подсказка «Обязательное поле», в случае обнаружения в списке дубликата группы устройств в верхней части страницы отобразится соответствующее сообщение. Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Сохранить».

Если проверки завершились без обнаружения ошибок, то окно редактирования закрывается, внесенные изменения сохраняются.

В журнал событий ПК «Efros ACS» будет внесено сообщение:

- при успешном завершении – сообщение типа «Инфо» в формате: «Администратор {имя_выполняющего_операцию_администратора}: Группа устройств {название_группы_устройств} успешно обновлена»;
- при обнаружении ошибки – сообщение типа «Ошибка» в формате: «Администратор {имя_выполняющего_операцию_администратора}: Ошибка обновления группы устройств - {текст_ошибки}».

3.7 Просмотр и ведение списка клиентского оборудования

3.7.1. Просмотр списка клиентского оборудования

Для просмотра списка клиентского оборудования, аутентифицирующегося в сети по MAC-адресу учетной записи в ПК «Efros ACS», пользователю необходимо перейти на страницу раздела «Инфраструктура» подраздел «Конечные точки сети», выбрав в панели главного меню ссылку «Конечные точки сети» или, если панель свернута, – пиктограмму «» и далее пиктограмму «**К**».

Страница подраздела содержит отдельные вкладки списков клиентского оборудования (КО) и групп КО. По умолчанию активной является вкладка «Устройства», содержащая список всех КО, контролируемых ПК «Efros ACS». КО добавляются, редактируются или удаляются в списке вручную администраторами ACS. На рис. 89 приведена страница с вкладкой «Устройства» для администраторов ACS.

 После установки ПК «Efros ACS» список КО пуст, на странице отображается сообщение «В системе нет конечных точек» и кнопка «Добавить» () для перехода на страницу добавления нового КО.

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

- название;
- статус КО: «Вкл» (включен) / «Выкл» (выключен). Слева расположена кнопка смены статуса КО – в зависимости от текущего статуса кнопка имеет вид: «» (выключить), «»(включить);
- MAC-адрес;
- количество групп, в которые входит КО. Является ссылкой, при выборе которой раскрывается список с наименованиями групп. При выборе наименования группы открывается страница просмотра/редактирования данных группы КО;
- описание КО;

— дата и время последних изменений, внесенных в данные КО.

<input type="checkbox"/>	Название	Статус	MAC-адрес	Группы	Описание	Последние изменения ↓	
<input type="checkbox"/>	DC2-205	■ Вкл.	25-45-74-56-14-23	2 ▾	2этаж, к. 205	16 марта, 06:17:52	
<input type="checkbox"/>	MFU2-203	■ Вкл.	34-15-23-64-56-23	2 ▾	МФУ 2этаж, к. 203	16 марта, 06:17:18	
<input type="checkbox"/>	pt1_01	■ Вкл.	23-44-23-45-56-68	1 ▾	1 этаж, к 01	16 марта, 06:16:18	

Всего конечных точек сети: 3

Строк на странице: 50 ▾ 1-3 из 3 < 1 >

Рисунок 90 – Рисунок 89 – Страница списка КО для администратора ACS

Над таблицей располагаются:

- поле поиска (Введите запрос для поиска и нажмите Enter). Правила поиска приведены в п. 3.2.2;
- кнопка «Добавить фильтр» () – для перехода в окно фильтрации. Правила фильтрации приведены в п. 3.2.4.

Для администраторов ACS на странице также доступны следующие кнопки:

- «Добавить» () – для добавления нового КО;
- «Изменить» () – для перехода на страницу редактирования записи списка;
- «Меню» () – для раскрытия меню с пунктами:
 - а) «Добавить в группу» () – при выборе меню открывается окно выбора группы, в которую добавляется КО;
 - б) «Создать копию» () – при выборе меню открывается страница создания нового КО, поля которой заполнены данными КО из соответствующей кнопке записи;
 - в) «Удалить» () – для удаления соответствующей записи списка.

3.7.2. Ведение списка КО

Добавление нового КО выполняется пользователем вручную средствами веб-приложения ПК «Efros ACS». Для добавления в список нового АСО вручную пользователю необходимо:

- 1) Нажать на странице списка КО (см. рис. 89) над таблицей кнопку «Добавить» или нажать в панели главного меню кнопку «Добавить» и выбрать в открывшемся меню пункты «Инфраструктура» → «Конечная точка». Откроется страница добавления КО, приведенная на рис. 90. Состав и описание элементов страницы приведены в таблице 25.

Рисунок 91 – Рисунок 90 – Страница добавления КО

Таблица 25 – Состав и описание элементов страницы добавления КО

Элемент	Описание
*Поле «Название»	Текстовое поле для ввода названия КО (до 50 символов)
Статус	Содержит две кнопки: <ul style="list-style-type: none"> — «Активен» – КО разрешена аутентификация по его учетной записи в ПК «Efros ACS»; — «Неактивен» – КО запрещен доступ в сеть по его учетной записи в ПК «Efros ACS».

Элемент	Описание
	По умолчанию нажата кнопка «Активен». Для администратора RO кнопки не доступны для нажатия
Кнопка «Добавить описание»	По нажатию кнопки на странице дополнительно отображается поле «Описание» – текстовое поле для ввода описания КО (до 250 символов). Под полем отображается кнопка «Удалить описание», по нажатию которой поле «Описание» очищается и удаляется
Группа полей «Основные настройки»	
*Поле «MAC-адрес»	Текстовое поле для ввода MAC-адреса устройства
Поле «Группы»	Поле со списком для выбора одной или нескольких групп, в которые входит КО. Список содержит названия групп, имеющихся в списке «Инфраструктура – Конечные точки сети – Группы» ПК «Efros ACS». После выбора групп в поле отображается их общее количество
Кнопки управления	
Добавить	По нажатию кнопки выполняется переход на страницу списка КО с сохранением внесенных данных
Отменить	По нажатию кнопки выполняется переход на страницу списка КО без сохранения внесенных данных
Сбросить	Кнопка отображается на странице после заполнения хотя бы одного поля. По нажатию кнопки все введенные данные на странице удаляются
* – Справа от поля расположен знак «?», при наведении на который курсора открывается всплывающая подсказка с правилами заполнения поля	

- 2) Заполнить поля страницы «Название» и «MAC-адрес» соответствующими данными добавляемого КО.
- 3) Добавить, при необходимости, описание КО, нажав кнопку «Добавить описание» и заполнив отобразившееся поле «Описание».
- 4) Выбрать статус подключения КО, нажатием соответствующей кнопки в поле «Статус».
- 5) Выбрать, при необходимости, группы устройств, в которые входит КО, для чего:

- установить курсор в поле «Группы»;
 - в раскрывшемся списке групп устройств ПК «Efros ACS» найти, при необходимости, требуемую группу или группы КО, для чего ввести в поле поиска последовательность символов из наименования группы;
 - установить флаг в строках групп, в которые должно входить КО;
 - выбор будет сохранен после установки курсора вне поля, в поле отобразится либо наименование выбранной группы, либо общее количество выбранных групп (если их выбрано две и более).
- б) Нажать в окне добавления КО кнопку «Добавить».

Будет запущен процесс проверки заполненности всех обязательных полей и уникальности добавляемого КО по названию и MAC-адресу.

 Поля, при наведении на которые курсора появляется всплывающая подсказка «Обязательное поле», обязательны для заполнения.

При обнаружении незаполненных обязательных полей рядом с первым из таких полей отобразится всплывающая подсказка «Обязательное поле», в случае обнаружения в списке дубликата КО в верхней части страницы отобразится соответствующее сообщение. Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Добавить».

Если проверки завершились без обнаружения ошибок, то окно добавления закрывается, КО добавляется в список устройств. Контроль устройства посредством ПК «Efros ACS» будет осуществляться сразу после успешного добавления КО в список.

В журнал событий ПК «Efros ACS» будет внесено сообщение:

- при успешном завершении – сообщение типа «Инфо» в формате: «Администратор {имя_выполняющего_операцию_администратора}: Устройство {название_устройства} успешно создано»;
- при обнаружении ошибки – сообщение типа «Ошибка» в формате: «Администратор {имя_выполняющего_операцию_администратора}: Ошибка создания устройства {название_устройства} - {текст_ошибки}».

КО может быть добавлено в список путем копирования записи имеющегося КО. Правила добавления КО путем копирования аналогичны правилам добавления АСО путем копирования и приведены в п.п. 3.5.3.2.

Созданная запись КО доступна администратору для:

- 1) Редактирования. Правила редактирования КО аналогичны правилам редактирования АСО и приведены в п.п. 3.5.3.4, за исключением следующего:
 - название КО может быть изменено только на странице редактирования данных КО;
 - статус КО может быть изменен как непосредственно в списке КО (выбран нажатием кнопки в столбце «Статус»), так и на странице редактирования данных КО.
- 2) Добавления КО в группу КО. Добавление выполняется либо при добавлении КО в список устройств, либо при редактировании учетной записи КО в поле «Группы» страницы создания/редактирования устройства. Кроме того, КО может быть добавлено в группу устройств непосредственно из списка устройств. Правила добавления КО в группу КО аналогичны правилам добавления АСО в группу АСО и приведены в п.п. 3.5.3.3.
- 3) Просмотра данных КО. Правила просмотра данных КО аналогичны правилам просмотра данных АСО и приведены в п.п. 3.5.3.5.

3.8 Просмотр и ведение списка групп КО

Для просмотра списка групп КО пользователю необходимо перейти на страницу раздела «Инфраструктура» подраздел «Конечные точки сети», выбрав в панели главного меню ссылку «Конечные точки сети» или, если панель свернута, – пиктограмму  и далее пиктограмму . Далее – перейти на вкладку «Группы». Вкладка содержит список всех групп КО, в которые объединены КО в ПК «Efros ACS».

На рис. 91 приведена страница с вкладкой «Устройства» для администраторов ACS.

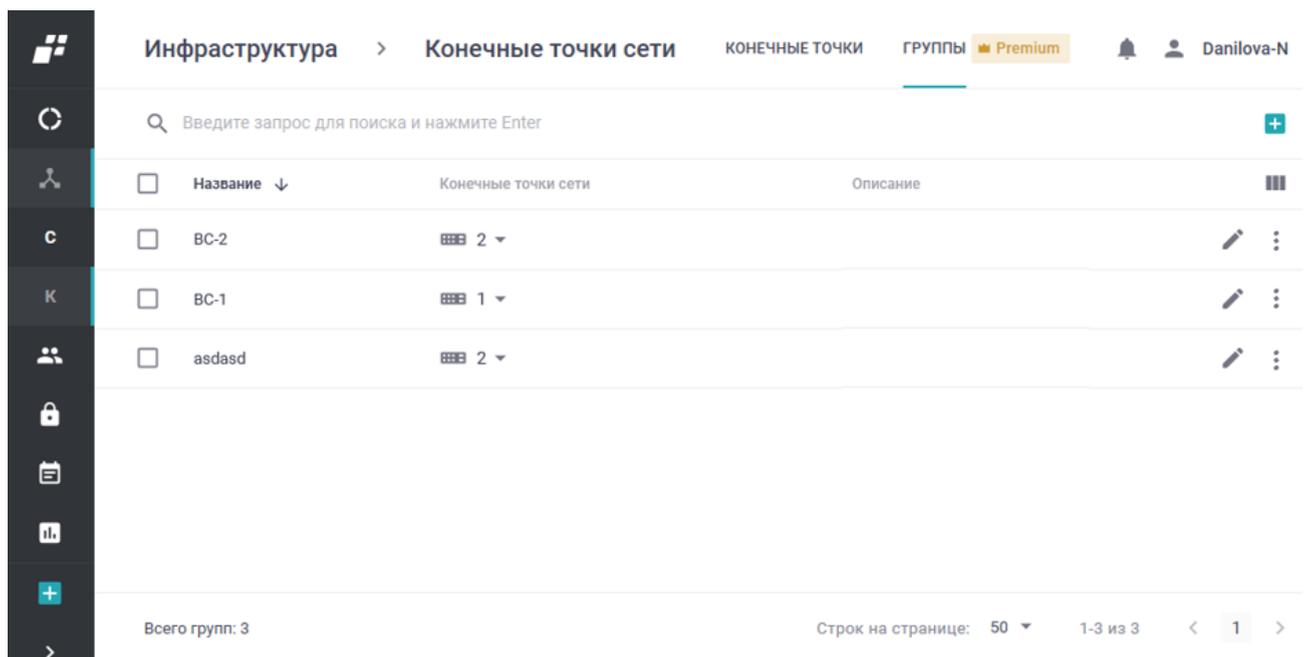


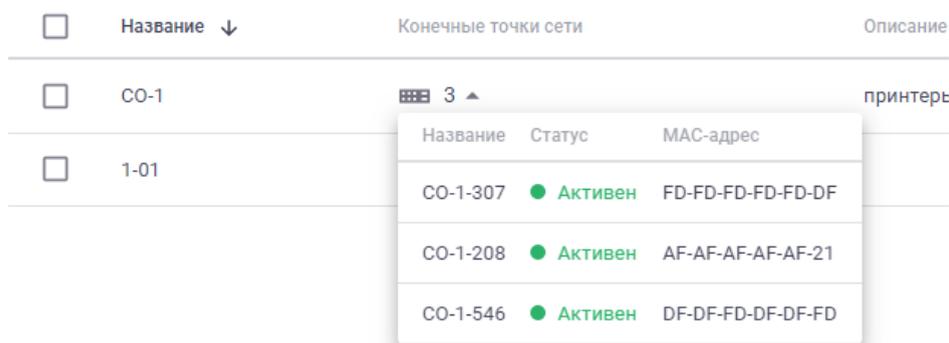
Рисунок 92 – Рисунок 91 – Страница списка групп КО для администратора ACS

i После установки ПК «Efros ACS» список групп КО пуст, на странице отображается сообщение «В системе нет групп конечных точек» и кнопка «Добавить» ([Добавить](#)) для перехода на страницу добавления новой группы КО.

Над таблицей располагается поле поиска. Правила поиска приведены в п. 3.2.2.

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

- название группы;
- количество КО, включенных в группу КО. Является ссылкой, при выборе которой раскрывается окно просмотра данных КО (рис. 92). При выборе названия одного из КО открывается страница просмотра/редактирования данных соответствующего КО;
- описание группы.



Название	Статус	MAC-адрес
CO-1-307	● Активен	FD-FD-FD-FD-FD-DF
CO-1-208	● Активен	AF-AF-AF-AF-AF-21
CO-1-546	● Активен	DF-DF-FD-DF-DF-FD

Рисунок 93 – Рисунок 92 – Окно просмотра данных КО, включенных в группу

Группы КО добавляются, редактируются или удаляются в ПК «Efros ACS» вручную администраторами ACS. Правила добавления, просмотра, редактирования и удаления групп КО аналогичны правилам ведения списка групп АСО и приведены в п. 3.6.2. Отличие групп КО от групп АСО заключается в отсутствии возможности назначения пользователей и групп пользователей, имеющих доступ к группам КО.

3.9 Просмотр и ведение списков пользователей и администраторов, групп пользователей

Для просмотра и ведения списков пользователей и администраторов, групп пользователей ПК «Efros ACS» пользователю необходимо перейти на страницу раздела «Учетные записи», выбрав в панели главного меню ссылку «Учетные записи» или, если панель свернута, – пиктограмму «».

Страница содержит отдельные вкладки ведения списков:

- «Пользователи» – пользователи ПК «Efros ACS» с ролью «Пользователь» (далее – пользователи);
- «Группы» – группы пользователей ПК «Efros ACS» с ролью «Пользователь»;
- «Администраторы» – пользователи ПК «Efros ACS» с ролями «ACS Администратор», «RO Администратор» и «CER Администратор» (далее – администраторы).

По умолчанию активной является вкладка «Пользователи», содержащая список всех пользователей, доступ к АСО которых контролируется ПК «Efros ACS».

Добавление нового пользователя выполняется администратором ACS вручную средствами веб-приложения ПК «Efros ACS» либо автоматически при импорте данных из ПК «Efros Config Inspector» (см. п.п. 3.4.4.1).

После установки и настройки ПК «Efros ACS» в БД ПК «Efros ACS» автоматически создается учетная запись пользователя с ролью «ACS Администратор»: с логином «administrator» и паролем «\$Qwerty123456\$» (далее – предустановленный

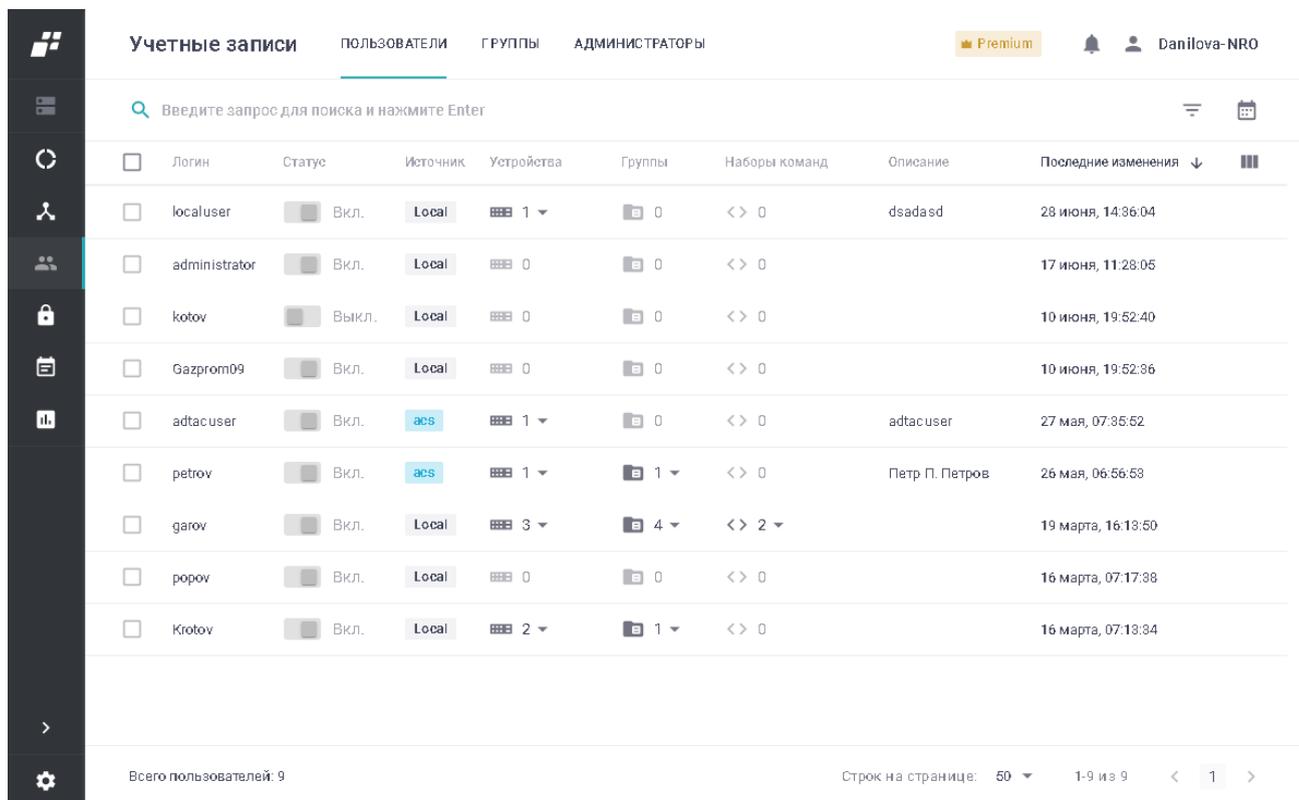
администратор ACS). Эта учетная запись отображается в таблице вкладки «Администраторы» и не доступна для редактирования и удаления. Добавление нового администратора выполняется администратором ACS вручную средствами веб-приложения ПК «Efros ACS».

Пользователи и администраторы могут быть как локальным пользователем ПК «Efros ACS», так и пользователем из внешней системы (LDAP, AD).

Примечание. После установки ПК «Efros ACS» списки раздела не содержат данные, кроме списка администраторов (содержит данные предустановленного администратора ACS), на странице отображается сообщение «В системе нет <название элемента списка>» и кнопка «Добавить» (Добавить) для перехода на страницу добавления нового элемента списка.

3.9.1. Просмотр списков пользователей и администраторов

На рис. 93 приведена страница с вкладкой «Пользователи» для администраторов RO, все данные доступны только для просмотра. На рис. 94 приведена страница с вкладкой «Пользователи» для администраторов ACS, данные доступны для редактирования. Состав и описание столбцов таблицы пользователей приведен в таблице 26.



Учетные записи	ПОЛЬЗОВАТЕЛИ	ГРУППЫ	АДМИНИСТРАТОРЫ	Premium	Данилова-NRO		
Логин	Статус	Источник	Устройства	Группы	Наборы команд	Описание	Последние изменения
localuser	Вкл.	Local	1	0	<> 0	dsada sd	28 июня, 14:36:04
administrator	Вкл.	Local	0	0	<> 0		17 июня, 11:28:05
kotov	Выкл.	Local	0	0	<> 0		10 июня, 19:52:40
Gazprom09	Вкл.	Local	0	0	<> 0		10 июня, 19:52:36
adtacuser	Вкл.	acs	1	0	<> 0	adtacuser	27 мая, 07:35:52
petrov	Вкл.	acs	1	1	<> 0	Петр П. Петров	26 мая, 06:56:53
garov	Вкл.	Local	3	4	<> 2		19 марта, 16:18:50
porov	Вкл.	Local	0	0	<> 0		16 марта, 07:17:38
Krotov	Вкл.	Local	2	1	<> 0		16 марта, 07:18:34

Всего пользователей: 9

Строк на странице: 50 1-9 из 9

Рисунок 94 – Рисунок 93 – Страница списка пользователей для администратора RO

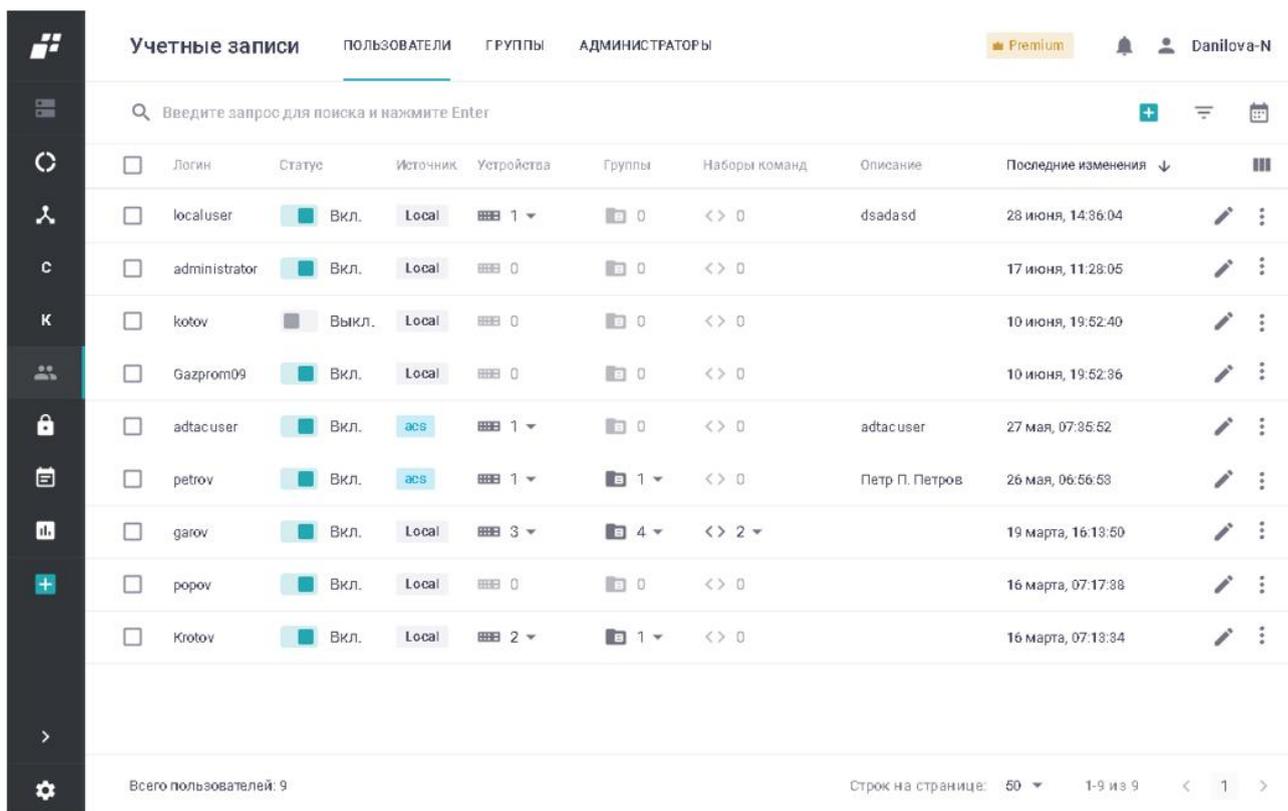


Рисунок 95 – Рисунок 94 – Страница списка пользователей для администратора ACS

Таблица 26 – Состав и описание столбцов таблицы пользователей

Столбец	Описание
Без названия	Содержит поля для флага. Предназначены для выбора записей для выполнения с ними дальнейших действий (создание копии, создание/редактирование группы пользователей, удаление выбранных пользователей). Поля доступны для редактирования (установки флага) только для администраторов ACS
Логин	Содержит логины пользователей
Статус	Содержит текущий статус пользователя: «Вкл» (активен) / «Выкл» (неактивен). Слева расположена кнопка смены статуса пользователя – в зависимости от текущего статуса кнопка имеет вид: «  » (отключить), «  » (активировать). Для администратора RO кнопки неактивны и отображаются в сером цвете. Администратор ACS не имеет возможности изменить статус для самого себя, для него кнопка «отключить» неактивна
Тип	Содержит пиктограмму:

Столбец	Описание
	<ul style="list-style-type: none"> — « Local », если учетная запись пользователя ПК «Efros ACS» локальная, не связана с учетной записью во внешней системе; — « acs », если учетная запись пользователя ПК «Efros ACS» связана с учетной записью во внешней системе. Текст в пиктограмме соответствует имени соединения из списка «Настройки системы» → «Внешние источники данных» → «LDAP», присвоенного внешней системе пользователя в ПК «Efros ACS»
Устройства	<p>Содержит данные о количестве доступных пользователям АСО.</p> <p>Количество является ссылкой, при выборе которой раскрывается список с данными АСО: название, IP-адрес, тип протокола</p>
Группа	<p>Содержит данные о количестве групп пользователей, в которые включен пользователь.</p> <p>Количество является ссылкой, при выборе которой раскрывается список с наименованиями групп. Наименование группы является ссылкой, при выборе которой открывается страница просмотра/редактирования данных группы пользователей</p>
Наборы команд	<p>Содержит пиктограммы «<>» и количество наборов команд, контролируемых при работе пользователя с АСО. Количество является ссылкой, при выборе которой раскрывается список с названиями наборов команд (список наборов команд ведется в разделе «Политики доступа» (см. п. 3.10)).</p> <p>При наведении курсора на название набора команд раскрывается окно со списком команд в соответствии с рис. 95. Для каждой команды указывается:</p> <ul style="list-style-type: none"> — тип действия: PERMIT (разрешить) или DENY (запретить); — команда; — аргумент команды
Описание	Содержит текст описания, введенный в карточках пользователей
Последние изменения	Содержит даты и время внесения последних изменений в данные пользователей
Без названия	<p>Столбец содержится в таблице только для администраторов ACS.</p> <p>Содержит кнопки:</p>

Столбец	Описание
	<p>— «Изменить» (✎) – для перехода на страницу редактирования карточки пользователя;</p> <p>— «Меню» (⋮) – для раскрытия меню с пунктами:</p> <p>а) «Добавить в группу» (+) – при выборе меню открывается окно выбора группы, в которую добавляется пользователь;</p> <p>б) «Создать копию» (📄) – при выборе меню открывается страница создания нового пользователя, поля которой заполнены данными пользователя из соответствующей кнопке записи (см. п.п. 3.9.4.3);</p> <p>в) «Удалить» (🗑) – для удаления соответствующей записи списка</p>

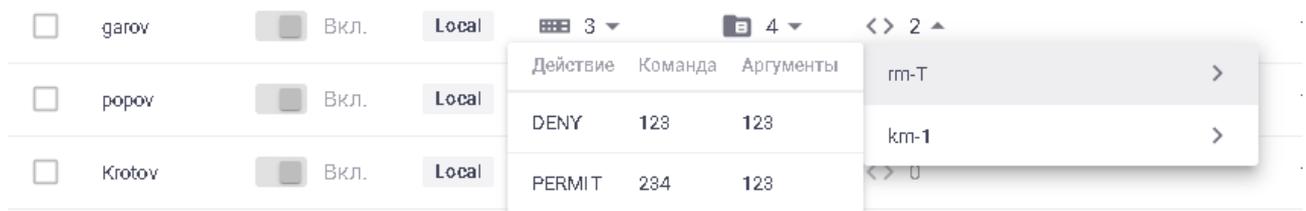


Рисунок 96 – Рисунок 95 – Окно со списком команд, контролируемых при работе пользователя с АСО

На рис. 96 приведена страница с вкладкой «Администраторы» для администраторов ACS, данные доступны для редактирования.

Логин	Статус	Источник	Описание	Последние изменения	
ACS\join	Вкл.	acs	join	2 июля, 14:58:47	
10\join	Вкл.	testLDAP	join	2 июля, 14:16:30	
Danilova-NRO	Вкл.	Local		2 июля, 07:46:50	
Zababurin-D	Вкл.	Local		2 июля, 07:48:09	
Shabanova-E	Выкл.	Local		2 июля, 07:48:04	
ACS\petrov	Вкл.	acs	Петр П. Петров	2 июля, 07:48:00	
Nebolsin-A	Вкл.	Local		2 июля, 07:42:57	
Makeev-M	Вкл.	Local		2 июля, 07:42:56	
test	Вкл.	Local		2 июля, 05:10:58	
Danilova-N	Вкл.	Local		1 июля, 13:36:40	
nick	Вкл.	Local		1 июля, 13:32:50	

Рисунок 97 – Рисунок 96 – Страница списка администраторов для администратора ACS

Состав и описание столбцов таблицы администраторов аналогичен составу таблицы пользователей (см. таблицу 26), за исключением следующего: столбцы «Устройства», «Группа» и «Наборы команд» отсутствуют, вместо кнопки «Меню» (⋮) содержится кнопка «Удалить» (🗑).

По умолчанию записи списков пользователей и администраторов отсортированы в порядке убывания даты и времени внесения последних изменений в данные пользователя.

Для администраторов ACS на страницах списков доступна кнопка «Добавить» (+) для перехода на страницу добавления нового пользователя или администратора.

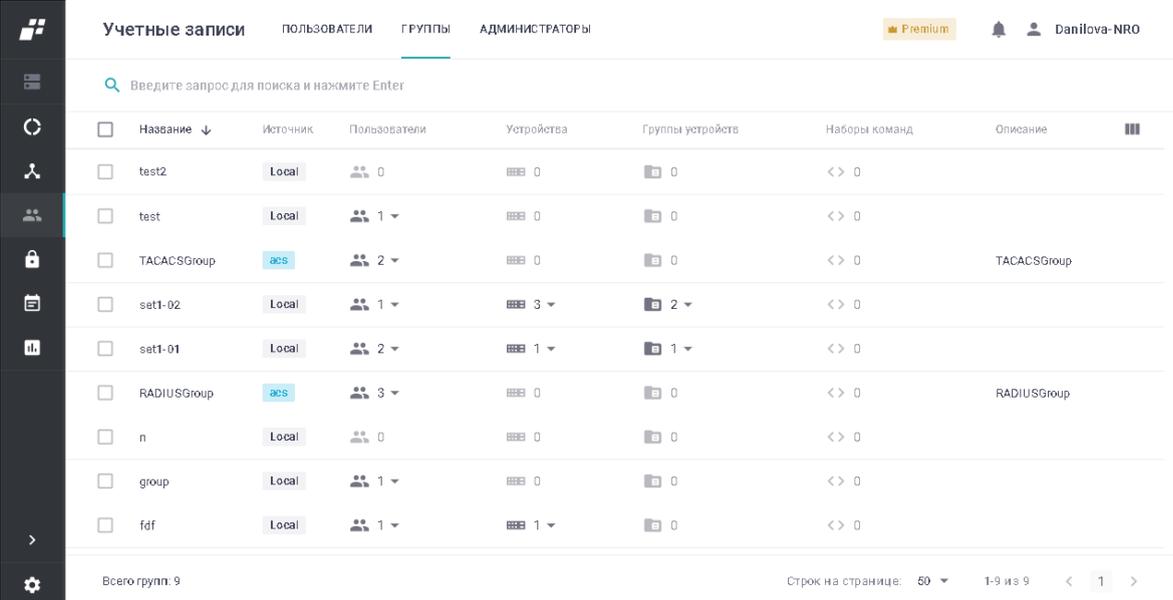
Над таблицей располагаются:

- поле поиска (🔍 Введите запрос для поиска и нажмите Enter). Правила поиска приведены в п. 3.2.2;
- кнопка «Добавить фильтр» (☰) – для перехода в окно фильтрации. Правила фильтрации приведены в п. 3.9.3;
- кнопка «Выбрать период» (📅) – правила выбора периода внесения последних изменений в данные пользователей приведены в п. 3.2.3.

3.9.2. Просмотр списка групп пользователей и данных групп пользователей

Для просмотра списка групп пользователей администратору необходимо перейти на страницу раздела «Учетные записи», выбрав в панели главного меню ссылку «Учетные записи» или, если панель свернута, – пиктограмму «». Далее – перейти на вкладку «Группы».

Вкладка содержит список всех групп пользователей, в которые объединены пользователи в ПК «Efros ACS». Группы пользователей добавляются, редактируются или удаляются в списке вручную администратором ACS. На рис. 97 приведена страница с вкладкой «Группы» для пользователей с ролью «RO Администратор», все данные доступны для просмотра. На рис. 98 приведена страница с вкладкой «Группы» для пользователей с ролью «ACS Администратор», данные доступны для редактирования. Состав и описание столбцов таблицы групп пользователей приведен в таблице 27.



<input type="checkbox"/>	Название ↓	Источник	Пользователи	Устройства	Группы устройств	Наборы команд	Описание	
<input type="checkbox"/>	test2	Local	 0	 0	 0	 0		
<input type="checkbox"/>	test	Local	 1 ▾	 0	 0	 0		
<input type="checkbox"/>	TACACSGroup	acs	 2 ▾	 0	 0	 0	TACACSGroup	
<input type="checkbox"/>	set1-02	Local	 1 ▾	 3 ▾	 2 ▾	 0		
<input type="checkbox"/>	set1-01	Local	 2 ▾	 1 ▾	 1 ▾	 0		
<input type="checkbox"/>	RADIUSGroup	acs	 3 ▾	 0	 0	 0	RADIUSGroup	
<input type="checkbox"/>	n	Local	 0	 0	 0	 0		
<input type="checkbox"/>	group	Local	 1 ▾	 0	 0	 0		
<input type="checkbox"/>	fdf	Local	 1 ▾	 1 ▾	 0	 0		

Всего групп: 9

Строк на странице: 50 ▾ 1-9 из 9 < 1 >

Рисунок 98 – Рисунок 97 – Страница списка групп пользователей для администратора RO

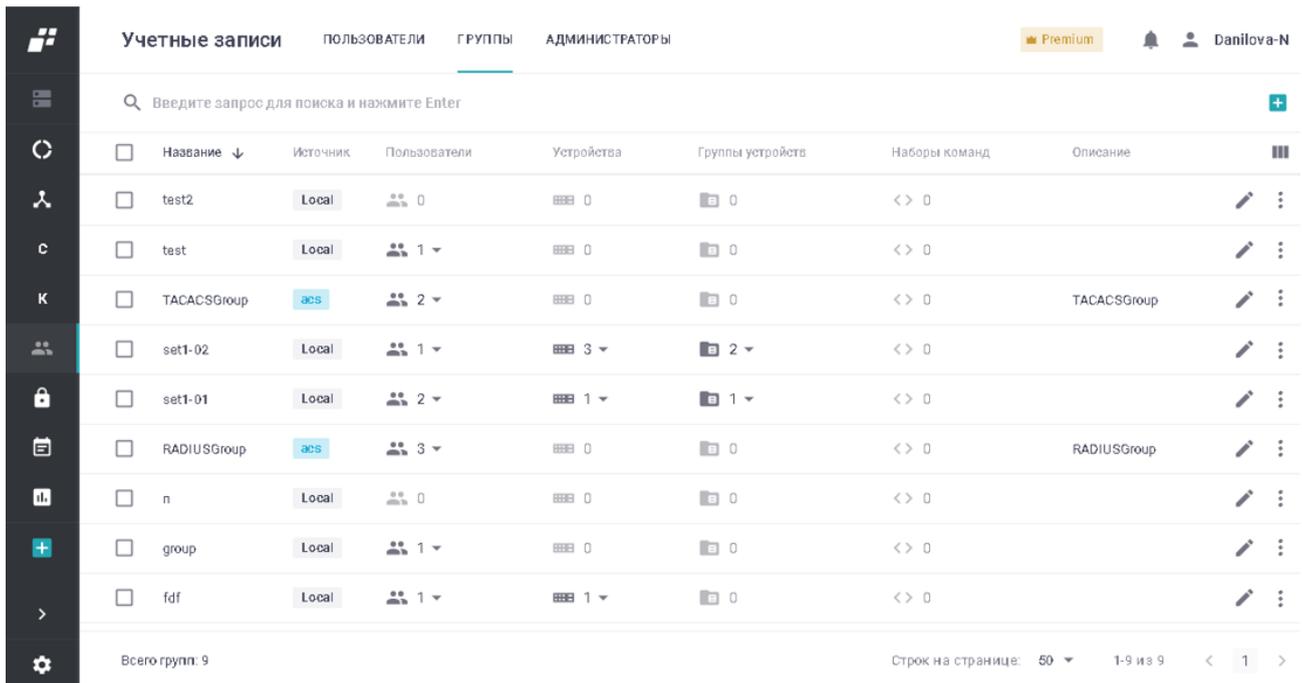


Рисунок 99 – Рисунок 98 – Страница списка групп пользователей для администратора ACS

Таблица 27 – Состав и описание столбцов таблицы групп пользователей

Столбец	Описание
Без названия	Содержит поля для флага. Предназначены для выбора записей для выполнения с ними дальнейших действий (создание копии, удаление выбранных групп). Поля доступны для редактирования (установки флага) только для администраторов ACS
Название	Содержит наименования групп пользователей
Описание	Содержит тексты описания, введенный в карточках групп пользователей
Тип группы	Содержит пиктограммы: <ul style="list-style-type: none"> — « Local » – соответствует локальным группам пользователей ПК «Efros ACS»; — « acs » – соответствует группам пользователей ПК «Efros ACS» связанным с группами пользователей во внешней системе. Текст в пиктограмме соответствует имени соединения из списка «Настройки системы» → «Внешние

Столбец	Описание
	источники данных» → «LDAP», присвоенного внешней системе группы в ПК «Efros ACS»
Пользователи	<p>Содержит пиктограммы «» и количество пользователей, включенных в группу. Количество является ссылкой, при выборе которой раскрывается список с данными пользователей:</p> <p>1. Для локальных групп в списке содержатся данные пользователей:</p> <ul style="list-style-type: none">— логин;— статус (активен, неактивен);— тип (локальный () или из внешней системы ()). <p>Логин пользователя является ссылкой, при выборе которой открывается страница просмотра (для администратора RO)/редактирования (для администратора ACS) данных пользователя.</p> <p>2. Для групп из внешних систем в списке содержатся только логины пользователей. Переход на страницу данных пользователя не выполняется</p>
Устройства	<p>Содержит пиктограммы «» и количество АСО, доступных пользователям группы. Количество является ссылкой, при выборе которой раскрывается список с данными АСО:</p> <ul style="list-style-type: none">— название;— IP-адрес;— тип протокола. <p>Название АСО является ссылкой, при выборе которой открывается страница просмотра (для администратора RO)/редактирования (для администратора ACS) данных АСО</p>
Группы устройств	<p>Содержит пиктограммы «» и количество групп АСО, доступных пользователям группы. Количество является ссылкой, при выборе которой раскрывается список с названиями групп АСО.</p> <p>Название группы АСО является ссылкой, при выборе которой открывается страница просмотра (для администратора RO)/редактирования (для администратора ACS) данных группы АСО</p>

Столбец	Описание
Наборы команд	<p>Содержит пиктограммы «<>» и количество наборов команд, контролируемых при работе пользователей группы с АСО. Количество является ссылкой, при выборе которой раскрывается список с названиями наборов команд (список наборов команд ведется в разделе «Политики доступа» (см. п. 3.10)).</p> <p>При наведении курсора на название набора команд раскрывается окно со списком команд в соответствии с рис. 99. Для каждой команды указывается:</p> <ul style="list-style-type: none"> — тип действия: PERMIT (разрешить) или DENY (запретить); — команда; — аргумент команды
Без названия	<p>Столбец содержится в таблице только для администраторов ACS. Содержит кнопки:</p> <ul style="list-style-type: none"> — «Изменить» (✎) – для перехода на страницу редактирования карточки группы пользователей; — «Меню» (⋮) – для раскрытия меню с пунктами: <ul style="list-style-type: none"> а) «Создать копию» (📄) – при выборе меню открывается страница создания новой группы пользователей, поля которой заполнены данными группы пользователей из соответствующей кнопке записи (см. п.п. 3.9.5.3); б) «Удалить» (🗑) – для удаления соответствующей записи списка

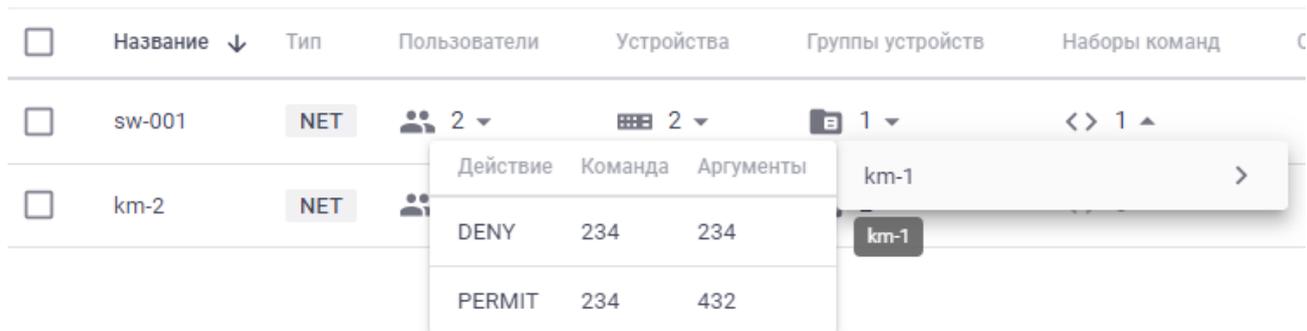


Рисунок 100 – Рисунок 99 – Окно со списком команд, включенных в набор команд «km-1»

Для администраторов ACS на странице доступна кнопка «Добавить» (+) для перехода на страницу добавления новой группы пользователей.

3.9.3. Фильтрация данных в таблицах пользователей и администраторов

Для фильтрации данных в таблицах пользователей и администраторов необходимо нажать над таблицей кнопку «Добавить фильтр» (≡). Откроется окно фильтрации. На рис. 100 приведено окно фильтрации для списка администраторов. Состав элементов окна и правила их заполнения приведены в таблице 28.

i В окне фильтрации списка пользователей:

- на вкладке «Пользователи» – отсутствует поле «Тип»;
- в окне выбора пользователей для включения их в группу – отсутствуют поля «Тип» и «Аутентификация».

Рисунок 101 – Рисунок 100 – Окно фильтрации

Таблица 28 – Состав и описание элементов окна фильтрации списка пользователей и администраторов

Элемент	Описание
Поле «Статус пользователя»	Поле-переключатель с положениями: — «Все» – в таблице содержатся записи всех пользователей/администраторов;

Элемент	Описание
	<ul style="list-style-type: none"> — «Активен» – в таблице содержатся записи пользователей/администраторов в статусе «Активен»; — «Не активен» – в таблице содержатся записи пользователей/администраторов в статусе «Не активен». <p>По умолчанию переключатель установлен в поле «Все»</p>
Поле «Тип»	<p>Поле-переключатель с положениями:</p> <ul style="list-style-type: none"> — «Все» – в таблице содержатся записи администраторов всех ролей; — «ACS» – в таблице содержатся записи пользователей с ролью «ACS Администратор»; — «RO» – в таблице содержатся записи пользователей с ролью «RO Администратор»; — «CER» – в таблице содержатся записи пользователей с ролью «CER Администратор». <p>По умолчанию переключатель установлен в поле «Все»</p>
Поле «Аутентификация»	<p>Поле-переключатель с положениями:</p> <ul style="list-style-type: none"> — «Все» – в таблице будут содержаться записи локальных пользователей\администраторов и пользователей/администраторов, учетная карточка которых связана с учетной карточкой пользователя внешней системы; — «LDAP» – в таблице будут содержаться записи пользователей/администраторов, учетная карточка которых связана с учетной карточкой пользователя внешней системы; — «Локальный пользователь» – в таблице будут содержаться записи локальных пользователей/администраторов. <p>По умолчанию выбрано значение «Все»</p>
Кнопки управления	
Применить	По нажатию кнопки окно фильтрации закрывается, введенные настройки фильтрации применяются

Элемент	Описание
Отменить	По нажатию кнопки окно фильтрации закрывается без применения введенных настроек

Далее необходимо:

- выбрать нажатием кнопки статус пользователей/администраторов;
- выбрать установкой переключателя в поле «Тип» роль администратора;
- выбрать установкой переключателя в поле «Аутентификация» тип аутентификации пользователя/администратора (все, локальный или связан с внешней системой);
- нажать кнопку «Применить».

После чего:

- окно фильтрации закроется;
- в таблице отобразятся записи пользователей/администраторов, соответствующие заданным параметрам фильтрации;
- слева от поля поиска отобразятся поля с заданными параметрам фильтрации.

Для отмены заданных правил фильтрации и отображения в таблице всех записей необходимо нажать кнопку «Очистить» () в каждом поле отдельно.

3.9.4. Ведение списка пользователей

3.9.4.1. Добавление пользователя с ролью «Пользователь»

Добавление нового пользователя выполняется администратором вручную средствами веб-приложения ПК «Efros ACS» либо автоматически при импорте данных из системы «Cisco ACS» (см. п.п. 3.4.4.3). Пользователь может быть, как локальным пользователем ПК «Efros ACS», так и пользователем из внешней системы.

Для добавления в список нового пользователя необходимо:

- 1) Нажать на странице списка пользователей (см. рис. 94) над таблицей кнопку «Добавить» или нажать в панели главного меню кнопку «Добавить» и выбрать в открывшемся меню пункты «Учетные записи» - «Пользователь». Откроется страница добавления пользователя, приведенная на рис. 101. Состав и описание элементов страницы приведены в таблице 29.
- 2) Выбрать установкой переключателя тип пользователя: локальный («Локальный») или из внешней системы («LDAP»).

- 3) Выбрать установкой переключателя в поле «Статус» текущий статус пользователя.
- 4) Заполнить поля страницы «Логин», «Пароль», «Группы пользователей» данными добавляемого пользователя в соответствии с правилами, приведенными в таблице 29, в зависимости от вида пользователя: локальный или пользователь внешней системы.
- 5)

! В поле «Группы пользователей» для выбора доступны только локальные группы пользователей, не имеющие связанной группы пользователей во внешней системе!

Рисунок 102 – Рисунок 101 – Страница добавления пользователя

Таблица 29 – Состав и описание элементов страницы добавления пользователя

Элемент	Описание
Поле «Тип пользователя»	Поле-переключатель с двумя положениями для выбора типа добавляемого пользователя. Содержит значения:

Элемент	Описание
	<ul style="list-style-type: none">— «Локальный» – локальный пользователь:— «LDAP» – пользователь из внешней системы – LDAP источника данных. <p>От выбранного положения переключателя зависит состав полей страницы добавления пользователя</p>
*Поле «Статус»	<p>Поле-переключатель с двумя положениями для выбора статуса пользователя:</p> <ul style="list-style-type: none">— «Активен» – пользователю разрешен доступ к устройствам в соответствии с заданными в ПК «Efros ACS» правами;— «Неактивен» – пользователю закрыт доступ к устройствам, контролируемым ПК «Efros ACS». <p>По умолчанию переключатель установлен в положение «Активен»</p>
Группа полей «Основные настройки»	
*Поле «Логин»	<p>Текстовое поле для ввода логина пользователя (до 50 символов).</p> <p>Если пользователь является:</p> <ul style="list-style-type: none">— локальным пользователем ПК «Efros ACS», то поле заполняется путем ввода логина в поле вручную;— пользователем внешней системы, то поле заполняется путем выбора логина из списка пользователей внешней системы, который открывается в поле после ввода последовательности символов из логина пользователя во внешней системе (не менее 3 символов)
*Поле «Пароль»	<p>Текстовое поле для ввода пароля пользователя. Отображается на странице только для локальных пользователей.</p> <p>Пароль должен соответствовать требованиям, заданным при настройке парольной политики, подробное описание приведено в п. 3.4.7.</p>

Элемент	Описание
	При вводе символы пароля заменяются знаком «●». Для просмотра введенного значения необходимо нажать в поле ввода кнопку «Просмотреть» (👁)
Поле «Описание»	Текстовое поле (до 250 символов). Если пользователь является: <ul style="list-style-type: none"> — локальным пользователем ПК «Efros ACS», то поле отображается на странице только после нажатия кнопки «Добавить описание», заполняется путем ввода текста описания в поле вручную. Под полем отображается кнопка «Удалить описание», по нажатию которой поле «Описание» очищается и удаляется; — пользователем внешней системы, то поле заполняется автоматически после выбора логина пользователя в поле «Логин» значением поля «Display Name» карточки пользователя во внешней системе
Поле «Группы пользователей»	Поле со списком для выбора одной или нескольких групп, в которые входит пользователь. Список содержит поле поиска и названия групп, имеющих в списке «Учетные записи → Группы». <p>После выбора групп в поле отображается их общее количество</p>
Группа полей «Доступы»	
Поле «Устройства»	Поле со списком для выбора устройств, к которым должен получить доступ пользователь. Список содержит поле поиска и названия АСО, имеющих в списке «Инфраструктура → Сетевое оборудование → Устройства». <p>После выбора АСО в поле отображается их общее количество</p>
Поле «Группы устройств»	Поле со списком для выбора групп устройств, к которым должен получить доступ пользователь. Список содержит поле поиска и названия групп АСО, имеющих в списке «Инфраструктура → Сетевое оборудование → Группы». <p>После выбора групп АСО в поле отображается их общее количество</p>
Панель настройки службы выполнения команд (рис. 102).	

Элемент	Описание
	<p>Раскрывается после установки переключателя «Служба выполнения команд» в положение «Включен» ().</p> <p>Внимание: Настройки службы выполнения команд пользователя имеют приоритет над настройками службы выполнения команд группы пользователей (см. п.п. 3.9.5.1)!</p>
*Поле «Привилегированный режим»	<p>Поле со списком для выбора режима привилегированного режима при работе с устройством. Содержит значения:</p> <ul style="list-style-type: none">— «Отключен» – отключение настройки привилегированного режима;— «Задать пароль» – привилегированный режим доступен по заданному в ПК «Efros ACS» паролю для привилегированного доступа (см. ниже поле «Пароль»);— «Разрешить без пароля» – привилегированный режим доступен без пароля;— «Запретить» – установка принудительного запрета на использование привилегированного режима пользователем;— «Использовать пароль пользователя» – привилегированный режим доступен по заданному в ПК «Efros ACS» паролю пользователя (см. выше поле «Пароль»)
*Поле «Пароль»	<p>Поле отображается только после выбора в поле «Привилегированный режим» значения «Задать пароль». Предназначено для ввода пароля авторизации пользователя для доступа к АСО в привилегированном режиме. Требования к вводимому значению аналогичны требованиям, приведенным выше для поля «Пароль»</p>
*Поле «Команды по умолчанию»	<p>Поле-переключатель с двумя положениями:</p> <ul style="list-style-type: none">— «Выполнять» – пользователю разрешено выполнение команд по умолчанию на устройстве;— «Не выполнять» – пользователю запрещено выполнение команд по умолчанию на устройстве. <p>По умолчанию переключатель установлен в положение «Не выполнять»</p>

Элемент	Описание
*Поле «Наборы команд»	Поле со списком для выбора набора команд, разрешенных или запрещенных пользователю для выполнения на АСО. Список содержит поле поиска и названия наборов команд, имеющихся в списке «Политики доступа → Наборы команд». После выбора наборов команд в поле отображается их общее количество
Панель доступа устройства «Время на»	Панель (рис. 103) предназначена для ограничения времени доступа пользователя на АСО. Раскрывается после установки переключателя «Время доступа на устройства» в положение «Включен» () Содержит поля «Начало» и «Конец» для ввода значений соответственно начала и окончания временного интервала доступа пользователя на устройство. Время начала должно быть меньше времени конца. Если панель активирована и заполнена, то вне указанного периода времени доступ пользователю к АСО запрещен
Кнопки управления	
Добавить	По нажатию кнопки выполняется переход на страницу списка пользователей с сохранением внесенных данных
Отменить	По нажатию кнопки выполняется переход на страницу списка пользователей без сохранения внесенных данных
Сбросить	Кнопка отображается на странице после заполнения хотя бы одного поля. По нажатию кнопки все введенные данные в окне удаляются
* – Справа от поля расположен знак «  », при наведении на который курсора открывается всплывающая подсказка с правилами заполнения поля	

 Служба выполнения команд

Привилегированный режим 

Отключен 

Команды по умолчанию 

Выполнять  Не выполнять 

Наборы команд 



Рисунок 103 – Рисунок 102 – Раскрытая панель настройки службы выполнения команд

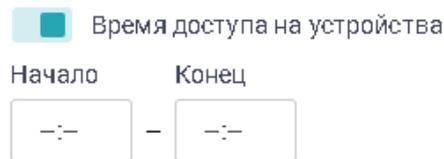


Рисунок 104 –

Рисунок 105 – Рисунок 103 – Раскрытая панель «Время доступа на устройства»

- 6) Добавить, при необходимости, описание для локального пользователя, нажав кнопку «Добавить описание» и заполнив отобразившееся поле «Описание».
- 7) Назначить доступные пользователю устройства и группы устройств, выбрав в полях панели «Доступ» требуемые АСО и группы АСО.
- 8) Выполнить настройку службы выполнения команд, для чего:
 - установить переключатель «Служба выполнения команд» в положение «Включен» ();
 - включить (выбором требований к паролю), отключить или запретить работу пользователя на устройстве в привилегированном режиме, выбрав в поле «Привилегированный режим» требуемое значение (см. таблицу 29);
 - если в поле «Привилегированный режим» выбрано значение «Задать пароль», ввести в добавленном поле «Пароль» пароль пользователя для доступа к устройству в привилегированном режиме;
 - установкой переключателя «Команды по умолчанию» в положение «Выполнять» или «Не выполнять» соответственно разрешить или запретить пользователю выполнение команд «по умолчанию» на устройстве;
 - выбрать установкой флагов в поле «Наборы команд» наборы команд, которые запрещены или разрешены пользователю для выполнения на устройстве.
- 9) Ограничить, при необходимости, время доступа пользователя на устройство, для чего:
 - установить переключатель «Время доступа на устройства» в положение «Включен» ();
 - ввести требуемые значения в поля «Начало» и «Конец».
- 10) Нажать в окне добавления пользователя кнопку «Добавить».

Будет запущен процесс проверки заполненности всех обязательных полей и уникальности добавляемого пользователя по логину.

 Допускается наличие нескольких пользователей с одинаковым логином разных типов – локальный или из внешней системы (в том числе несколько пользователей из нескольких внешних систем). Таким пользователям в списке «Пользователи» ПК «Efros ACS» не может быть назначено доступным одно и то же устройство. Если на шаге 6 было выбрано устройство, уже доступное другому пользователю с тем же логином ранее, то отобразится сообщение об ошибке. При необходимости выдачи пользователям прав доступа на это устройство, необходимо добавить пользователей в группу пользователей, имеющую доступ к устройству.

При обнаружении незаполненных обязательных полей, рядом с первым из таких полей отобразится всплывающая подсказка «Обязательное поле», в случае обнаружения в списке дубликата пользователя в верхней части страницы отобразится соответствующее сообщение. Администратору необходимо корректно заполнить поля окна и повторно нажать кнопку «Добавить».

Если проверки завершились без обнаружения ошибок, то окно добавления закрывается, пользователь добавляется в список пользователей, перезапускаются службы протоколов TACACS+ и RADIUS для применения новых настроек. Доступ к устройствам в соответствии с заданными настройками пользователь получит после успешного перезапуска служб.

В журнал событий ПК «Efros ACS» будет внесено сообщение:

- при успешном завершении – сообщение типа «Инфо» в формате: «Администратор {имя_выполняющего_операцию_администратора}: Пользователь {имя_пользователя} успешно создан»;
- при обнаружении ошибки – сообщение типа «Ошибка» в формате: «Администратор {имя_выполняющего_операцию_администратора}: Ошибка создания пользователя - {текст_ошибки}».

3.9.4.2. Добавление пользователя с административной ролью

Добавление нового администратора выполняется администратором ACS вручную средствами веб-приложения ПК «Efros ACS». Администратор может быть, как локальным пользователем ПК «Efros ACS», так и пользователем из внешней системы.

Для добавления в список нового администратора необходимо:

- 1) Нажать на странице списка администраторов (см. рис. 96) над таблицей кнопку «Добавить» или нажать в панели главного меню кнопку «Добавить» и выбрать в открывшемся меню пункты «Учетные записи»–«Администратор». Откроется страница добавления администратора, приведенная на рис. 104. Состав и описание элементов страницы приведены в таблице 30.

Рисунок 106 – Рисунок 104 – Страница добавления администратора

Таблица 30 – Состав и описание элементов страницы добавления администратора

Элемент	Описание
Поле «Тип пользователя»	Поле-переключатель с двумя положениями для выбора типа добавляемого пользователя. Содержит значения: <ul style="list-style-type: none"> — «Локальный» – локальный пользователь; — «LDAP» – пользователь из внешней системы. От выбранного положения переключателя зависит состав полей страницы добавления пользователя
*Поле «Статус»	Переключатель с двумя положениями: <ul style="list-style-type: none"> — «Активен» (🟢) – администратору разрешен доступ к приложению в соответствии с заданными в ПК «Efras ACS» правами; — «Неактивен» (🔴) – администратору закрыт доступ к приложению ПК «Efras ACS». По умолчанию переключатель установлен в положение «Активен»

Элемент	Описание
*Поле «Логин»	<p>Текстовое поле для ввода логина администратора (до 50 символов).</p> <p>Если администратор является:</p> <ul style="list-style-type: none">— локальным пользователем ПК «Efros ACS», то поле заполняется путем ввода логина в поле вручную;— пользователем внешней системы, то поле заполняется путем выбора логина из списка пользователей внешней системы, который открывается в поле после ввода последовательности символов из логина пользователя во внешней системе (не менее 3 символов)
*Поле «Пароль»	<p>Текстовое поле для ввода пароля пользователя. Отображается на странице только для локальных пользователей.</p> <p>Пароль должен соответствовать требованиям, заданным при настройке парольной политики, подробное описание приведено в п. 3.4.7.</p> <p>При вводе символы пароля заменяются знаком «●». Для просмотра введенного значения необходимо нажать в поле ввода кнопку «Просмотреть» (👁)</p>
Поле «Описание»	<p>Текстовое поле (до 250 символов). Если пользователь является:</p> <ul style="list-style-type: none">— локальным пользователем ПК «Efros ACS», то поле отображается на странице только после нажатия кнопки «Добавить описание», заполняется путем ввода текста описания в поле вручную. Под полем отображается кнопка «Удалить описание», по нажатию которой поле «Описание» очищается и удаляется;— пользователем внешней системы, то поле заполняется автоматически после выбора логина пользователя в поле «Логин» значением поля «Display Name» карточки пользователя во внешней системе
Группа полей «Уровень доступа»/*Поле «Роль администратора»	<p>Переключатель с тремя положениями:</p> <ul style="list-style-type: none">— «Полный доступ» – администратору будет назначена роль «ACS Администратор»— «Выпуск сертификатов» – администратору будет назначена роль «СЕР Администратор»;

Элемент	Описание
	— «Только просмотр» – администратору будет назначена роль «RO Администратор»
Группа полей «Подчиненные серверы»	<p>Содержит поля со списком:</p> <ul style="list-style-type: none"> — «Сервер» – для выбора из списка подчиненных серверов ПК «Efros ACS» сервера, к которому назначается доступ пользователю; — «Уровень доступа» – для выбора из списка возможных уровней доступа «Полный доступ» и «Только просмотр» уровень доступа пользователя к подчиненному серверу. <p>Добавление новых серверов в список выполняется по нажатию кнопки «Добавить» (+) в строке предыдущего сервера. Удаление неактуальных записей в списке выполняется по нажатию кнопки «Удалить» (-) в строке удаляемого сервера.</p> <p>Примечание. Доступ пользователя к подчиненному серверу может быть назначен также в карточке подчиненного сервера (см. п. 3.4.8)</p>
Кнопки управления	
Добавить	По нажатию кнопки выполняется переход на страницу списка администраторов с сохранением внесенных данных
Отменить	По нажатию кнопки выполняется переход на страницу списка администраторов без сохранения внесенных данных
Сбросить	Кнопка отображается на странице после заполнения хотя бы одного поля. По нажатию кнопки все введенные данные в окне удаляются
* – Справа от поля расположен знак «?», при наведении на который курсора открывается всплывающая подсказка с правилами заполнения поля	

- 2) Выбрать установкой переключателя тип пользователя: локальный («Локальный») или из внешней системы («LDAP»).
- 3) Выбрать установкой переключателя в поле «Статус» текущий статус администратора.
- 4) Заполнить поля страницы «Логин», «Пароль» данными добавляемого администратора в соответствии с правилами, приведенными в таблице 30, в зависимости от вида администратора: локальный или пользователь внешней системы.

- 5) Добавить, при необходимости, описание для локального пользователя, нажав кнопку «Добавить описание» и заполнив отобразившееся поле «Описание».
- 6) Выбрать установкой переключателя роль администратора «Полный доступ», «Выпуск сертификатов» или «Только просмотр».
- 7) Назначить, при необходимости, доступ пользователю к подчиненным серверам. Для выдачи доступа к одному серверу – выбрать в полях «Сервер» и «Уровень доступа» соответственно требуемый подчиненный сервер и уровень доступа к нему пользователя: «Полный доступ» или «Только просмотр». Для добавления другого подчиненного сервера – нажать кнопку «Добавить» (+) и заполнить поля «Сервер» и «Уровень доступа».
- 8) Нажать в окне добавления администратора кнопку «Добавить».

Будет запущен процесс проверки заполненности всех обязательных полей и уникальности добавляемого администратора по логину.

При обнаружении незаполненных обязательных полей рядом с первым из таких полей отобразится всплывающая подсказка «Обязательное поле», в случае обнаружения в списке дубликата администратора в верхней части страницы отобразится соответствующее сообщение. Администратору ACS необходимо корректно заполнить поля окна и повторно нажать кнопку «Добавить».

Если проверки завершились без обнаружения ошибок, то окно добавления закрывается, администратор добавляется в список администраторов.

В журнал событий ПК «Efros ACS» будет внесено сообщение:

- при успешном завершении – сообщение типа «Инфо» в формате: «Администратор {имя_выполняющего_операцию_администратора}: Пользователь {имя_пользователя} успешно создано»;
- при обнаружении ошибки – сообщение типа «Ошибка» в формате: «Администратор {имя_выполняющего_операцию_администратора}: Ошибка создания пользователя - {текст_ошибки}».

3.9.4.3. Добавление пользователя/администратора путем копирования записи имеющегося пользователя/администратора

Для добавления нового пользователя/администратора путем копирования записи имеющегося пользователя/администратора администратору ACS необходимо:

- 1) Выбрать установкой флага в левой крайней графе таблицы списка пользователей/администраторов исходного пользователя/администратора и нажать в отобразившейся в верхней части таблицы строке выбора операций (рис. 105) кнопку «Создать копию» (□) либо нажать в строке исходного

пользователя/администратора кнопку «Меню» (⋮) и выбрать в раскрывшемся меню пункт «Создать копию» (📄).

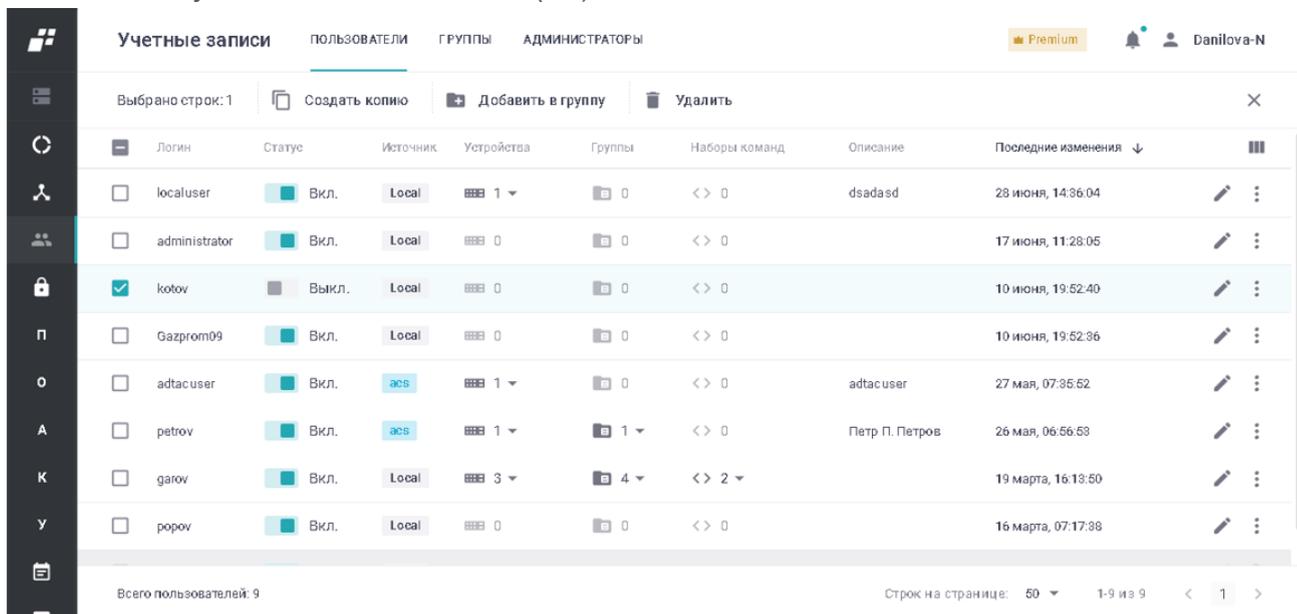


Рисунок 107 – Рисунок 105 – Страница списка пользователей со строкой выбора операций

- 2) Откроется страница добавления нового пользователя/администратора, аналогичная приведенной на рис. 101/104. Все поля страницы будут заполнены данными исходного пользователя/администратора, кроме поля «Логин» и «Описание».
- 3) Далее пользователю необходимо внести требуемые изменения и нажать кнопку «Добавить». Правила заполнения полей страниц аналогичны правилам добавления пользователя/администратора (см. п.п. 3.9.4.1, 3.9.4.2).

Будет запущен процесс проверки заполненности всех обязательных полей и уникальности добавляемого пользователя/администратора по логину.

i Допускается наличие нескольких пользователей с одинаковым логином разных типов – локальный или из внешней системы (в том числе несколько пользователей из нескольких внешних систем). Таким пользователям в ПК «Efros ACS» не может быть назначено доступным одно и то же устройство, если было выбрано устройство уже доступное другому пользователю с тем же логином ранее, то отобразится сообщение об ошибке.

i Допускается наличие нескольких пользователей с одинаковым логином разных типов – локальный или из внешней системы (в том числе несколько пользователей

из нескольких внешних систем). Таким пользователям в списке «Пользователи» ПК «Efros ACS» не может быть назначено доступным одно и то же устройство. При необходимости выдачи пользователям прав доступа на это устройство необходимо добавить пользователей в группу пользователей, имеющую доступ к устройству.

При обнаружении незаполненных обязательных полей рядом с первым из таких полей отобразится всплывающая подсказка «Обязательное поле», в случае обнаружения в списке дубликата пользователя/администратора в верхней части страницы отобразится соответствующее сообщение. Администратору ACS необходимо корректно заполнить поля окна и повторно нажать кнопку «Добавить».

Если проверки завершились без обнаружения ошибок, то окно добавления закрывается, пользователь/администратор добавляется в список администраторов.

В журнал событий ПК «Efros ACS» будет внесено сообщение:

- при успешном завершении – сообщение типа «Инфо» в формате: «Администратор {имя_выполняющего_операцию_администратора}: Пользователь {имя_пользователя} успешно создано»;
- при обнаружении ошибки – сообщение типа «Ошибка» в формате: «Администратор {имя_выполняющего_операцию_администратора}: Ошибка создания пользователя - {текст_ошибки}».

3.9.4.4. Добавление пользователя в группу пользователей

Добавление пользователя в группу пользователей выполняется либо при его добавлении в список пользователей (см. п.п. 3.9.4.1 и 3.9.4.3), либо при редактировании учетной записи пользователя (см. п.п. 3.9.4.5) в поле «Группы» страницы создания/редактирования пользователя. Кроме того, пользователь может быть добавлен в группу пользователей непосредственно из списка пользователей.

Для добавления пользователя в группу пользователей из списка пользователей администратору ACS необходимо:

- 1) Выбрать установкой флага в левой крайней графе таблицы списка пользователей добавляемого пользователя и нажать в отобразившейся в верхней части таблицы строке выбора операций (см. рис. 105) кнопку «Добавить в группу» (+) либо нажать в строке исходного пользователя/администратора кнопку «Меню» (⋮) и выбрать в раскрывшемся меню пункт «Добавить в группу» (+).
- 2) Откроется окно выбора группы пользователей, приведенное на рис. 106.
- 3) Выбрать в раскрывающемся списке групп пользователей окна наименование требуемой группы.

- 4) Нажать кнопку «Добавить». Окно закроеся. В указанную группу будет добавлен выбранный на шаге 1 пользователь.

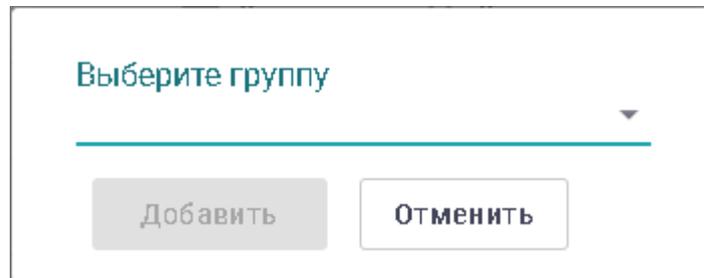


Рисунок 108 – Рисунок 106 – Окно выбора группы пользователей

Будет запущен процесс проверки корректности данных группы и уникальности пользователя по логину.

Если проверки завершились без обнаружения ошибок, то пользователь добавляется в группу, перезапускаются службы протоколов TACACS+ и RADIUS для применения новых настроек. Контроль доступа пользователя к АСО с обновленными правами будет осуществляться после успешного перезапуска служб.

В журнал событий ПК «Efros ACS» будут внесены сообщения:

- 1) При успешном завершении – сообщения типа «Инфо» в формате:
 - «Администратор{имя_выполняющего_операцию_администратора}: Успешно обновлён пользователь {имя_пользователя}»;
 - «Администратор {имя_выполняющего_операцию_администратора}: Группа пользователей {название_группы_пользователей} успешно обновлена».
- 2) При обнаружении ошибки – сообщения типа «Ошибка» в формате:
 - «Администратор {имя_выполняющего_операцию_администратора}: Ошибка обновления пользователя {имя_пользователя} - {текст_ошибки}»;
 - «Администратор {имя_выполняющего_операцию_администратора}: Ошибка обновления группы пользователей - {текст_ошибки}».

3.9.4.5. Редактирование пользователя/администратора

Редактирование данных пользователей/администраторов выполняется администратором ACS вручную средствами веб-приложения ПК «Efros ACS».

Для редактирования данных администратору ACS необходимо выбрать в списке с помощью «мыши» логин требуемого пользователя либо нажать в строке пользователя/администратора кнопку «Изменить» (✎). Откроется страница редактирования данных пользователя/администратора. Страница содержит внесенные

ранее данные. Состав элементов страниц аналогичен составу страниц добавления пользователя/администратора (см. п.п. 3.9.4.1 и п.п. 3.9.4.2).

При редактировании локальных пользователей/администраторов для изменения доступны все данные пользователя, кроме поля «Тип пользователя».

 В режиме редактирования пароль пользователя/администратора, заданный ранее не доступен для просмотра, но поле «Пароль» доступно для редактирования. Администратор ACS имеет возможность сменить пароль пользователя/администратора!

При редактировании пользователя/администратора, связанного с внешней системой, логин и описание не доступны для редактирования, для изменения доступен статус пользователя/администратора и для пользователей доступны для изменения:

- параметры настройки службы выполнения команд (в том числе список назначенных наборов команд);
- список доступных устройств;
- список групп пользователей.

Правила заполнения доступных для редактирования полей страницы аналогичны правилам добавления пользователя/администратора (см. п.п. 3.9.4.1 и п.п. 3.9.4.2).

Далее администратору ACS необходимо внести требуемые изменения и нажать кнопку «Сохранить».

Будет запущен процесс проверки заполненности всех обязательных полей и уникальности редактируемого пользователя/администратора по логину.

 Допускается наличие нескольких пользователей с одинаковым логином разных типов – локальный или из внешней системы (в том числе несколько пользователей из нескольких внешних систем). Таким пользователям в списке «Пользователи» ПК «Efros ACS» не может быть назначено доступным одно и то же устройство. При необходимости выдачи пользователям прав доступа на это устройство необходимо добавить пользователей в группу пользователей, имеющую доступ к устройству.

При обнаружении незаполненных обязательных полей рядом с первым из таких полей отобразится всплывающая подсказка «Обязательное поле», в случае обнаружения в списке дубликата пользователя/администратора в верхней части страницы отобразится соответствующее сообщение. Администратору ACS необходимо корректно заполнить поля окна и повторно нажать кнопку «Сохранить».

Если проверки завершились без обнаружения ошибок, то окно редактирования закрывается, внесенные изменения сохраняются. При внесении изменений в данные пользователя перезапускаются службы протоколов TACACS+ и RADIUS для применения новых настроек. Внесенные изменения будут применяться при контроле доступа пользователя к устройствам посредством ПК «Efros ACS» после успешного перезапуска служб.

В журнал событий ПК «Efros ACS» будет внесено сообщение:

- при успешном завершении – сообщение типа «Инфо» в формате: «Администратор {имя_выполняющего_операцию_администратора}: Успешно обновлён пользователь {имя_пользователя}»;
- при обнаружении ошибки – сообщение типа «Ошибка» в формате: «Администратор {имя_выполняющего_операцию_администратора}: Ошибка обновления пользователя {имя_пользователя} - {текст_ошибки}».

3.9.4.6. Просмотр данных пользователя/администратора

Для просмотра данных одного пользователя/администратора необходимо выбрать в таблице вкладки «Пользователи»/«Администраторы» с помощью «мыши» логин пользователя/администратора, после чего:

- для администратора RO откроется страница просмотра соответствующей записи списка;
- для администратора ACS откроется страница редактирования данных соответствующей записи списка.

Состав элементов страницы зависит от роли пользователя/администратора и наличия связанной с ним учетной записи в AD (см. п.п. 3.9.4.1 и п.п. 3.9.4.2).

Администратор имеет возможность просмотреть все данные пользователя/администратора, кроме пароля. Для пользователя с ролью «Пользователь» для просмотра доступны:

- настройки службы выполнения команд;
- список АСО, доступ к которым назначен пользователю;
- список групп, в которые пользователь включен.

Списки наборов команд, АСО и групп пользователей открываются в отдельном окне по нажатию кнопки «Просмотреть» (для администратора RO) или «Изменить» (для администратора ACS) в соответствующем поле страницы просмотра/редактирования данных пользователя.

3.9.5. Ведение списка групп пользователей

3.9.5.1. Добавление группы пользователей из списка пользователей

Для добавления в список новой группы пользователей из списка пользователей администратору ACS необходимо:

- 1) Выбрать в списке пользователей установкой флагов пользователей, объединяемых в группу. В верхней части таблицы отобразится строка в соответствии с рис. 107.

The screenshot shows a web interface for user management. At the top, there are tabs for 'Учетные записи', 'ПОЛЬЗОВАТЕЛИ', 'ГРУППЫ', and 'АДМИНИСТРАТОРЫ'. The 'ПОЛЬЗОВАТЕЛИ' tab is active. Below the tabs, there are buttons for 'Создать группу', 'Добавить в группу', and 'Удалить'. A table lists users with columns for 'Логин', 'Статус', 'Источник', 'Устройства', 'Группы', 'Наборы команд', 'Описание', and 'Последние изменения'. The 'газов' user is selected, and the 'Кротов' user is also selected. At the bottom, it says 'Всего пользователей: 9' and 'Строк на странице: 50'.

Логин	Статус	Источник	Устройства	Группы	Наборы команд	Описание	Последние изменения
localuser	Вкл.	Local	1	0	<> 0	dsadaed	28 июня, 14:36:04
administrator	Вкл.	Local	0	0	<> 0		17 июня, 11:28:05
kotov	Выкл.	Local	0	0	<> 0	Кот К. Котовааааа	10 июня, 19:52:40
Gazprom09	Вкл.	Local	0	0	<> 0		10 июня, 19:52:36
adtacuser	Вкл.	acs	1	0	<> 0	adtacuser	27 мая, 07:36:52
petrov	Вкл.	acs	1	1	<> 0	Петр П. Петров	26 мая, 06:56:53
газов	Вкл.	Local	3	4	<> 2		19 марта, 16:13:50
поров	Вкл.	Local	0	0	<> 0		16 марта, 07:17:38
Кротов	Вкл.	Local	2	1	<> 0		16 марта, 07:13:34

Рисунок 109 – Рисунок 107 – Страница списка пользователей со строкой выбора операций

- 2) Нажать в строке кнопку «Создать группу» (📁). Откроется страница добавления группы пользователей, приведенная на рис. 108. Состав и описание элементов страницы приведены в таблице 31.
- 3) Выбрать установкой переключателя тип группы пользователей: локальная («Локальная») или из внешней системы («LDAP»).
- 4) Заполнить поле страницы «Название» в соответствии с правилами, приведенными в таблице 31, в зависимости от вида группы: локальная или из внешней системы.
- 5) Добавить, при необходимости, описание для локальной группы, нажав кнопку «Добавить описание» и заполнив отобразившееся поле «Описание».
- 6) Выбрать в списке поля «Пользователи» логины пользователей, входящих в группу.

- 7) Назначить доступные пользователям группы устройства и группы устройств, выбрав в полях панели «Основные настройки» требуемые АСО и группы АСО.
- 8) Выполнить настройку службы выполнения команд (аналогично настройке службы для пользователя (см. п.п. 3.9.4.1)).
- 9)

! Настройки службы выполнения команд пользователя имеют приоритет над настройками службы выполнения команд группы пользователей!

Рисунок 110 – Рисунок 108 – Страница добавления группы пользователей

Таблица 31 – Состав и описание элементов страницы добавления группы пользователей из списка пользователей

Элемент	Описание
Поле «Тип группы»	<p>Поле-переключатель с двумя положениями для выбора типа добавляемой группы. Содержит значения:</p> <ul style="list-style-type: none"> — «Локальная» – локальная группа: — «LDAP» – группа из внешней системы. <p>От выбранного положения переключателя зависит состав полей страницы добавления группы</p>

Элемент	Описание
*Поле «Название»	<p>Текстовое поле для ввода названия группы пользователей (до 50 символов). Если группа является:</p> <ul style="list-style-type: none"> — локальной, то поле заполняется путем ввода названия в поле вручную; — группой пользователей внешней системы, то поле заполняется путем выбора названия группы из списка групп пользователей внешней системы, который открывается в поле после ввода последовательности символов из названия группы (не менее 3 символов)
Поле «Описание»	<p>Текстовое поле (до 250 символов). Если группа является:</p> <ul style="list-style-type: none"> — локальной группой ПК «Efros ACS», то поле отображается на странице только после нажатия кнопки «Добавить описание», заполняется путем ввода текста описания в поле вручную. Под полем отображается кнопка «Удалить описание», по нажатию которой поле «Описание» очищается и удаляется; — группой внешней системы, то поле заполняется автоматически после выбора названия группы в поле «Логин» значением поля «Display Name» карточки группы во внешней системе
Группа полей «Основные настройки»	
Поле «Пользователи»	<p>Поле со списком для выбора пользователей, входящих в группу. Список содержит поле поиска и логины пользователей, имеющих в списке «Учетные записи → Пользователи».</p> <p>После выбора пользователей в поле отображается их общее количество</p>
Поле «Устройства»	<p>Поле со списком для выбора устройств, к которым должны получить доступ пользователи группы. Список содержит поле поиска и названия АСО, имеющих в списке «Инфраструктура → Сетевое оборудование → Устройства».</p> <p>После выбора АСО в поле отображается их общее количество</p>
Поле «Группы устройств»	<p>Поле со списком для выбора групп устройств, к которым должны получить доступ пользователи группы. Список содержит поле поиска и названия групп АСО, имеющих в списке «Инфраструктура → Сетевое оборудование → Группы».</p>

Элемент	Описание
	После выбора групп АСО в поле отображается их общее количество
Панель настройки службы выполнения команд (рис. 109). Раскрывается после установки переключателя «Служба выполнения команд» в положение «Включен» ()	
*Поле «Привилегированный режим»	Поле со списком для включения/отключения и выбора пароля (при включении) привилегированного режима для управления устройством. Содержит значения: <ul style="list-style-type: none">— «Отключен» – отключение настройки привилегированного режима;— «Задать пароль» – привилегированный режим доступен по заданному в ПК «Efros ACS» паролю для привилегированного доступа (см. ниже поле «Пароль»);— «Разрешить без пароля» – привилегированный режим доступен без пароля;— «Запретить» – установка принудительного запрета на использование привилегированного режима пользователем;— «Использовать пароль пользователя» – привилегированный режим доступен по заданному в ПК «Efros ACS» для пользователя группы паролю
*Поле «Пароль»	Поле отображается только после выбора в поле «Привилегированный режим» значения «Задать пароль». Предназначено для ввода пароля авторизации пользователей группы для доступа к АСО в привилегированном режиме. Пароль должен соответствовать требованиям, заданным при настройке парольной политики, подробное описание приведено в п.3.4.7. При вводе символы пароля заменяются знаком «●». Для просмотра введенного значения необходимо нажать в поле ввода кнопку «Просмотреть» ()
*Поле «Команды по умолчанию»	Поле-переключатель с двумя положениями: <ul style="list-style-type: none">— «Выполнять» – пользователям группы разрешено выполнение команд по умолчанию на устройстве;

Элемент	Описание
	<p>— «Не выполнять» – пользователям группы запрещено выполнение команд по умолчанию на устройстве.</p> <p>По умолчанию переключатель установлен в положение «Не выполнять»</p>
*Поле «Наборы команд»	<p>Поле со списком для выбора набора команд, разрешенных или запрещенных пользователям группы для выполнения на АСО. Список содержит поле поиска и названия наборов команд, имеющихся в списке «Политики доступа → Наборы команд».</p> <p>После выбора наборов команд в поле отображается их общее количество</p>
Панель доступа на устройства «Время на устройства»	<p>Предназначена для ограничения времени доступа пользователей группы на АСО.</p> <p>Раскрывается после установки переключателя «Время доступа на устройства» в положение «Включен».</p> <p>Содержит поля «Начало» и «Конец» для ввода значений соответственно начала и окончания временного интервала доступа пользователей группы на устройство.</p> <p>Время начала должно быть меньше времени конца.</p> <p>Если панель активирована и заполнена, то вне указанного периода времени доступ пользователям группы к АСО запрещен</p>
Кнопки управления	
Добавить	По нажатию кнопки выполняется переход на страницу списка групп пользователей с сохранением внесенных данных
Отменить	По нажатию кнопки выполняется переход на страницу списка групп пользователей без сохранения внесенных данных
Сбросить	Кнопка отображается на странице после заполнения хотя бы одного поля. По нажатию кнопки все введенные данные в окне удаляются
* – Справа от поля расположен знак «?», при наведении на который курсора открывается всплывающая подсказка с правилами заполнения поля	

← Новая группа пользователей Premium Danilova-N

Тип группы ? Название ?
Локальная LDAP TG-1 [Добавить описание](#)

Основные настройки

Пользователи ? Устройства ? Группы устройств
Выбрано: 3 Выбрано: 2 1-01

Служба выполнения команд
Привилегированный реж... ? Команды по умолчанию ? Наборы команд ?
Отключен Выполнять Не выполнять

Время доступа на устройства

Добавить Отменить Сбросить

Рисунок 111 – Рисунок 109 – Страница добавления группы пользователей с раскрытой панелью настройки службы выполнения команд

10) Ограничить, при необходимости, время доступа пользователей группы на устройства, для чего:

- установить переключатель «Время доступа на устройства» в положение «Включен» ();
- ввести требуемые значения в поля «Начало» и «Конец».

11) Нажать в окне добавления группы пользователей кнопку «Добавить».

Будет запущен процесс проверки заполненности всех обязательных полей и уникальности добавляемой группы пользователей по названию.

При обнаружении незаполненных обязательных полей рядом с первым из таких полей отобразится всплывающая подсказка «Обязательное поле», в случае обнаружения в списке дубликата группы пользователей в верхней части страницы отобразится соответствующее сообщение. Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Добавить».

Если проверки завершились без обнаружения ошибок, то окно добавления закрывается, группа пользователей добавляется в список групп пользователей, группа становится доступна для выбора при создании/редактировании пользователей.

В журнал событий ПК «Efros ACS» будет внесено сообщение:

- при успешном завершении – сообщение типа «Инфо» в формате: «Администратор {имя_выполняющего_операцию_администратора}: Группа пользователей {название_группы_пользователей} успешно создана»;
- при обнаружении ошибки – сообщение типа «Ошибка» в формате: «Администратор {имя_выполняющего_операцию_администратора}: Ошибка создания группы пользователей - {текст_ошибки}».

3.9.5.2. Добавление группы пользователей из списка групп пользователей или из главного меню

Для добавления в список новой группы пользователей из списка групп пользователей или из главного меню администратору ACS необходимо:

- 1) Нажать на странице списка групп пользователей (см. рис. 98) над таблицей кнопку «Добавить» или нажать в панели главного меню кнопку «Добавить» и выбрать в открывшемся меню пункты «Учетные записи»–«Группа пользователей». Откроется страница добавления группы пользователей (см. рис. 108). В поле «Состав группы» будет отображаться кнопка «Добавить» и будут отсутствовать данные о количестве выбранных пользователей.
- 2) Далее – повторить действия по созданию группы, приведенные в п.п. 3.9.5.1. При этом для заполнения поля «Состав группы» необходимо нажать не кнопку «Изменить», а кнопку «Добавить».

В журнал событий ПК «Efros ACS» будут внесены соответствующие сообщения.

3.9.5.3. Добавление группы пользователей путем копирования записи имеющейся группы пользователей

Для добавления новой группы пользователей путем копирования записи имеющейся группы пользователей администратору ACS необходимо:

- 1) Выбрать установкой флага в левой крайней графе таблицы списка групп пользователей исходную группу пользователей и нажать в отобразившейся в верхней части таблицы строке выбора операций (рис. 110) кнопку «Создать копию» () либо нажать в строке исходной группы пользователя кнопку «Меню» () и выбрать в раскрывшемся меню пункт «Создать копию» ()
- 2) Откроется страница добавления новой группы пользователей, аналогичная приведенной на рис. 108. Все поля страницы будут заполнены данными исходной группы пользователей, кроме поля «Название».

- 3) Далее администратору необходимо внести требуемые изменения и нажать кнопку «Добавить». Правила заполнения полей страницы аналогичны правилам добавления группы пользователей (см. п.п. 3.9.5.1 и 3.9.5.2).

Выбрано строк: 1	Создать копию	Удалить					
Название ↓	Источник	Пользователи	Устройства	Группы устройств	Наборы команд	Описание	
<input type="checkbox"/> test2	Local	0	0	0	<> 0		
<input type="checkbox"/> test	Local	1	0	0	<> 0		
<input type="checkbox"/> TACACSGroup	acs	2	0	0	<> 0	TACACSGroup	
<input type="checkbox"/> set1-02	Local	1	3	2	<> 0		
<input type="checkbox"/> set1-01	Local	2	1	1	<> 0		
<input checked="" type="checkbox"/> RADIUSGroup	acs	3	0	0	<> 0	RADIUSGroup	
<input type="checkbox"/> n	Local	0	0	0	<> 0		
<input type="checkbox"/> group	Local	1	0	0	<> 0		
<input type="checkbox"/> fdf	Local	1	1	0	<> 0		

Всего групп: 9 Строк на странице: 50 1-9 из 9 < 1 >

Рисунок 112 – Рисунок 110 – Страница списка групп пользователей со строкой выбора операций

Будет запущен процесс проверки заполненности всех обязательных полей и уникальности добавляемой группы пользователей по названию.

При обнаружении незаполненных обязательных полей рядом с первым из таких полей отобразится всплывающая подсказка «Обязательное поле», в случае обнаружения в списке дубликата группы пользователей в верхней части страницы отобразится соответствующее сообщение. Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Добавить».

Если проверки завершились без обнаружения ошибок, то окно добавления закрывается, группа пользователей добавляется в список групп пользователей, группа становится доступна для выбора при создании/редактировании пользователей.

В журнал событий ПК «Efros ACS» будет внесено сообщение:

- при успешном завершении – сообщение типа «Инфо» в формате: «Администратор {имя_выполняющего_операцию_администратора}: Группа пользователей {название_группы_пользователей} успешно создана»;

- при обнаружении ошибки – сообщение типа «Ошибка» в формате: «Администратор {имя_выполняющего_операцию_администратора}: Ошибка создания группы пользователей - {текст_ошибки}».

3.9.5.4. Просмотр данных группы пользователей

Для просмотра данных одной группы пользователей необходимо выбрать в таблице с помощью «мыши» наименование группы, после чего:

- для пользователя-администратора RO откроется страница просмотра соответствующей записи списка;
- для пользователя-администратора ACS откроется страница редактирования данных соответствующей записи списка (см. п.п. 3.9.5.1).

Пользователь имеет возможность просмотреть:

- данные группы пользователей;
- настройки службы выполнения команд;
- список АСО и групп АСО, доступ к которым назначен пользователям группы;
- список пользователей, включенных в группу.

3.9.5.5. Редактирование группы пользователей

Редактирование данных группы пользователей выполняется администратором ACS вручную средствами веб-приложения ПК «Efros ACS». При редактировании для внесения изменений в данные:

- локальной группы – доступны все данные группы;
- группы пользователей из внешней системы – доступен для внесения изменений только настройки службы выполнения команд, состав доступных пользователям группы АСО и групп АСО.

Для редактирования данных группы пользователей администратору ACS необходимо выбрать в списке с помощью «мыши» наименование требуемой группы либо нажать в строке группы кнопку «Изменить» (✎). Откроется страница редактирования группы пользователей. Страница содержит внесенные ранее данные. Состав элементов страницы и правила заполнения полей страницы аналогичны составу страницы добавления группы пользователей и правилам добавления группы (см. п.п.3.9.5.1). Далее пользователю необходимо внести требуемые изменения и нажать кнопку «Сохранить».

Будет запущен процесс проверки заполненности всех обязательных полей и уникальности редактируемой группы пользователей по наименованию.

При обнаружении незаполненных обязательных полей рядом с первым из таких полей отобразится всплывающая подсказка «Обязательное поле», в случае обнаружения в списке дубликата группы пользователей в верхней части страницы отобразится соответствующее сообщение. Администратору необходимо корректно заполнить поля окна и повторно нажать кнопку «Сохранить».

Если проверки завершились без обнаружения ошибок, то окно редактирования закрывается, внесенные изменения сохраняются.

В журнал событий ПК «Efros ACS» будет внесено сообщение:

- при успешном завершении – сообщение типа «Инфо» в формате: «Администратор {имя_выполняющего_операцию_администратора}: Группа пользователей {название_группы_пользователей} успешно обновлена»;
- при обнаружении ошибки – сообщение типа «Ошибка» в формате: «Администратор {имя_выполняющего_операцию_администратора}: Ошибка обновления группы пользователей - {текст_ошибки}».

3.10 Настройка политик доступа

Для ведения списка преднастроенных политик управления доступом¹⁰ администратору ACS необходимо выбрать в панели главного меню приложения ссылку «Политики доступа» или, если панель свернута, – пиктограмму «».

Раздел «Политики доступа» содержит страницы:

- «Наборы политик» – для формирования наборов политик доступа, содержащих основные правила доступа, а также правила аутентификации и авторизации;
- «Профили оборудования» – для формирования профилей оборудования;
- «Профили авторизации» – для формирования профилей авторизации;
- «Загружаемые ACL» – для формирования загружаемых списков управления доступом (Downloadable Access Control List – DACL);
- «Наборы команд» – содержит список настроенных политик доступа пользователей к контролируемым устройствам;
- «Условия» – содержит конструктор условий для формирования шаблонов, используемых при создании правил доступа, аутентификации и авторизации в наборах политик.

Элементы записей списков могут добавляться как из списка соответствующей сущности по нажатию кнопки «Добавить» () над таблицей списка, так и из главного меню. Окно

¹⁰ Политика управления доступом – набор команд с заданными параметрами (доступные/запрещенные действия с указанными аргументами)

добавления сущности из главного меню раскрывается после нажатия в главном меню кнопки «Добавить» и выбора в открывшемся меню пунктов «Политики доступа» – «<Название сущности>».

3.10.1. Наборы политик

Наборы политик позволяют сгруппировать политики аутентификации и авторизации в рамках одного набора правил.

При создании наборов политик можно настроить правила для выбора служб доступа к сети на уровне набора атрибутов, источников идентификации на уровне политики аутентификации и сетевых разрешений на уровнях политики авторизации. Поддерживается определение условий, используя RADIUS-словари различных производителей.

 Поддерживается создание нескольких наборов политик, которые будут обрабатываться последовательно, после получения запроса.

Для настройки основного правила доступа необходимо открыть страницу «Наборы политик», содержащую список настроенных политик доступа. Политики доступа добавляются, редактируются или удаляются в списке вручную администраторами ACS.

На рис. 111 приведена страница «Наборы политик» для администраторов ACS, данные доступны для редактирования (администраторам RO вкладка не доступна).

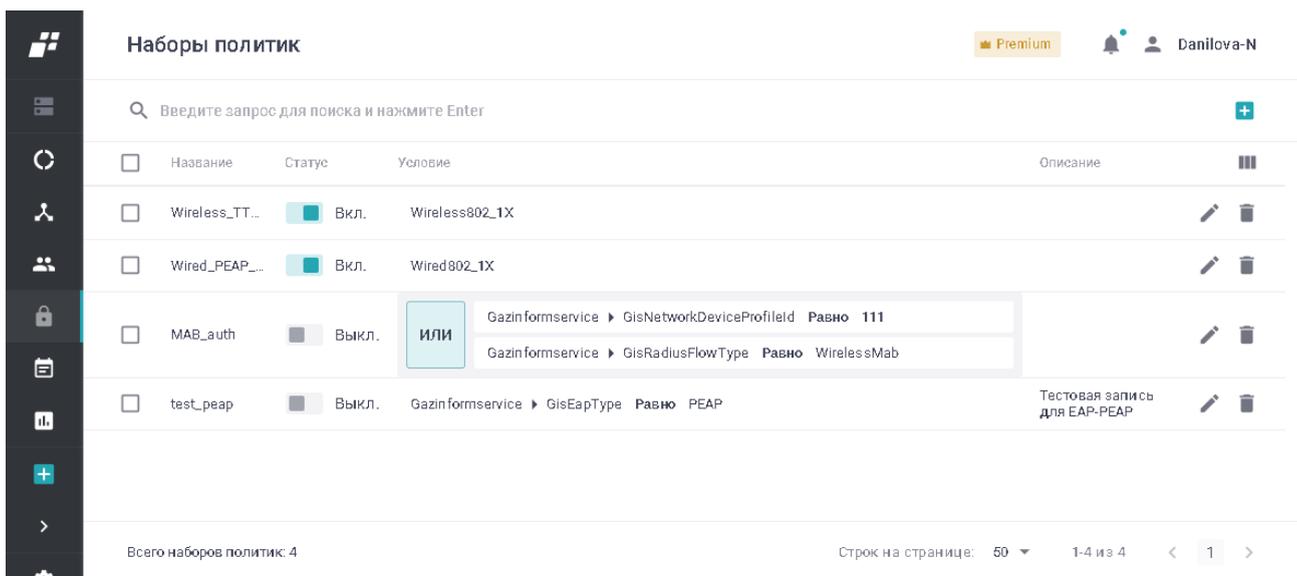


Рисунок 113 – Рисунок 111 – Страница «Наборы политик»

 После установки ПК «Efros ACS» список наборов политик пуст, на странице отображается сообщение «В системе нет наборов политик» и кнопка «Добавить»  для перехода на страницу создания нового набора политик.

Для администраторов ACS на странице для конфигурирования наборов политик доступны следующие кнопки:

- «Добавить»  – для добавления нового основного набора правил;
- «Изменить»  – для перехода на страницу редактирования записи списка;
- «Удалить»  – для удаления соответствующей записи списка.

Для каждой записи списка отображаются данные:

- название;
- статус – «Вкл» (Активен) / «Выкл» (Неактивен). Слева расположена кнопка смены статуса набора политик – в зависимости от текущего статуса набора кнопка имеет вид: «» (по нажатию статус изменяется на «Выкл» (Неактивен)), «» (по нажатию статус изменяется на «Вкл» (Активен));
- условие – шаблон или набор шаблонов условий, входящих в основное условие данной политики;
- описание.

Над таблицей располагается поле поиска  – для ввода последовательности символов из искомой записи. Процесс поиска запускается после ввода символов нажатием клавиши ENTER клавиатуры.

3.10.1.1. Добавление набора политик

Наборы политик настраиваются иерархически, где на верхнем уровне набора политик – основное правило, которое можно просмотреть из таблицы наборов политик, применяется ко всему набору и сопоставляется перед правилами для остальных политик и исключений. После основного правила применяются политики (наборы правил) аутентификации и авторизации в рамках данного набора политик.

Для добавления в список нового набора политик администратору ACS необходимо:

- 1) Нажать над таблицей наборов политик кнопку «Добавить»  или нажать в панели главного меню кнопку «Добавить» и выбрать в открывшемся меню пункты «Политики доступа»–«Набор политик». Откроется страница добавления набора политик с активной вкладкой «Настройки» (для формирования основного правила набора политик), приведенной на рис. 112. Состав и описание элементов страницы приведены в таблице 32.

- 2) Заполнить поле страницы «Название».
- 3) Добавить, при необходимости, описание для набора политик, нажав кнопку «Добавить описание» и заполнив отобразившееся поле «Описание».
- 4) Сформировать основное правило, выполнив действия в соответствии с п. 3.10.6 или воспользоваться заранее сформированными шаблонами условий.

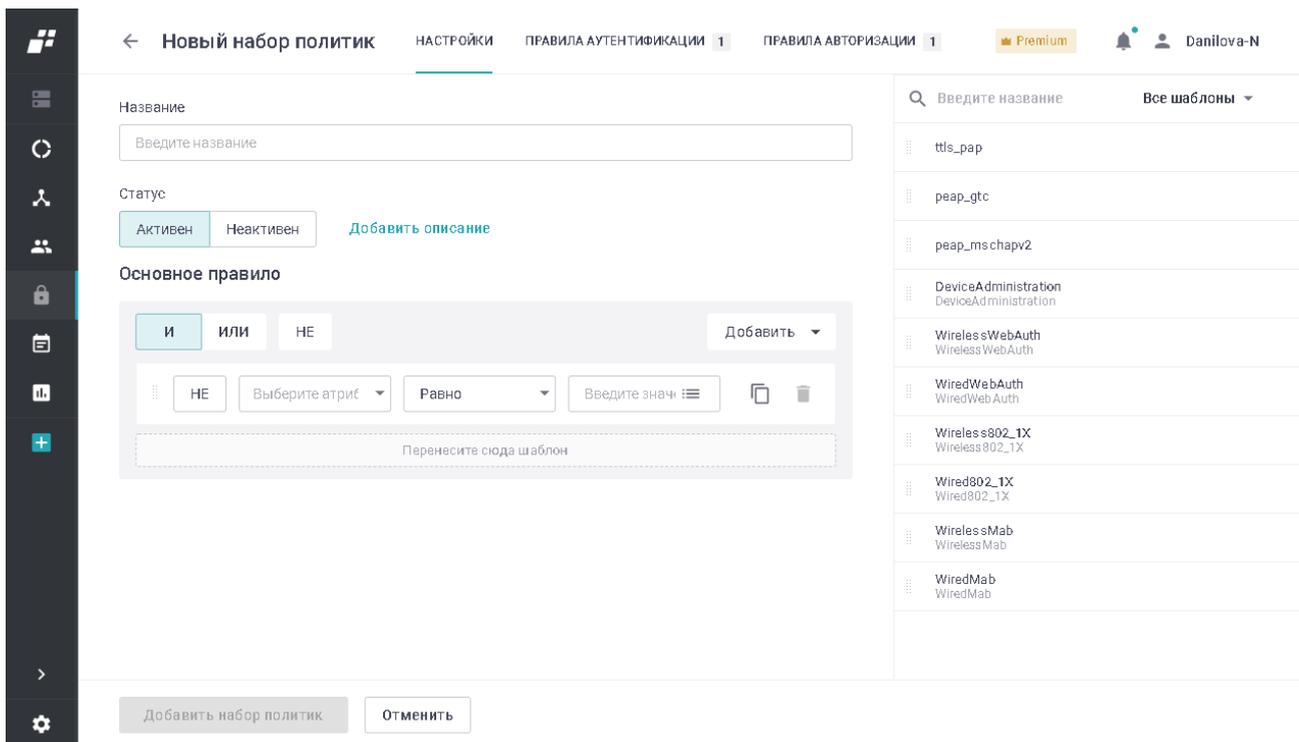


Рисунок 114 – Рисунок 112 – Окно добавления набора политик. Вкладка «Настройки»

Таблица 32 – Состав и описание элементов вкладки «Настройки» окна добавления набора политик

Элемент	Описание
Поле «Название»	Текстовое поле для ввода названия набора политик (до 50 символов)
Кнопка «Добавить описание»	По нажатию кнопки на странице дополнительно отображается поле «Описание» – текстовое поле для ввода описания набора политик (до 250 символов). Под полем отображается кнопка «Удалить описание», по нажатию которой поле «Описание» очищается и удаляется
Поле «Статус»	Поле с кнопками выбора текущего статуса набора: «Активен» или «Неактивен». Статус может быть изменен как на

Элемент	Описание
	странице редактирования параметров набора политик, так и в списке наборов политик
Основное правило	
Формирование основного правила происходит аналогично формированию шаблона условий, описание приведено в п. 3.10.6.	
Для использования ранее сформированных в разделе «Условия» шаблонов условий необходимо перенести путем перетаскивания из перечня шаблонов в правой части страницы наименования требуемого шаблона в поле «Перенесите сюда шаблон»	
Добавить	По нажатию кнопки выполняется переход на страницу списка набора политик с сохранением внесенных данных
Отменить	По нажатию кнопки выполняется переход на страницу списка набора политик доступа без сохранения внесенных данных
Сбросить	По нажатию кнопки значения поля окна создания набора политик устанавливаются в положение по умолчанию

- 5) Перейти во вкладку «Правила аутентификации» для определения политики аутентификации (набора правил аутентификации) в рамках данного набора политик (рис. 113). По умолчанию вкладка содержит одно предустановленное в ПК «Efros ACS» правило аутентификации «Default», правило по умолчанию включено и не доступно для выключения (кнопка в графе «Статус» неактивна). Правила формирования списка правил аутентификации приведены в п.п. 3.10.1.2.

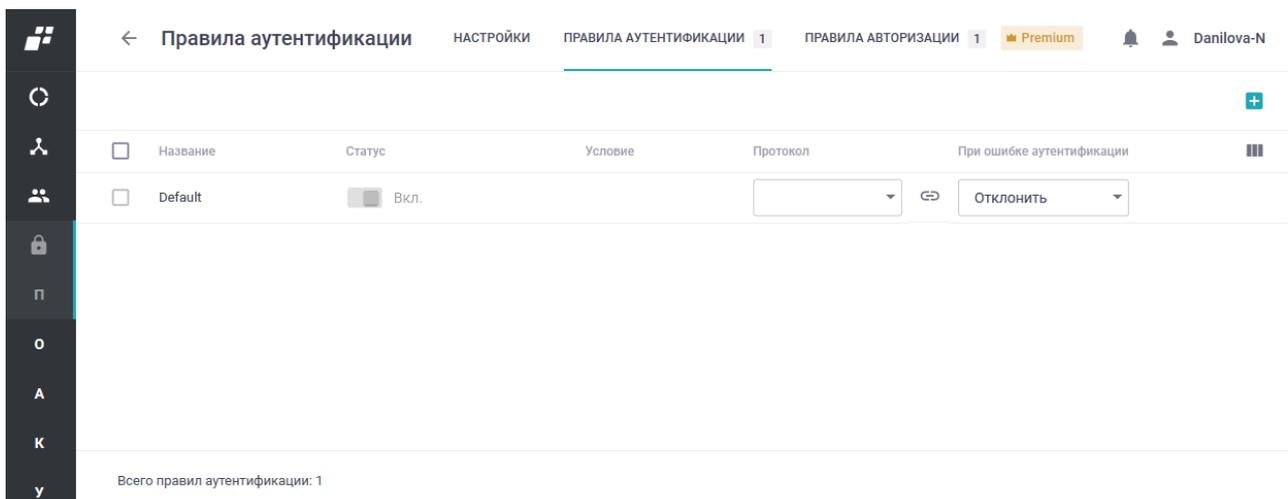


Рисунок 115 – Рисунок 113 – Вкладка «Правила аутентификации»

- 6) Перейти во вкладку «Правила авторизации» для определения политики авторизации (набора правил авторизации) в рамках данного набора политик (рис. 114). По умолчанию вкладка содержит одно предустановленное в ПК «Efros ACS» правило авторизации «Default», правило по умолчанию включено и не доступно для выключения (кнопка в графе «Статус» неактивна). Правила формирования списка правил аутентификации приведены в п.п. 3.10.1.3.
- 7) После настройки политик аутентификации и авторизации вернуться во вкладку «Настройки» и нажать в окне добавления набора политик кнопку «Добавить набор политик».

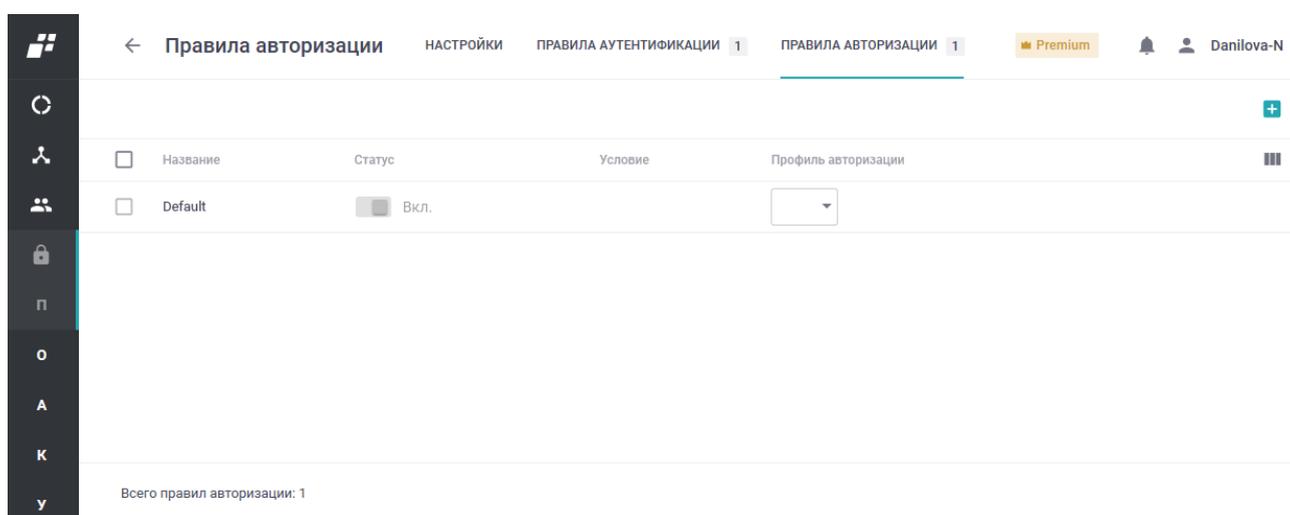


Рисунок 116 – Рисунок 114 – Вкладка «Правила авторизации»

Будет запущен процесс проверки заполненности всех обязательных полей, наличия хотя бы одной команды и уникальности добавляемого набора политик по наименованию. При:

- обнаружении незаполненных обязательных полей рядом с первым из таких полей отобразится всплывающая подсказка «Обязательное поле»;
- пустом списке команд в верхней части страницы отобразится соответствующее сообщение;
- обнаружении в списке дубликата набора политик в верхней части страницы отобразится соответствующее сообщение.

Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Добавить набор политик».

Если проверки завершились без обнаружения ошибок, то окно добавления закрывается, набор политик доступа добавляется в список.

В журнал событий ПК «Efros ACS» будет внесено сообщение:

- при успешном завершении – сообщение типа «Инфо» в формате: «Администратор {имя_выполняющего_операцию_администратора}: Политика {название_политики доступа} успешно создана»;
- при обнаружении ошибки – сообщение типа «Ошибка» в формате: «Администратор {имя_выполняющего_операцию_администратора}: Ошибка создания политики - {текст_ошибки}».

3.10.1.2. Правила формирования правил аутентификации

После установки комплекса доступна к использованию предустановленное правило аутентификации «Default» (см. рис. 113). По умолчанию правило активировано.

Для добавления в список нового правила аутентификации администратору ACS необходимо:

- 1) Нажать над таблицей правил аутентификации кнопку «Добавить» (+). Откроется страница добавления правила аутентификации, приведенная на рис. 115. Состав и описание элементов страницы приведены в таблице 33.

← Новое правило аутентификации

Premium Danilova-N

Название:

Статус:

Протокол:

При ошибке аутентификации:

ИЛИ ИЛИ НЕ

НЕ Выберите ат: Введите зн:

Перенесите сюда шаблон

Введите название Все шаблоны

- ttls_pap
- peap_gtc
- peap_mschap2
- testnn
- testnn
- DeviceAdministration
- DeviceAdministration
- WirelessWebAuth
- WirelessWebAuth
- WiredWebAuth
- WiredWebAuth
- Wireless802_1X
- Wireless802_1X
- Wired802_1X
- Wired802_1X
- WirelessMab

Рисунок 117 – Рисунок 115 – Страница добавления правила аутентификации

Таблица 33 – Состав и описание элементов страницы добавления правила аутентификации

Элемент	Описание
Поле «Название»	Текстовое поле для ввода названия правила аутентификации (до 50 символов)
Поле «Статус»	Поле с кнопками выбора текущего статуса правила: «Активен» или «Неактивен». Статус может быть изменен как на странице редактирования параметров правила аутентификации, так и в списке правил аутентификации
Поле «Протокол»	Поле является полем со списком для выбора протокола аутентификации. Список доступных для выбора протоколов зависит от текущих настроек комплекса (параметры доступа в сеть, наличие подключения внешних источников данных, наличие профилей сертификатов)
Область настройки условий	
<p>Сформированные условия правила аутентификации представляет собой иерархичную структуру, заведение атрибутов происходит аналогично формированию шаблона условий, описание которого приведено в п. 3.10.6.</p> <p>Для использования ранее сформированных в разделе «Условия» шаблонов условий необходимо перенести путем перетаскивания из перечня шаблонов в правой части страницы наименования требуемого шаблона в поле «Перенесите сюда шаблон»</p>	
Добавить	По нажатию кнопки выполняется переход на страницу списка правил аутентификации с сохранением внесенных данных
Отменить	По нажатию кнопки выполняется переход на страницу списка правил аутентификации без сохранения внесенных данных
Сбросить	По нажатию кнопки значения поля страницы создания правила аутентификации устанавливаются в положение по умолчанию

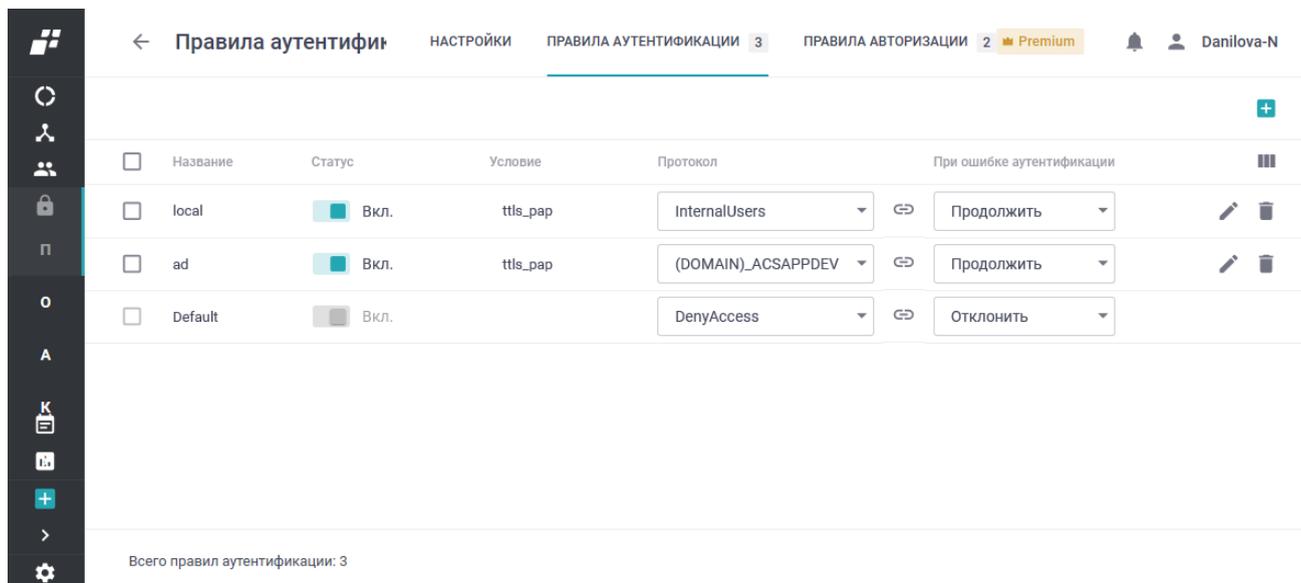
- 2) Заполнить поле страницы «Название», выбрать «Статус».
- 3) Выбрать в поле «Протокол» используемый устройством протокол аутентификации.
- 4) Выбрать в поле «При ошибке аутентификации» выполняемое при ошибке аутентификации действие: отклонить запрос устройства на аутентификацию или продолжить процесс аутентификации.

5) Сформировать условия, определяющие правила аутентификации, выполнив действия в соответствии с п. 3.10.6 или воспользоваться заранее сформированными шаблонами условий.

6) После настройки правила аутентификации нажать кнопку «Добавить».

Будет запущен процесс проверки заполненности всех обязательных полей, наличия хотя бы одной команды и уникальности добавляемого правила аутентификации по наименованию. В случае обнаружения в списке дубликата правила аутентификации в верхней части страницы отобразится соответствующее сообщение. Пользователю необходимо корректно заполнить поля страницы и повторно нажать кнопку «Добавить».

Если проверки завершились без обнаружения ошибок, то страница добавления закрывается, правило аутентификации добавляется в список правил аутентификации (рис. 116).



<input type="checkbox"/>	Название	Статус	Условие	Протокол	При ошибке аутентификации	
<input type="checkbox"/>	local	<input checked="" type="checkbox"/> Вкл.	tls_pas	InternalUsers	Продолжить	<input type="checkbox"/>
<input type="checkbox"/>	ad	<input checked="" type="checkbox"/> Вкл.	tls_pas	(DOMAIN)_ACSAPPDEV	Продолжить	<input type="checkbox"/>
<input type="checkbox"/>	Default	<input type="checkbox"/> Вкл.		DenyAccess	Отклонить	<input type="checkbox"/>

Всего правил аутентификации: 3

Рисунок 118 – Рисунок 116 – Список правил аутентификации набора политик

В списке правило доступно для:

- активации/деактивации – статус правила изменяется нажатием кнопки смены статуса в графе «Статус» – в зависимости от текущего статуса набора кнопка имеет вид: «» (по нажатию статус изменяется на «Выкл» (Неактивен)), «» (по нажатию статус изменяется на «Вкл» (Активен));
- смены протокола аутентификации путем выбора нового значения в списке поля графы «Протокол»;

- смены действия, выполняемого при ошибке аутентификации путем выбора требуемого значения в списке поля графы «При ошибке аутентификации»: «Отклонить» или «Продолжить»;
- перехода на страницу редактирования параметров правила по нажатию кнопки «Изменить» (✎). При редактировании все параметры правила доступны для внесения изменений аналогично созданию правила. Сохраняются внесенные изменения по нажатию кнопки «Сохранить»;
- удаления по нажатию кнопки «Удалить» (🗑).

Примечание. Предустановленное правило аутентификации «Default» не доступно для смены статуса, редактирования и удаления, доступно для смены протокола и действия, выполняемого при ошибке аутентификации.

После внесения любых изменений в список правил аутентификации для сохранения изменений необходимо перейти на вкладку «Настройки» набора политик и нажать кнопку «Сохранить».

3.10.1.3. Правила формирования правил авторизации

После установки комплекса доступна к использованию предустановленное правило авторизации «Default» (см. рис. 114). По умолчанию правило активировано.

Для добавления в список нового правила авторизации администратору ACS необходимо:

- 1) Нажать над таблицей политик авторизации кнопку «Добавить» (+). Откроется страница добавления правила авторизации, приведенное на рис. 117. Состав и описание элементов страницы приведены в таблице 34.
- 2) Заполнить поле страницы «Название», выбрать «Статус» и указать «Профиль авторизации».
- 3) Сформировать условия, определяющие правило авторизации, выполнив действия в соответствии с п. 3.10.6 или воспользоваться заранее сформированными шаблонами условий.
- 4) После настройки правила авторизации нажать в окне добавления кнопку «Добавить».

Будет запущен процесс проверки заполненности всех обязательных полей, наличия хотя бы одной команды и уникальности добавляемого правила авторизации по наименованию. В случае обнаружения в списке дубликата правила авторизации в верхней части страницы отобразится соответствующее сообщение. Пользователю необходимо корректно заполнить поля страницы и повторно нажать кнопку «Добавить».

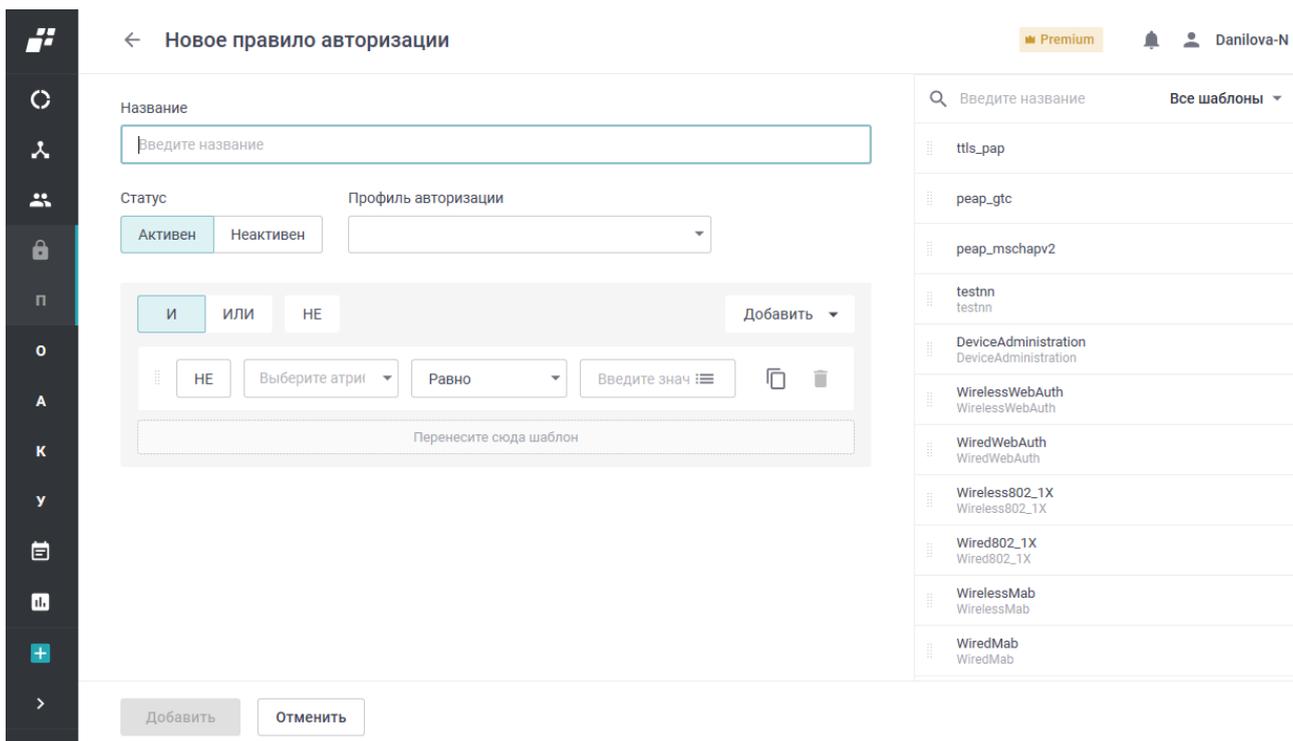


Рисунок 119 – Рисунок 117 – Страница добавления правила авторизации

Таблица 34 – Состав и описание элементов страницы добавления правила авторизации

Элемент	Описание
Поле «Название»	Текстовое поле для ввода названия правила авторизации (до 50 символов)
Поле «Статус»	Поле с кнопками выбора текущего статуса правила: «Активен» или «Неактивен». Статус может быть изменен как на странице редактирования параметров правила авторизации, так и в списке правил авторизации
Поле «Профиль авторизации»	Поле является полем со списком для выбора профиля авторизации. Список доступных для выбора профилей соответствует списку подраздела «Профили авторизации» раздела «Политики доступа»
Область настройки условий	
<p>Сформированное правило авторизации представляет собой иерархичную структуру, заведение атрибутов происходит аналогично формированию шаблона условий, описание которого приведено в разделе 3.10.5 «Конструктор условий».</p> <p>Для использования ранее сформированных в разделе «Условия» шаблонов условий необходимо перенести путем перетаскивания из перечня шаблонов в правой части страницы наименования требуемого шаблона в поле «Перенесите сюда шаблон»</p>	

Элемент	Описание
Кнопки управления	
Добавить	По нажатию кнопки выполняется переход на страницу списка правил авторизации с сохранением внесенных данных
Отменить	По нажатию кнопки выполняется переход на страницу списка правил авторизации без сохранения внесенных данных
Сбросить	По нажатию кнопки значения поля страницы создания правила авторизации устанавливаются в положение по умолчанию

Если проверки завершились без обнаружения ошибок, то страница добавления закрывается, правило авторизации добавляется в список правил авторизации (рис. 118).

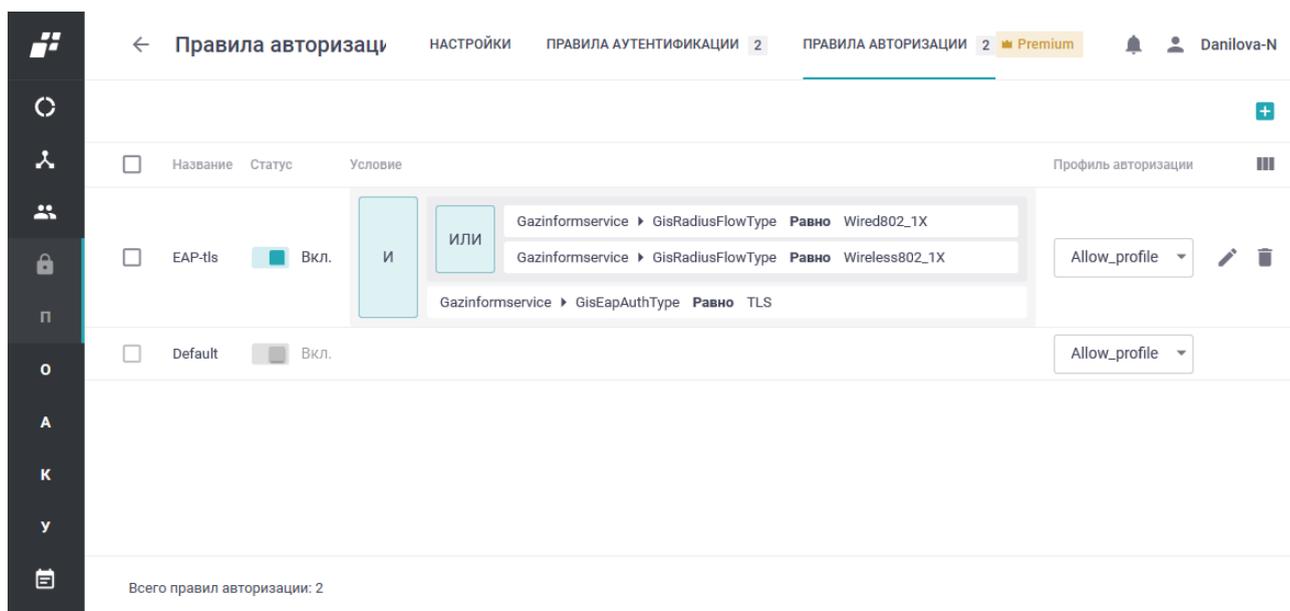


Рисунок 120 – Рисунок 118 – Список правил авторизации набора политик

В списке правило доступно для:

- активации/деактивации – статус правила изменяется нажатием кнопки смены статуса в графе «Статус» – в зависимости от текущего статуса набора кнопка имеет вид: «» (по нажатию статус изменяется на «Выкл» (Неактивен)), «» (по нажатию статус изменяется на «Вкл» (Активен));
- смены профиля авторизации путем выбора нового значения в списке поля графы «Профиль авторизации»;

- перехода на страницу редактирования параметров правила по нажатию кнопки «Изменить» (). При редактировании все параметры правила доступны для внесения изменений аналогично созданию правила. Сохраняются внесенные изменения по нажатию кнопки «Сохранить»;
- удаления по нажатию кнопки «Удалить» (.

 Предустановленное правило авторизации «Default» не доступно для смены статуса, редактирования и удаления, доступно для смены профиля авторизации.

После внесения любых изменений в список правил аутентификации для сохранения изменений необходимо перейти на вкладку «Настройки» набора политик и нажать кнопку «Сохранить».

3.10.1.4. Редактирование набора политик

Редактирование выполняется администратором ACS вручную средствами веб-приложения ПК «Efros ACS». При редактировании для внесения изменений доступны все данные набора команд.

Для редактирования администратору ACS необходимо выбрать в списке с помощью «мыши» название требуемого набора политик либо нажать в строке кнопку «Изменить» (). Откроется страница редактирования, которая содержит внесенные ранее данные. Состав элементов страницы и правила заполнения полей страницы аналогичны составу страницы добавления набора политик и правилам добавления набора политик (см. п.п. 3.10.1.1). Далее пользователю необходимо внести требуемые изменения и нажать кнопку «Сохранить».

Будет запущен процесс проверки заполненности всех обязательных полей, наличия хотя бы одной команды и уникальности добавляемого набора политик доступа по наименованию. При:

- обнаружении незаполненных обязательных полей рядом с первым из таких полей отобразится всплывающая подсказка «Обязательное поле»;
- пустом списке команд в верхней части страницы отобразится соответствующее сообщение;
- обнаружении в списке дубликата политики доступа в верхней части страницы отобразится соответствующее сообщение.

Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Сохранить».

Если проверки завершились без обнаружения ошибок, то окно редактирования закрывается, набор политик обновляется согласно внесенным данным.

В журнал событий ПК «Efros ACS» будет внесено сообщение:

- при успешном завершении – сообщение типа «Инфо» в формате: «Администратор {имя_выполняющего_операцию_администратора}: Политика {название_набора_политик} успешно обновлена»;
- при обнаружении ошибки – сообщение типа «Ошибка» в формате: «Администратор {имя_выполняющего_операцию_администратора}: Ошибка обновления политики - {текст_ошибки}».

3.10.2. Ведение списка профилей оборудования

Профиль оборудования определяет набор параметров (набор атрибутов протокола Radius), на основе которых в ПК «Efros ACS» определяется производитель оборудования и правила обработки запросов, поступающих от устройств.

На рисунке 119 приведена страница с вкладкой «Профили оборудования» для администраторов ACS данные доступны для редактирования. На странице для администраторов RO над таблицей отсутствует кнопка «Добавить» (+) и в таблице отсутствуют кнопки:

- «Изменить» (✎) – для перехода на страницу редактирования записи списка;
- «Копировать» (📄) – для добавления в список копии профиля оборудования
- «Удалить» (🗑) – для удаления соответствующей записи списка.

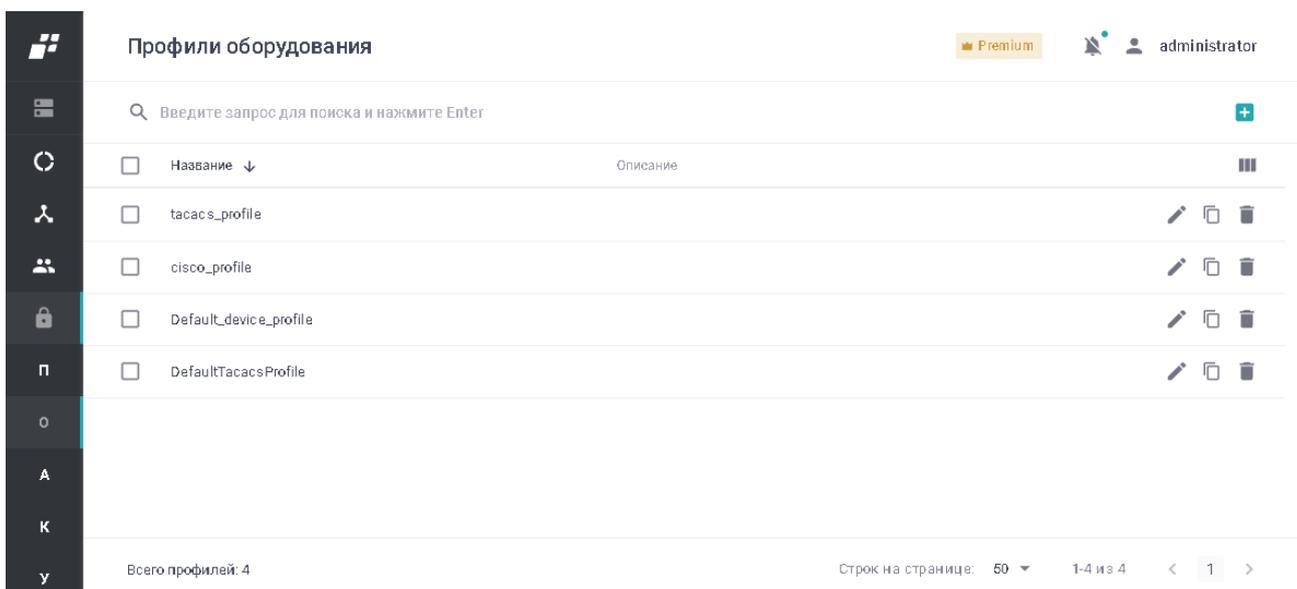


Рисунок 121 – Рисунок 119 – Страница профили оборудования

Таблица содержит встроенные профили оборудования «Default_device_profile» и «DefaultTacacsProfile» производителя «Efros ACS».

Для каждой записи списка отображаются данные:

- название;
- описание;
- производитель (по умолчанию графа скрыта).

Над таблицей располагается поле поиска (🔍) – для ввода последовательности символов из искомой записи. Процесс поиска запускается после ввода символов нажатием клавиши ENTER клавиатуры.

3.10.2.1. Добавление профиля оборудования

Для добавления в список нового профиля оборудования администратору ACS необходимо:

- 1) Нажать над таблицей профилей кнопку «Добавить» (+) или нажать в панели главного меню кнопку «Добавить» и выбрать в открывшемся меню пункты «Политики доступа»–«Профиль оборудования». Откроется окно добавления профиля оборудования, приведенное на рис. 120. Состав и описание элементов страницы приведены в таблице 35.

← Новый профиль сетевого оборудования Premium administrator

Название
Введите название [Добавить описание](#)

Основные настройки

Производитель Выберите производителя RADIUS словари Выберите

Аутентификация / Авторизация

- > Условия типа потока
- > Поиск узла (MAB)
- Разрешения
 - Установить ACL

Добавить Отменить

Рисунок 122 – Рисунок 120 – Окно добавления профиля оборудования

Таблица 35 – Состав и описание элементов окна добавления профиля сетевого оборудования

Элемент	Описание
Поле «Название»	Текстовое поле для ввода названия профиля сетевого оборудования (до 50 символов)
Кнопка «Добавить описание»	По нажатию кнопки на странице дополнительно отображается поле «Описание» – текстовое поле для ввода описания профиля сетевого оборудования (до 250 символов). Под полем отображается кнопка «Удалить описание», по нажатию которой поле «Описание» очищается и удаляется
Группа полей «Основные настройки»	
Поле «Производитель»	Поле со списком для выбора производителя оборудования
Поле «Radius словари»	<p>Поле со списком для выбора системных словарей, которые содержат различные атрибуты, необходимые при построении условий и правил для политик аутентификации и авторизации. В поле установкой флагов могут быть выбраны один или несколько словарей</p> <p>Доступны для добавления следующие словари:</p> <ul style="list-style-type: none">— Gazinformservice;— Efros-ACS;— ADSL-Forum;— FreeRADIUS;— Cisco-VPN3000;— Cisco-VPN5000;— Cisco-BBSM;— Cisco-ASA;— Cisco;— 3com;— CheckPoint;— Eltex;— H3C;— HP;— Huawei;— Microsoft;— Radius
Группа полей «Аутентификация / Авторизация»	

Элемент	Описание
	По умолчанию дерево полей группы свернуто, в заголовке отображается кнопка раскрытия дерева «>»
	Подгруппа полей «Условия типа потока». Содержит список типов аутентификации. Предназначена для определения условий, по которым будет проходить аутентификация и авторизация оборудования в комплексе, какие атрибуты будут обрабатываться в зависимости от запроса
Проводная аутентификация по MAC-адресам	Типы аутентификации включаются/выключаются по нажатию кнопки соответственно «  »/ «  » слева от названия каждого условия.
Беспроводная аутентификация по MAC-адресам	При включении типа аутентификации в окне дополнительно отображаются поля для формирования списка условий проверки устройства при его подключении – списка проверяемых при подключении устройства атрибутов и их значений.
Проводная аутентификация по стандарту 802.1X	Примечание. Для выбора доступны фиксированные атрибуты, поддерживаемые словарями (из списка ранее выбранных в поле «Radius словари»), которые можно использовать в соответствующем условии политики доступа.
Беспроводная аутентификация по стандарту 802.1X	Далее для включенного типа аутентификации формируется список условий проверки, для каждого условия выбирается атрибут и присваивается соответствующее значение.
Управление сетевыми устройствами	Условия добавляются по нажатию кнопки «Добавить» () строка для ввода параметров нового условия добавляется под строкой условия, в которой нажата кнопка «Добавить». Лишние условия удаляются по нажатию кнопки «Удалить» () в соответствующей строке
	Подгруппа полей «Поиск узла (MAB)». Содержит поле «Поиск узла процесса». Предназначена для настройки аутентификации конечных точек сети в комплексе
Поиск узла процесса	Возможность аутентификации MAB для конечных точек сети включается/выключается по нажатию кнопки соответственно «  »/ «  » слева от названия поля «Поиск узла процесса». Если возможность выключена, то аутентификация MAB для редактируемого профиля оборудования будет недоступна (то есть завершится с ошибкой).

Элемент	Описание
	<p>После включения возможности в окне дополнительно отображаются поля для включения/отключения и настройки проверки оборудования при его аутентификации по условиям для протоколов PAP/ASCII, CHAP, EAP-MD5.</p> <p>Проверка для каждого протокола включается/выключается отдельно по нажатию кнопки соответственно «»/ «» слева от названия проверки.</p> <p>Для каждой включенной проверки дополнительно отображаются поля для флагов:</p> <ul style="list-style-type: none"> — «Проверить пароль» – при установленном флаге выполняется проверка пароля, пришедшего от оборудования; — «Убедиться, что идентификатор вызывающей станции равен MAC-адресу» – при установленном флаге выполняется сравнение значения атрибута User-Name и значения атрибута Calling-Station-ID протокола RADIUS
<p>Подгруппа полей «Разрешения».</p> <p>Содержит поле «Установить ACL». Предварительно расширенный список доступа (extended ACL) должен быть настроен на оборудовании</p>	
<p>Установить ACL</p>	<p>Возможность добавления списка управления доступом включается/выключается по нажатию кнопки соответственно «»/ «» слева от названия поля «Установить ACL».</p> <p>После включения возможности в окне дополнительно отображается поле для выбора атрибута из radius-словарей, добавленных в программный комплекс.</p> <p>Необходимо указать, в каком атрибуте будет осуществляться отправка имени ACL, который будет применен на оборудовании</p>
<p>Кнопки управления</p>	
<p>Добавить</p>	<p>По нажатию кнопки выполняется переход на страницу списка профилей сетевого оборудования с сохранением внесенных данных</p>
<p>Отменить</p>	<p>По нажатию кнопки выполняется переход на страницу списка профилей сетевого оборудования без сохранения внесенных данных</p>

Элемент	Описание
Сбросить	По нажатию кнопки значения поля окна создания профиля сетевого оборудования устанавливаются в положение по умолчанию

- 2) Заполнить поле страницы «Название».
- 3) Добавить, при необходимости, описание для профиля оборудования, нажав кнопку «Добавить описание» и заполнив отобразившееся поле «Описание».
- 4) Выбрать производителя сетевого оборудования.
- 5) Выбрать словари, которые далее будут применены при построении условий и правил для условий аутентификации и авторизации (см. шаг 6).
- 6) Определить условия прохождения аутентификации сетевого оборудования в комплексе, для чего в разделе «Аутентификации / Авторизация»:
 - сформировать список типов доступа и для каждого типа определить требуемые условия. (выбрать атрибуты и их значения) например, см. рис. 121;
 - включить возможность аутентификации MAB для конечных точек сети, сформировать список проверок оборудования при его аутентификации по условиям для и для включенных проверок задать необходимость проверки при подключении устройства пароля и равенства идентификатора вызывающей станции MAC-адресу;
 - при необходимости добавить имя предварительно настроенного ACL на оборудовании в поле «Установить ACL».

✓ Аутентификация / Авторизация

✓ Условия типа потока

Проводная аутентификация по MAC-адресам

NAS-Port-Type	=	Ethernet	-	+
Service-Type	=	Call-Check	-	+
Выберите атрибут	=	Введите значение	-	+

🔍 Device

- 📁 Gazinformservice
 - GisNetworkDeviceProfileId
 - GisNetworkDeviceProfileNa...
 - GisNetworkDeviceId
 - GisNetworkDeviceName
- 📁 Radius
 - EAP-Type-DeviceConnect-EAP...

✓ Поиск узла (MAB)

Поиск узла процесса

Via PAP/ASCII

Via CHAP

Проверить пароль Убедиться, что идентификатор вызывающей станции равен MAC-адресу

Via EAP-MD5

Рисунок 123 – Рисунок 121 – Определение условий прохождения аутентификации оборудования

7) Нажать в окне добавления профиля оборудования кнопку «Добавить».

Будет запущен процесс проверки заполненности всех обязательных полей и уникальности добавляемого профиля оборудования по наименованию.

При обнаружении незаполненных обязательных полей рядом с первым из таких полей отобразится всплывающая подсказка «Обязательное поле», в случае обнаружения в списке дубликата профиля оборудования в верхней части страницы отобразится соответствующее сообщение. Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Добавить».

Если проверки завершились без обнаружения ошибок, то окно добавления закрывается, профиль оборудования добавляется в список профилей оборудования и становится доступен для выбора при создании/редактировании устройства.

В журнал событий ПК «Efros ACS» будут внесены соответствующие сообщения.

Удаление созданного профиля оборудования выполняется в соответствии с разделом 3.2.6.

3.10.2.2. Добавление профиля оборудования путем копирования имеющейся записи

Для добавления нового профиля оборудования путем копирования записи имеющегося профиля пользователю необходимо:

- 1) Выбрать установкой флага в левой крайней графе таблицы списка профилей исходный профиль. В верхней части таблицы отобразится строка выбора операций в соответствии с рис. 122.

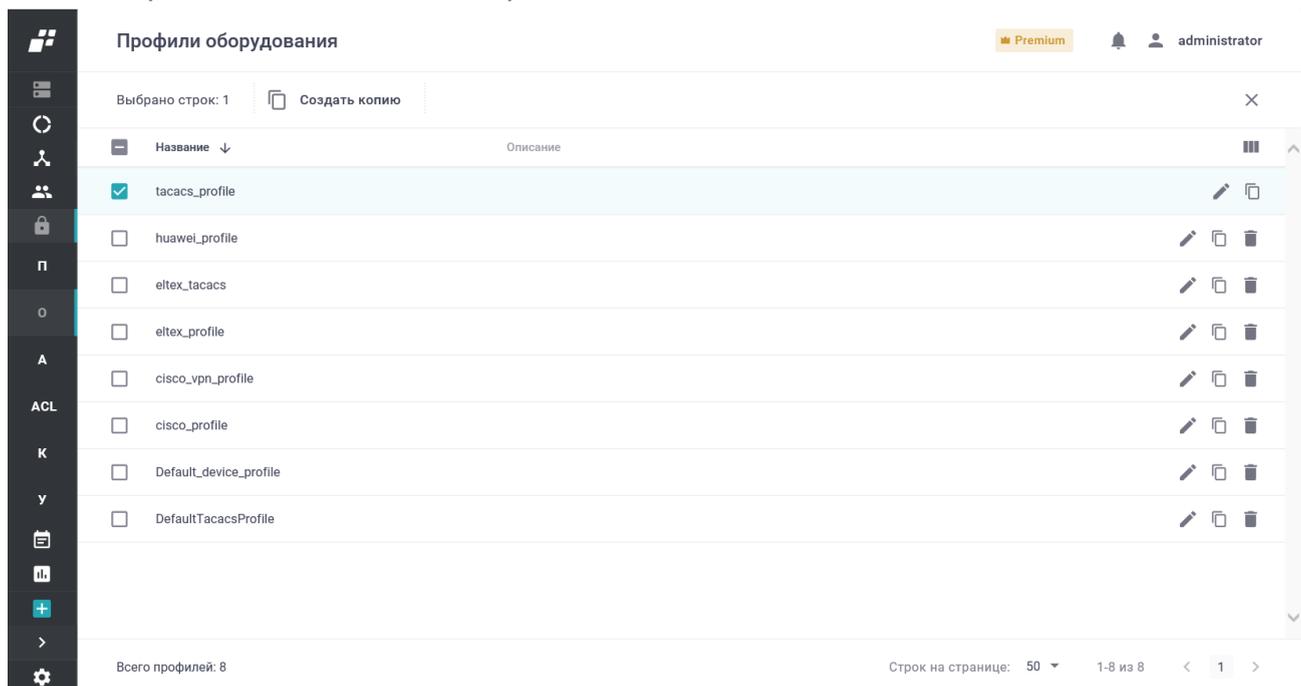


Рисунок 124 – Рисунок 122 – Страница списка профилей оборудования со строкой выбора операций

- 2) Нажать в строке кнопку «Создать копию» (📄). Откроется страница добавления нового профиля оборудования, аналогичная приведенной на рис. 120. Все поля страницы будут заполнены данными исходного профиля, кроме поля «Название».
- 3) Далее пользователю необходимо внести требуемые изменения и нажать кнопку «Добавить». Правила заполнения полей страницы и действия системы после нажатия кнопки «Добавить» приведены в п.п.3.10.2.1.

3.10.3. Ведение списка профилей авторизации

На рисунке 123 приведена страница с вкладкой «Профили авторизации» для администраторов ACS данные доступны для редактирования.

Примечание. После установки комплекса список содержит один предустановленный профиль авторизации «Default authorization profile», связанный с профилем оборудования «Default device profile».

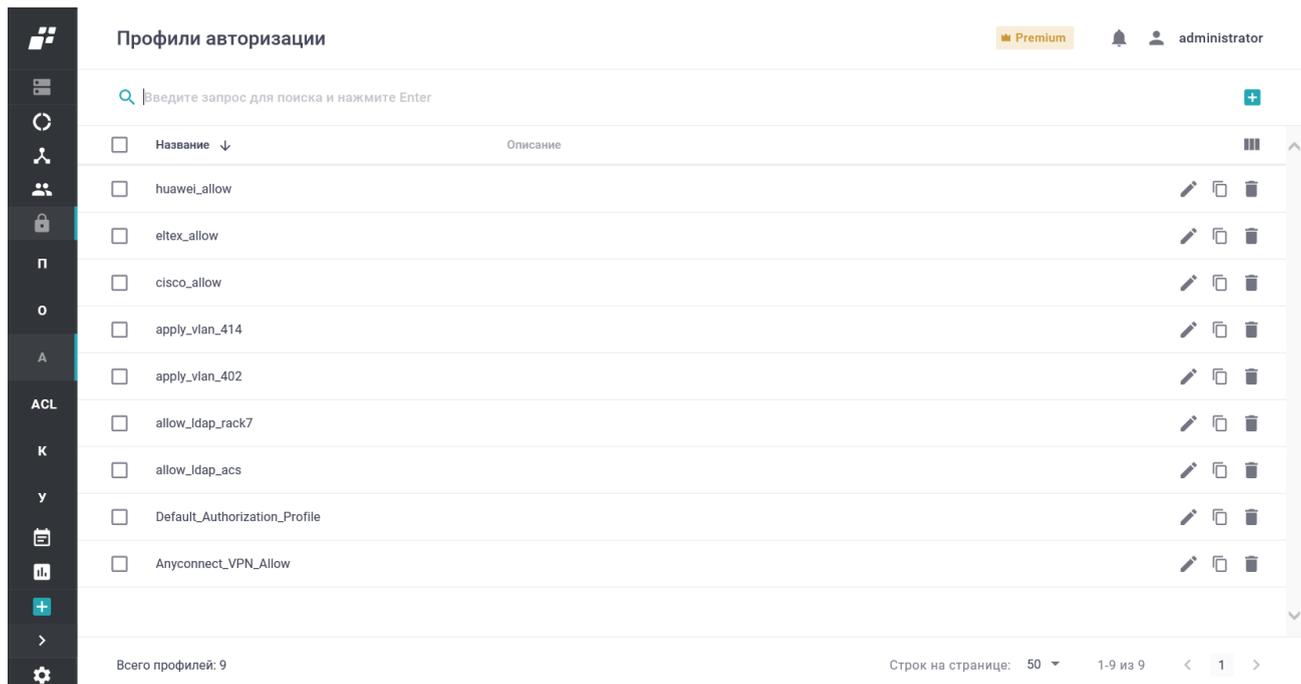


Рисунок 125 – Рисунок 123 – Страница «Профили авторизации»

На странице для администраторов RO над таблицей отсутствует кнопка «Добавить» (+) и в таблице отсутствуют кнопки:

- «Изменить» (✎) – для перехода на страницу редактирования записи списка. При редактировании все данные профиля доступны для внесения изменений;
- «Копировать» (📄) – для добавления в список копии профиля авторизации
- «Удалить» (🗑) – для удаления соответствующей записи списка.

Для каждой записи списка отображаются название и описание.

Над таблицей располагается поле поиска (🔍) – для ввода последовательности символов из искомой записи. Процесс поиска запускается после ввода символов нажатием клавиши ENTER клавиатуры.

3.10.3.1. Добавление профиля авторизации

Для добавления в список нового профиля оборудования администратору ACS необходимо:

- 1) Нажать над таблицей профилей кнопку «Добавить» (+) или нажать в панели главного меню кнопку «Добавить» и выбрать в открывшемся меню пункты «Политики доступа»–«Профиль авторизации». Откроется страница добавления профиля авторизации, приведенная на рис. 124. Состав и описание элементов страницы приведены в таблице 36.

Рисунок 126 – Рисунок 124 – Страница добавления профиля авторизации

Таблица 36 – Состав и описание элементов страницы добавления профиля авторизации

Элемент	Описание
Поле «Название»	Текстовое поле для ввода названия профиля сетевого оборудования (до 50 символов)
Кнопка «Добавить описание»	По нажатию кнопки на странице дополнительно отображается поле «Описание» – текстовое поле для ввода описания профиля авторизации (до 250 символов). Под полем

Элемент	Описание
	отображается кнопка «Удалить описание», по нажатию которой поле «Описание» очищается и удаляется
Группа полей «Основные настройки»	
Поле «Тип доступа»	Поле с двумя кнопками для выбора типа доступа профиля авторизации: «Разрешен» или «Запрещен». По умолчанию выбран тип доступа «Разрешен»
Поле «Профиль сетевого оборудования»	Поле со списком для выбора профиля оборудования, с которым связан профиль авторизации. Список содержит записи из списка подраздела «Профили оборудования» (см п. 3.10.2)
Группа полей «Основные задачи»	
Загружаемые ACL	<p>Добавление загружаемого списка управления доступом включается/выключается по нажатию кнопки соответственно «»/ «» слева от названия поля «Загружаемые ACL».</p> <p>После включения возможности в окне дополнительно отображается поле для выбора предварительно составленного DACL (см. подробнее п.3.10.4)</p> <p>Внимание.</p> <p>Данное поле доступно, если в ранее выбранном профиле сетевого оборудования присутствует radius-словарь производителя Cisco.</p>
ACL	<p>Добавление имени расширенного списка доступа (extended ACL), который предварительно заведен непосредственно на оборудовании.</p> <p>Внимание.</p> <p>При указании имени в конце обязательно добавить .in.</p> <p>Пример записи:</p> <div style="display: flex; align-items: center; margin-top: 10px;"> <div style="margin-right: 10px;">  ACL </div> <div style="border: 1px solid #ccc; padding: 5px; display: inline-block;">TEST-ACL.in</div> </div>

Элемент	Описание
Группа полей «Настройка атрибутов»	Предназначена для формирования списка проверяемых при подключении устройства атрибутов и их значений. Примечание. Для выбора доступны фиксированные атрибуты, поддерживаемые словарями, доступными в ПК «Efros ACS». Проверяемые атрибуты добавляются по нажатию кнопки «Добавить» (+), строка для выбора атрибута и его значения добавляется под строкой, в которой нажата кнопка «Добавить». Лишние строки с атрибутами удаляются по нажатию кнопки «Удалить» (-) в соответствующей строке
Кнопки управления	
Добавить	По нажатию кнопки выполняется переход на страницу списка профилей авторизации с сохранением внесенных данных
Отменить	По нажатию кнопки выполняется переход на страницу списка профилей авторизации без сохранения внесенных данных
Сбросить	По нажатию кнопки значения поля окна создания профиля авторизации устанавливаются в положение по умолчанию

- 2) Заполнить поле страницы «Название».
- 3) Добавить, при необходимости, описание для профиля авторизации, нажав кнопку «Добавить описание» и заполнив отобразившееся поле «Описание».
- 4) Выбрать тип доступа профиля.
- 5) Выбрать связанный профиль сетевого оборудования.
- 6) Выбрать при необходимости DACL. Загружаемый список управления доступом предварительно создается в комплексе (см. п. 3.10.4);
- 7) Указать при необходимости имя расширенного списка управления доступом (ACL). Данный список предварительно заводится непосредственно на сетевом оборудовании.
- 8) Сформировать список проверяемых атрибутов и их значений.
- 9) Нажать кнопку «Добавить».

Будет запущен процесс проверки заполненности всех обязательных полей и уникальности добавляемого профиля оборудования по наименованию.

При обнаружении незаполненных обязательных полей рядом с первым из таких полей отобразится всплывающая подсказка «Обязательное поле», в случае обнаружения в

списке дубликата профиля авторизации в верхней части страницы отобразится соответствующее сообщение. Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Добавить».

Если проверки завершились без обнаружения ошибок, то окно добавления закрывается, профиль авторизации добавляется в список профилей авторизации и становится доступен для выбора при создании/редактировании правил авторизации в наборах политик.

В журнал событий ПК «Efros ACS» будут внесены соответствующие сообщения.

Удаление созданного профиля авторизации выполняется в соответствии с разделом 3.2.6.

3.10.3.2. Добавление профиля авторизации путем копирования имеющейся записи

Для добавления нового профиля авторизации путем копирования записи имеющегося профиля пользователю необходимо:

- 1) Выбрать установкой флага в левой крайней графе таблицы списка профилей исходный профиль. В верхней части таблицы отобразится строка выбора операций в соответствии с рис. 125.
- 2) Нажать в строке кнопку «Создать копию» (). Откроется страница добавления нового профиля авторизации, аналогичная приведенной на рис. 124. Все поля страницы будут заполнены данными исходного профиля, кроме поля «Название».
- 3) Далее пользователю необходимо внести требуемые изменения и нажать кнопку «Добавить». Правила заполнения полей страницы и действия системы после нажатия кнопки «Добавить» приведены в п.п. 3.10.3.1.

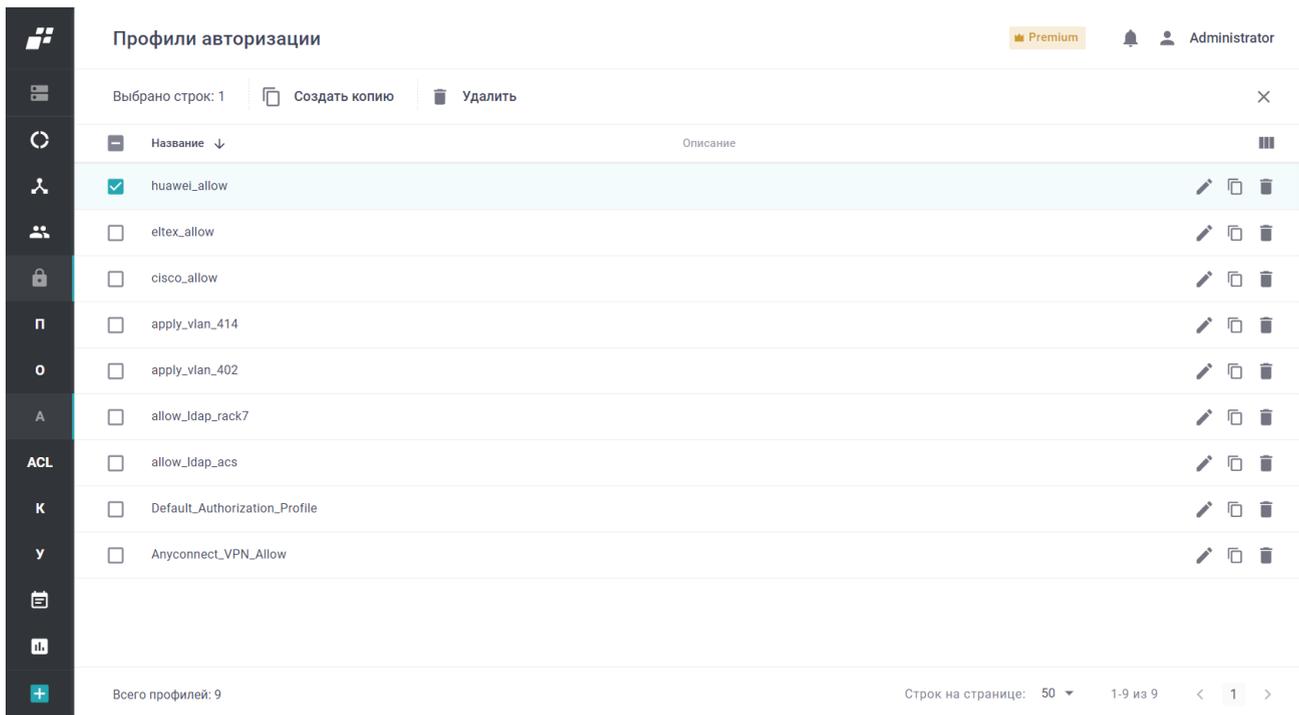


Рисунок 127 – Рисунок 125 – Страница списка профилей авторизации со строкой выбора операций

3.10.4. Загружаемые ACL

Загружаемые ACL работают только с оборудованием Cisco!

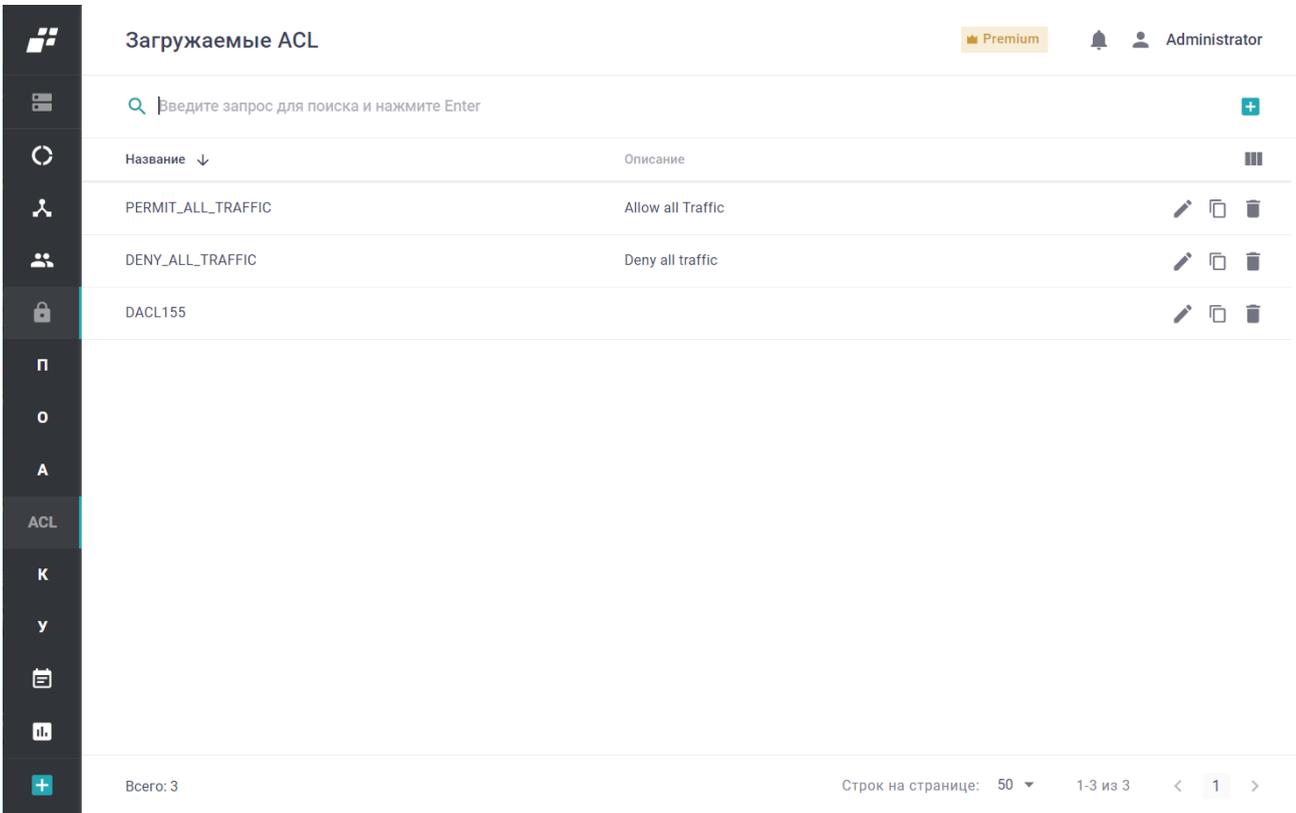
В данном разделе осуществляется настройка загружаемого списка управления доступом (DACL) непосредственно на программном комплексе для дальнейшей передачи на порт коммутатора в виде атрибутов RADIUS, специфичных для поставщика cisco-av-pair.

Для просмотра и ведения списка загружаемых ACL пользователю необходимо выбрать в главном меню раздела «Политики доступа» подраздел «Загружаемые ACL», откроется соответствующая страница, содержащая список созданных ранее наборов, загружаемых ACL (списков управления доступом, которые применяются на порт коммутатора). Загружаемые ACL добавляются, редактируются или удаляются в списке вручную администраторами ACS.

На рис. 126 приведена страница с вкладкой «Загружаемые ACL» для администраторов ACS, данные доступны для редактирования. На странице для администраторов RO над таблицей отсутствует кнопка «Добавить набор» () и в таблице отсутствуют кнопки:

- «Изменить» () – для перехода на страницу редактирования записи списка;
- «Удалить» () – для удаления соответствующей записи списка.

Над таблицей располагается поле поиска (🔍) – для ввода последовательности символов из искомой записи. Процесс поиска запускается после ввода символов нажатием клавиши ENTER клавиатуры.



Название ↓	Описание	
PERMIT_ALL_TRAFFIC	Allow all Traffic	  
DENY_ALL_TRAFFIC	Deny all traffic	  
DACL155		  

Рисунок 128 – Рисунок 126 – Страница загружаемых ACL

Для каждой записи списка отображаются данные:

- название – является ссылкой, при выборе которой раскрывается страница с возможностью редактирования текущего загружаемого ACL (рис. 127);
- описание.

The screenshot shows the configuration page for a loaded ACL named "PERMIT_ALL_TRAFFIC". The interface includes a sidebar with navigation icons and a main content area. The main content area has the following elements:

- Header: "← PERMIT_ALL_TRAFFIC" and "Premium Administrator".
- Form fields:
 - "Название" (Name): Input field containing "PERMIT_ALL_TRAFFIC".
 - "Описание" (Description): Input field containing "Allow all Traffic".
 - "Удалить описание" (Delete description): A blue link below the description field.
 - "DACL": Input field containing "permit ip any any".
 - "Проверить синтаксис" (Check syntax): A button below the DACL field.
- Buttons: "Сохранить" (Save) and "Отменить" (Cancel) at the bottom.

Рисунок 129 – Рисунок 127 – Загружаемый ACL

3.10.4.1. Добавление загружаемых ACL

Для добавления в список нового списка администратору ACS необходимо:

- 1) Нажать над таблицей кнопку «Добавить» (+) или нажать в панели главного меню кнопку «Добавить» и выбрать в открывшемся меню пункты «Политики доступа»– «Набор команд». Откроется окно добавления загружаемых ACL, приведенное на рис. 128. Состав и описание элементов страницы приведены в таблице 37.

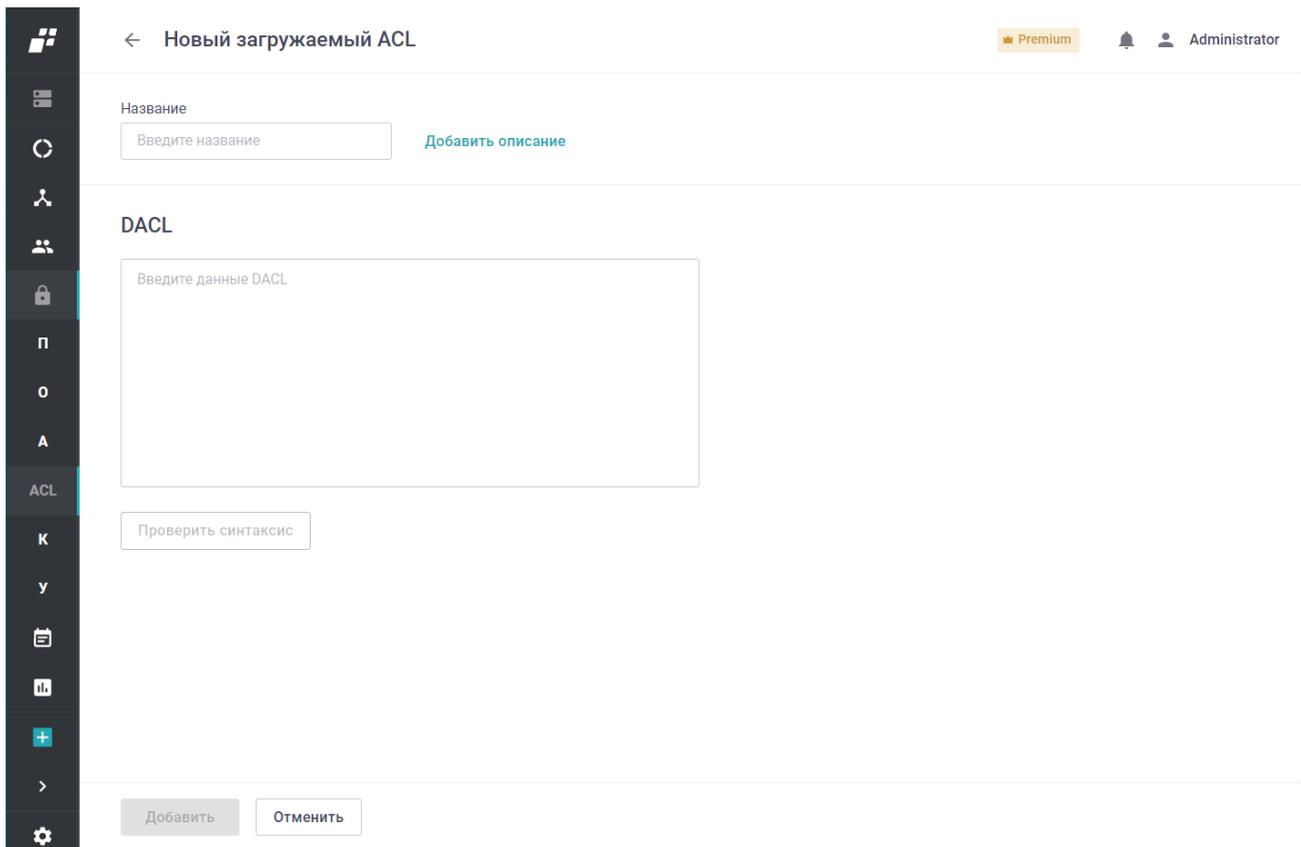


Рисунок 130 – Рисунок 128 – Страница добавления набора команд

Таблица 37 – Состав и описание элементов страницы добавления загружаемых ACL

Элемент	Описание
Поле «Название»	Текстовое поле для ввода названия политики доступа (до 50 символов)
Кнопка «Добавить описание»	По нажатию кнопки на странице дополнительно отображается поле «Описание» – текстовое поле для ввода описания (до 250 символов). Под полем отображается кнопка «Удалить описание», по нажатию которой поле «Описание» очищается и удаляется
DACL	DACL – Downloadable Access Control List Поле для заполнения аргументов доступа. Внимание. Заполнение поля осуществляется в соответствии с синтаксисом оборудования Cisco! Список представляет собой набор текстовых выражений, в каждом правиле определяется действие над пакетом: permit (разрешить) или deny (запретить).

Элемент	Описание
	<p>Проверка осуществляется по очередности приведенных выражений.</p> <p>В конце списка стоит неявный запрет на весь трафик (deny any), используется ограничивающий контроль доступа: запрещено все, что явно не разрешено выражениями.</p> <p>Под полем отображается кнопка «Проверить синтаксис», по нажатию которой осуществляется проверка корректности введенных аргументов.</p>
Кнопки управления	
Добавить	По нажатию кнопки выполняется переход на страницу загружаемых ACL с сохранением внесенных данных
Отменить	По нажатию кнопки выполняется переход на страницу загружаемых ACL без сохранения внесенных данных
Сбросить	Кнопка отображается на странице после заполнения хотя бы одного поля. По нажатию кнопки все введенные данные в окне удаляются

- 2) Заполнить поле страницы «Название».
- 3) Добавить, при необходимости, описание для DACL, нажав кнопку «Добавить описание» и заполнив отобразившееся поле «Описание».
- 4) Сформировать список контроля доступа.
- 5) Нажать кнопку «Добавить».

Будет запущен процесс проверки заполненности всех обязательных полей, наличия хотя бы одной команды и уникальности добавляемой политики доступа по наименованию.

При:

- обнаружении незаполненных обязательных полей рядом с первым из таких полей отобразится всплывающая подсказка «Обязательное поле»;
- пустом списке команд в верхней части страницы отобразится соответствующее сообщение;
- обнаружении в списке дубликата политики доступа в верхней части страницы отобразится соответствующее сообщение.

Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Добавить».

Если проверки завершились без обнаружения ошибок, то окно добавления закрывается, политика доступа добавляется в список политик доступа и становится доступна для выбора при создании/редактировании пользователя, группы пользователей.

В журнал событий ПК «Efros ACS» будет внесено сообщение:

- при успешном завершении – сообщение типа «Инфо» в формате: «Администратор {имя_выполняющего_операцию_администратора}: Политика доступа {название_политики_доступа} успешно создана»;
- при обнаружении ошибки – сообщение типа «Ошибка» в формате: «Администратор {имя_выполняющего_операцию_администратора}: Ошибка создания политики доступа - {текст_ошибки}».

3.10.4.2. Добавление загружаемых ACL путем копирования записи имеющегося набора команд

Для добавления нового DACL путем копирования записи необходимо:

- 1) Нажать в строке кнопку «Создать копию» (). Откроется страница добавления нового набора команд, аналогичная приведенной на рис. 129. Все поля страницы будут заполнены данными исходного набора, кроме поля «Название».
- 2) Далее пользователю необходимо внести требуемые изменения и нажать кнопку «Добавить». Правила заполнения полей страницы и действия системы после нажатия кнопки «Добавить» приведены в п.п. 3.10.4.1

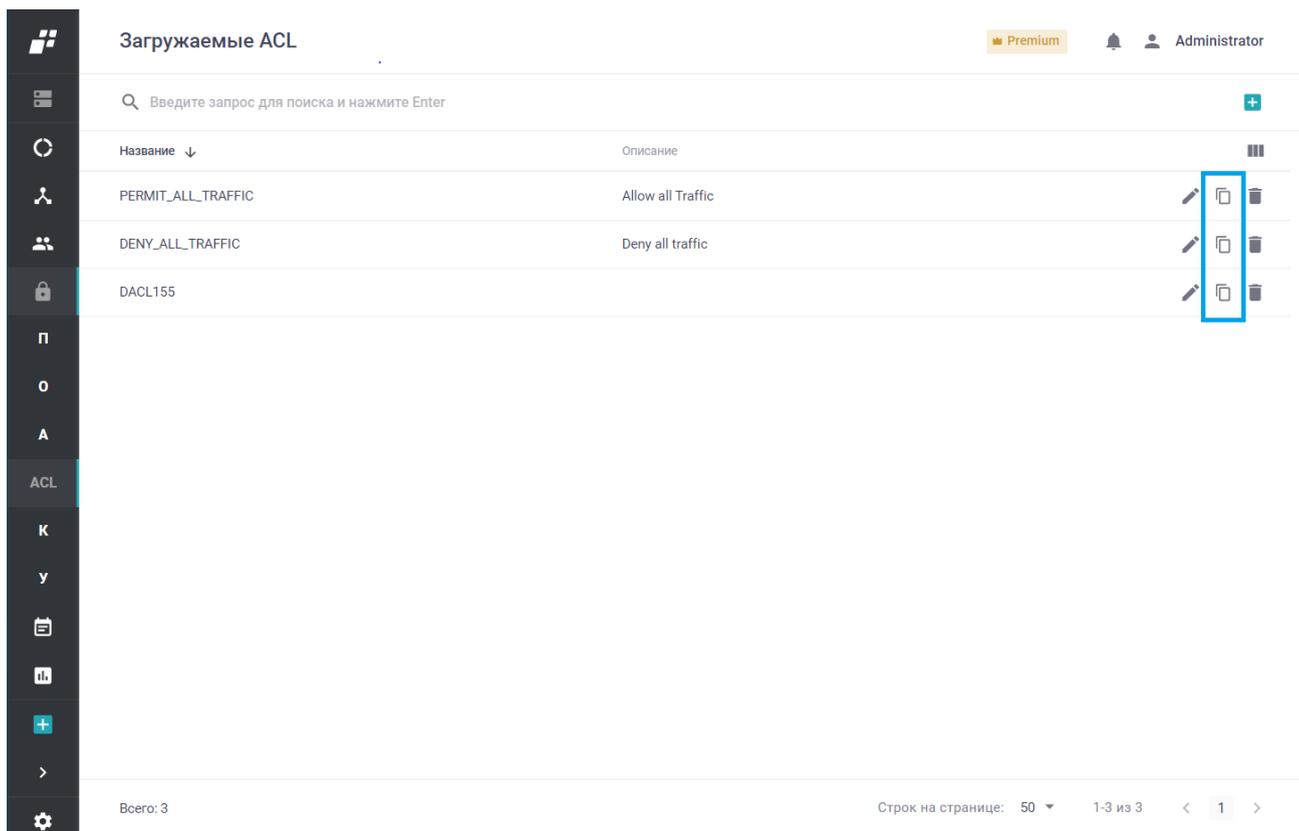


Рисунок 131 – Рисунок 129 – Страница списка набора команд со строкой выбора операций

3.10.5. Наборы команд

Для просмотра и ведения списка набора команд пользователю необходимо выбрать в главном меню раздела «Политики доступа» и подраздел «Наборы команд». Откроется страница «Политики доступа» с активной вкладкой «Служба выполнения команд», содержащая список созданных ранее наборов команд (политик доступа пользователей к контролируемым устройствам). Политики доступа добавляются, редактируются или удаляются в списке вручную администраторами ACS.

На рис. 130 приведена страница с вкладкой «Служба выполнения команд» для администраторов ACS, данные доступны для редактирования. На странице для администраторов RO над таблицей отсутствует кнопка «Добавить набор» (+) и в таблице отсутствуют кнопки:

- «Изменить» (✎) – для перехода на страницу редактирования записи списка;
- «Удалить» (🗑) – для удаления соответствующей записи списка.

Над таблицей располагается поле поиска (🔍) – для ввода последовательности символов из искомой записи. Процесс поиска запускается после ввода символов нажатием клавиши ENTER клавиатуры.

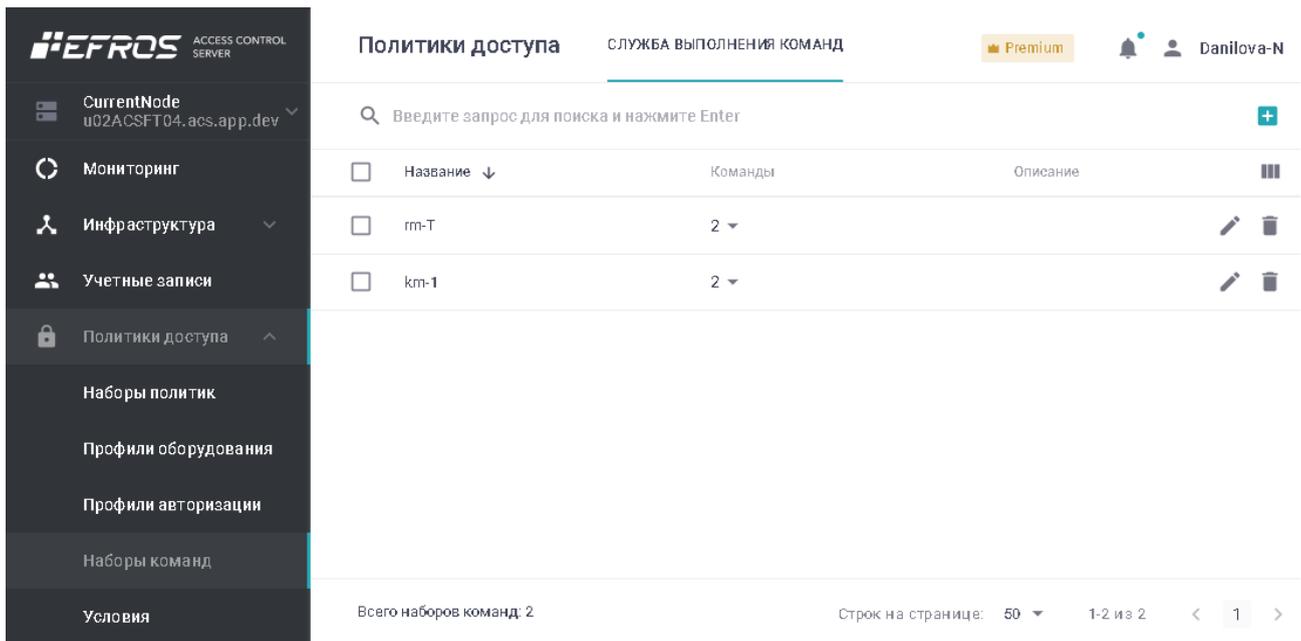


Рисунок 132 – Рисунок 130 – Страница списка службы выполнения команд

Для каждой записи списка отображаются данные:

- название;
- количество входящих в политику доступа команд. Является ссылкой, при выборе которой раскрывается список команд с указанием соответствующих действий и аргументов (рис. 131);
- описание.

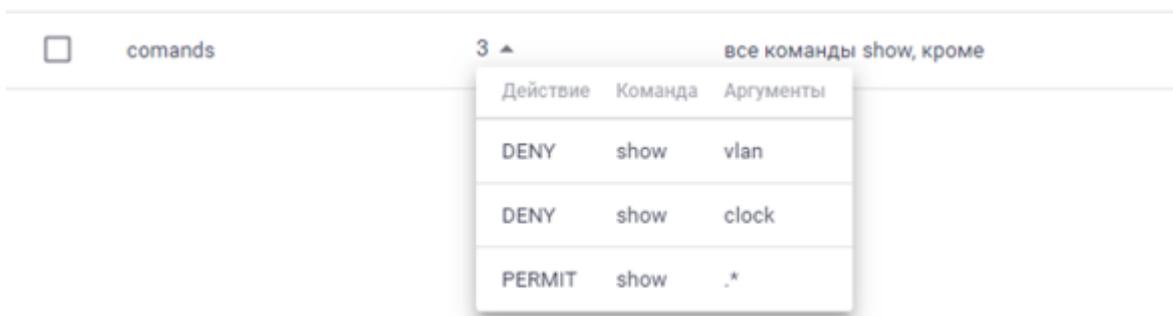


Рисунок 133 – Рисунок 131 – Набор команд с раскрытым списком команд

3.10.5.1. Добавление набора команд

Для добавления в список нового набора команд администратору ACS необходимо:

- 1) Нажать над таблицей кнопку «Добавить» (+) или нажать в панели главного меню кнопку «Добавить» и выбрать в открывшемся меню пункты «Политики доступа»– «Набор команд». Откроется окно добавления набора команд, приведенное на рис. 132. Состав и описание элементов страницы приведены в таблице 38.

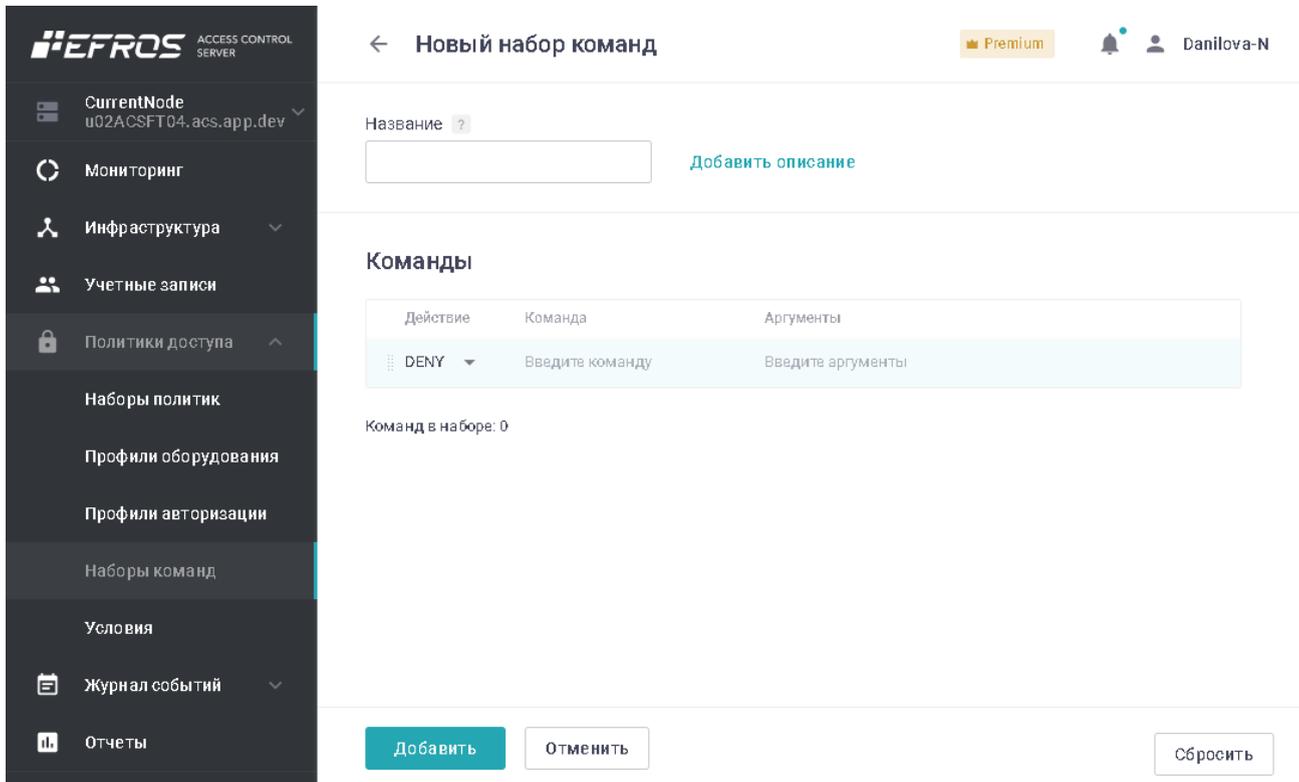


Рисунок 134 – Рисунок 132 – Страница добавления набора команд

Таблица 38 – Состав и описание элементов страницы добавления набора команд

Элемент	Описание
Поле «Название»	Текстовое поле для ввода названия политики доступа (до 50 символов)
Кнопка «Добавить описание»	По нажатию кнопки на странице дополнительно отображается поле «Описание» – текстовое поле для ввода описания набора команд (до 250 символов). Под полем отображается кнопка «Удалить описание», по нажатию которой поле «Описание» очищается и удаляется
Таблица команд	После заполнения содержит список разрешенных (PERMIT) или запрещенных (DENY) для выполнения команд с указанными аргументами. Правила ведения списка приведены в п.п. 3.10.5.3

Элемент	Описание
Кнопки управления	
Добавить	По нажатию кнопки выполняется переход на страницу списка политик доступа с сохранением внесенных данных
Отменить	По нажатию кнопки выполняется переход на страницу списка политик доступа без сохранения внесенных данных
Сбросить	Кнопка отображается на странице после заполнения хотя бы одного поля. По нажатию кнопки все введенные данные в окне удаляются

- 2) Заполнить поле страницы «Название».
- 3) Добавить, при необходимости, описание для набора команд, нажав кнопку «Добавить описание» и заполнив отобразившееся поле «Описание».
- 4) Сформировать список команд политики доступа, выполнив действия в соответствии с п.п. 3.10.5.3.
- 5) Нажать кнопку «Добавить».

Будет запущен процесс проверки заполненности всех обязательных полей, наличия хотя бы одной команды и уникальности добавляемой политики доступа по наименованию.

При:

- обнаружении незаполненных обязательных полей рядом с первым из таких полей отобразится всплывающая подсказка «Обязательное поле»;
- пустом списке команд в верхней части страницы отобразится соответствующее сообщение;
- обнаружении в списке дубликата политики доступа в верхней части страницы отобразится соответствующее сообщение.

Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Добавить».

Если проверки завершились без обнаружения ошибок, то окно добавления закрывается, политика доступа добавляется в список политик доступа и становится доступна для выбора при создании/редактировании пользователя, группы пользователей.

В журнал событий ПК «Efros ACS» будет внесено сообщение:

- при успешном завершении – сообщение типа «Инфо» в формате: «Администратор {имя_выполняющего_операцию_администратора}: Политика доступа {название_политики_доступа} успешно создана»;

- при обнаружении ошибки – сообщение типа «Ошибка» в формате: «Администратор {имя_выполняющего_операцию_администратора}: Ошибка создания политики доступа - {текст_ошибки}».

3.10.5.2. Добавление набора команд путем копирования записи имеющегося набора команд

Для добавления нового набора команд путем копирования записи необходимо:

- 1) Выбрать установкой флага в левой крайней графе таблицы списка набора команд исходную политику. В верхней части таблицы отобразится строка выбора операций в соответствии с рис. 133.
- 2) Нажать в строке кнопку «Создать копию» (📄). Откроется страница добавления нового набора команд, аналогичная приведенной на рис. 132. Все поля страницы будут заполнены данными исходного набора команд, кроме поля «Название».
- 3) Далее пользователю необходимо внести требуемые изменения и нажать кнопку «Добавить». Правила заполнения полей страницы и действия системы после нажатия кнопки «Добавить» приведены в п.п. 3.10.5.1

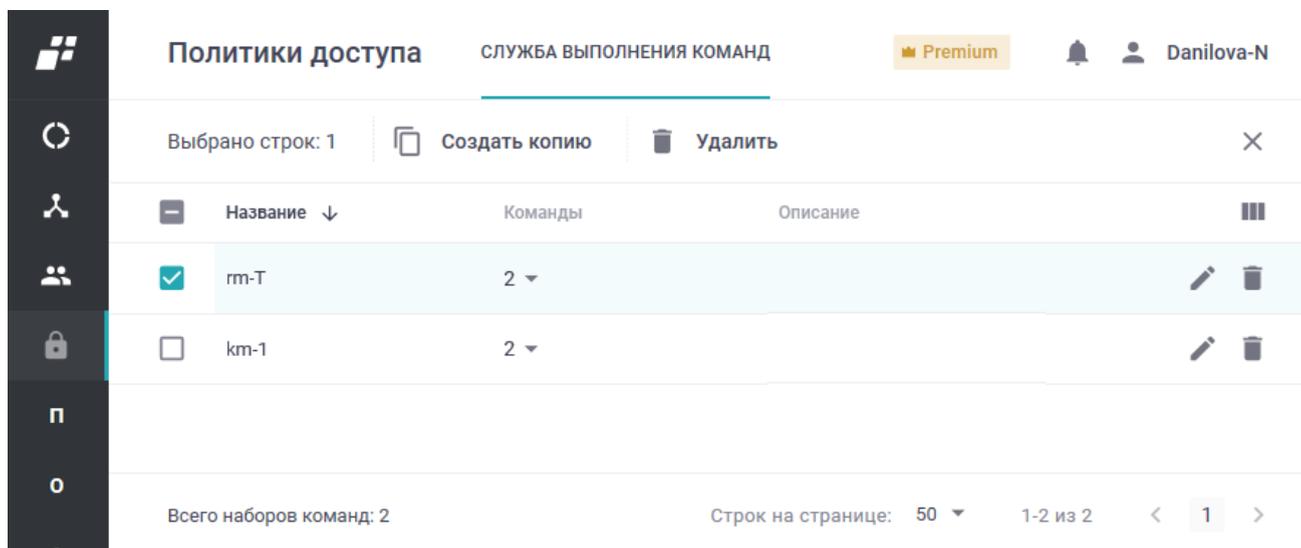


Рисунок 135 – Рисунок 133 – Страница списка набора команд со строкой выбора операций

3.10.5.3. Ведение списка набора команд

Для добавления в набор команды на странице добавления/редактирования (см. рис. 133) необходимо:

- 1) Выбрать в столбце «Действия» одно из действий: PERMIT (разрешить) или DENY (запретить).
- 2) Ввести в столбце «Команда» наименование команды. В строке добавляемой команды в соответствии с рис. 134 отобразятся кнопки:

Действие	Команда	Аргументы
DENY ▾	qwe	Введите аргументы  

Рисунок 136 – Рисунок 134 – Строка таблицы команд в режиме добавления/редактирования команды

- 3) «Сохранить» () – для сохранения внесенных изменений;
- 4) «Сбросить» () – для удаления внесенных данных.
- 5) Ввести в поле «Аргументы» значение аргумента, с которым команда соответственно разрешена или запрещена к выполнению.
- 6) Нажать кнопку «Сохранить» ()

 Наименование команды не должно содержать пробелов. В значении аргумента допустимы любые символы. Суммарное количество символов в наименовании команды и значении аргумента не должно превышать 512 символов.

После сохранения внесенных изменений в таблице в соответствии с рис. 135 добавится строка для ввода новой команды, в строке добавленной команды отобразятся кнопки:

- «Редактировать» () – для перехода в режим редактирования данных команды;
- «Копировать» () – для добавления в таблицу копии команды;
- «Создать выше» () – для добавления в таблицу строки новой команды над строкой исходной команды;
- «Создать ниже» () – для добавления в таблицу строки новой команды под строкой исходной команды;
- «Удалить» () – для удаления строки команды.

 Удаление команды выполняется без подтверждения действия со стороны пользователя!

Действие	Команда	Аргументы						
⋮ DENY	qwe	.*						
⋮ DENY ▾	Введите команду	Введите аргументы						

Рисунок 137 – Рисунок 135 – Таблица команд после добавления первой команды

Администратор ACS имеет возможность добавить далее требуемые команды:

- заполняя новые строки;
- копируя имеющиеся команды;
- добавляя и заполняя строки выше и ниже строк имеющихся команд.

 Скопированные команды должны быть отредактированы, поскольку в списке не допускаются дубликаты сочетания значений «Команда», «Аргумент».

В сформированном списке администратор ACS имеет возможность:

- редактировать имеющиеся команды (по кнопке «Редактировать»);
- удалять неактуальные команды (по кнопке «Удалить»);
- задавать последовательность проверки доступности выполнения команд с заданными аргументами при попытках доступа пользователей ПК «Efros ACS» к АСО.

Порядок следования команд в списке изменяется путем перетаскивания символов  строк вверх/вниз.

-  1) Если в наборе команд для команды с каким-то аргументом задано значение «PERMIT», то разрешено будет выполнять только эту команду с таким аргументом. Остальные аргументы – запрещены.
- 2) Если в наборе команд для команды с аргументом задано значение «DENY», то правило будет наложено. Чтобы разрешить выполнение этой же команды с другими аргументами необходимо в одной из строк ниже в списке команд указать действие «PERMIT» с аргументом «.*».

3.10.5.4. Редактирование набора команд

Редактирование выполняется администратором ACS вручную средствами веб-приложения ПК «Efros ACS». При редактировании для внесения изменений доступны все данные набора команд.

Для редактирования администратору ACS необходимо выбрать в списке с помощью «мыши» название требуемого набора команд либо нажать в строке кнопку «Изменить» (✎). Откроется страница редактирования, которая содержит внесенные ранее данные. Состав элементов страницы и правила заполнения полей страницы аналогичны составу страницы добавления политики доступа и правилам добавления политики (см. п.п. 3.10.5.1). Далее пользователю необходимо внести требуемые изменения и нажать кнопку «Сохранить».

Будет запущен процесс проверки заполненности всех обязательных полей, наличия хотя бы одной команды и уникальности добавляемой политики доступа по наименованию. При:

- обнаружении незаполненных обязательных полей рядом с первым из таких полей отобразится всплывающая подсказка «Обязательное поле»;
- пустом списке команд в верхней части страницы отобразится соответствующее сообщение;
- обнаружении в списке дубликата политики доступа в верхней части страницы отобразится соответствующее сообщение.

Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Сохранить».

Если проверки завершились без обнаружения ошибок, то окно добавления закрывается, политика доступа добавляется в список политик доступа и становится доступна для выбора при создании/редактировании пользователя, группы пользователей.

В журнал событий ПК «Efros ACS» будет внесено сообщение:

- при успешном завершении – сообщение типа «Инфо» в формате: «Администратор {имя_выполняющего_операцию_администратора}: Политика доступа {название_политики_доступа} успешно обновлена»;
- при обнаружении ошибки – сообщение типа «Ошибка» в формате: «Администратор {имя_выполняющего_операцию_администратора}: Ошибка обновления политики доступа - {текст_ошибки}».

3.10.6. Конструктор условий

Конструктор условий используется для создания и управления шаблонами условий, для дальнейшего применения данных шаблонов как части правил, настроенных для

конкретного набора политик, или для сохранения в наборе для дальнейшего использования. Созданный шаблон условий поддерживает до трех уровней вложенности условий (правил), которые могут быть построены с любым уровнем сложности.

Для перехода в конструктор условий необходимо выбрать в разделе «Политики доступа» панели главного меню приложения ссылку «Условия» либо нажать в панели главного меню кнопку «Добавить» и выбрать в открывшемся меню пункты «Политики доступа»– «Условие». Откроется страница «Условия» (рис. 136), содержащая блоки полей:

- «Конструктор условий» – предоставляет инструменты для создания, сохранения и редактирования шаблонов условий;
- список предустановленных и созданных ранее пользователями (пользовательских) шаблонов условий. По умолчанию список содержит наименования всех имеющихся в системе шаблонов. Пользователь может отфильтровать список, выбрав в меню фильтрации списка (рис. 137) значения «Мои шаблоны» (пользовательские шаблоны) или «Предустановленные шаблоны».

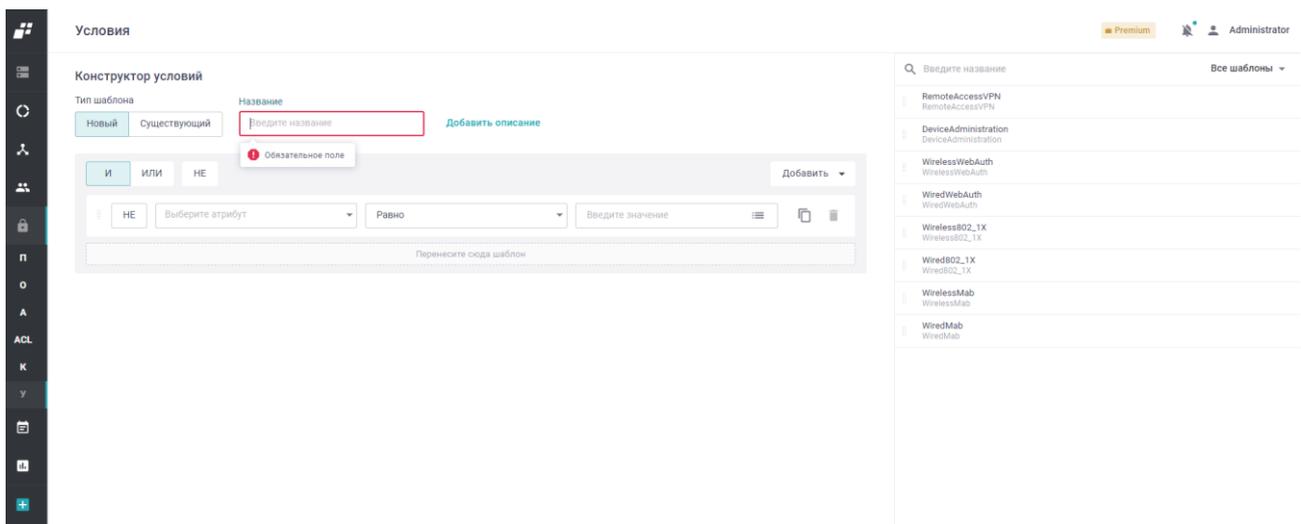


Рисунок 138 – Рисунок 136 – Страница «Условия»

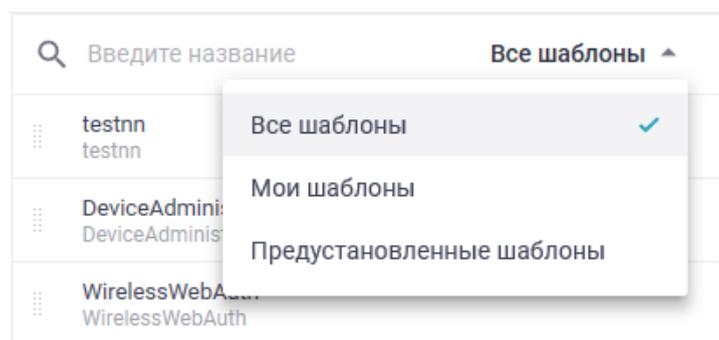


Рисунок 139 – Рисунок 137 – Меню фильтрации списка шаблонов условий

Шаблоны условий добавляются и редактируются вручную администраторами ACS в соответствии с п.п. 3.10.6.1. Шаблоны могут быть использованы для создания новых шаблонов условий.

Для удаления доступны только пользовательские шаблоны, не включенные в текущий момент времени в списки условий в наборах политик. Для удаления шаблона необходимо навести курсор на строку требуемого шаблона в списке шаблонов страницы «Условия», нажать отобразившуюся в строке кнопку «Удалить» (🗑️) и нажать в открывшемся окне подтверждения кнопку «Удалить».

3.10.6.1. Добавление нового шаблона условий

Для добавления в список нового шаблона условий администратору ACS необходимо:

- 1) Выбрать в блоке полей «Конструктор условий» страницы «Условия» (см. рис. 136) тип шаблона «Новый».
- 2) Заполнить обязательное поле «Название», при необходимости добавить описание в соответствующее поле.
- 3) Для создания нового условия редактор появляется только с одной пустой строкой с выбранным по умолчанию оператором «И», в которую необходимо добавить первое правило (рис. 138). Описание полей редактора приведено в таблице 38.

Рисунок 140 – Рисунок 138 – Поле для добавления первого правила

Таблица 39 – Состав и описание элементов страницы добавления шаблона условий

Элемент	Описание
Поле «Тип шаблона»	Поле с кнопками для выбора типа шаблона: — «Новый» – для создания нового шаблона условий; — «Существующий» – для создания нового шаблона на базе созданного ранее шаблона. По умолчанию нажата кнопка «Новый»
Поле «Шаблоны»	Поле отображается на странице только после выбора типа шаблона «Существующий». Содержит список созданных

Элемент	Описание
	ранее пользователями шаблонов условий (предустановленные шаблоны не доступны для внесения изменений и в списке не отображаются)
Поле «Название»	Текстовое поле для ввода названия шаблона (до 50 символов)
Поле «Описание»	Текстовое поле для ввода описания шаблона (до 250 символов)
Группа полей (редактор) для формирования списка условий	
Группа кнопок «И», «ИЛИ»	Предназначены для выбора оператора для определения условия обработки запроса. По умолчанию выбран оператор «И»
Кнопка «НЕ»	Предназначена для определения правила обработки результата выполнения оператора, выбранного выше («И», «ИЛИ»). По умолчанию оператор выключен
Кнопка «Добавить»	Кнопка для добавления нового условия или иерархического уровня. По нажатию кнопки раскрывается меню для выбора действия по добавлению: <ul style="list-style-type: none">— нового шаблона;— условия «ИЛИ»;— условия «И»
Группа полей для задания атрибутов	Содержит: <ul style="list-style-type: none">— кнопка оператора «НЕ». По умолчанию оператор выключен;— поле выбора атрибута. Содержит список системных словарей и их атрибутов, доступных пользователю для выбора проверяемого атрибута;— поле выбора условия. Содержит значения условий: «Равно», «Не равно», «Содержит», «Не содержит», «Начинается с», «не начинается с», «Заканчивается на», «Не заканчивается на»;— поле ввода/выбора значения атрибута (правила заполнения зависят от типа выбранного ранее атрибута: число, константа, строка);— кнопка «Дублировать» () – для дублирования правила в рамках одного уровня или уровня полностью;

Элемент	Описание
	— кнопка «Удалить» () – для удаления правила в рамках одного уровня или уровня полностью
Поле «Перенесите сюда шаблон»	Поле предназначено для вставки условия из имеющегося в системе шаблона (список шаблонов в правой части страницы «Условия»)
Кнопки управления	
Добавить	По нажатию кнопки выполняется переход на страницу списка политик доступа с сохранением внесенных данных
Отменить	По нажатию кнопки выполняется переход на страницу «Мониторинг» без сохранения внесенных данных
Сбросить	По нажатию кнопки значения поля окна создания шаблона условий устанавливаются в положение по умолчанию

4) Новое правило можно указать самостоятельно, выбрав вручную атрибут из предлагаемого списка, проверяемое условие и значение атрибута, либо выбрав в списке шаблонов в правой части страницы требуемый шаблон условий и перетащив его наименование в поле «Перенесите сюда шаблон». Для добавления нового правила в рамках одного уровня иерархии необходимо воспользоваться кнопкой «Добавить» → «Новый шаблон» (рис. 139). Для копирования правила в рамках одного уровня необходимо воспользоваться кнопкой «Дублировать» () , для удаления – «Удалить» () .

5)

 При выборе условия на верхнем уровне иерархии («И», «ИЛИ», «НЕ»), оно применяется к этому разделу и ко всем нижестоящим уровням. Поддерживается иерархия до трех уровней вложенности.

6) Для добавления нового уровня вложенности необходимо воспользоваться кнопкой «Добавить» → «Условие ИЛИ» или «Условие И».

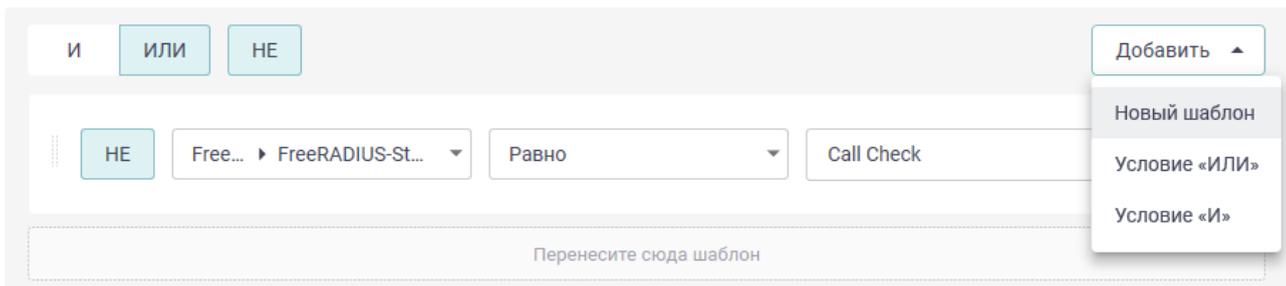


Рисунок 141 – Рисунок 139 – Поле для добавления нового правила на другом уровне

7) Добавление необходимых правил осуществляется аналогичным образом (рис. 140).

8)

i Строки с добавляемыми новыми уровнями имеют отступ, основанный на его положении в иерархии. Чтобы изменить оператор, после того как был выбран и создан соответствующий уровень, необходимо изменить опцию сверху данного уровня (нажать кнопку «И», «ИЛИ», «НЕ»).

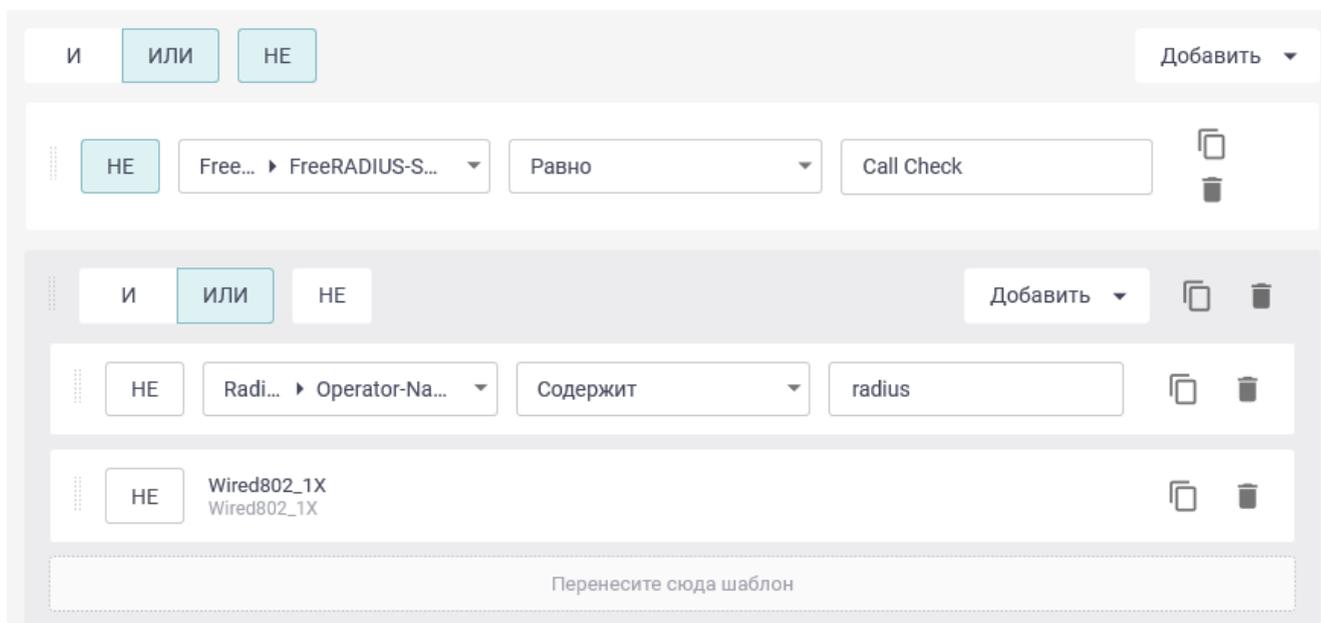


Рисунок 142 – Рисунок 140 – Добавление правил для построения шаблона условий

9) После определения необходимых условий для сохранения шаблона необходимо нажать кнопку «Добавить».

Будет запущен процесс проверки уникальности добавляемого шаблона условий по названию, заполненности всех обязательных полей и корректности выбранных пар атрибут-значение.

При обнаружении незаполненных обязательных полей рядом с первым из таких полей отобразится всплывающая подсказка «Обязательное поле», в случае обнаружения в списке дубликата шаблона или некорректно заданных условий в верхней части страницы отобразится соответствующее сообщение. Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Добавить».

Если проверки завершились без обнаружения ошибок, то созданный шаблон будет добавлен в набор условий, его наименование отобразится в списке шаблонов (в правой части страницы). Шаблон станет доступен для выбора при формировании условий в наборах политик (см. раздел 3.10.1).

В журнал событий ПК «Efros ACS» будет внесено соответствующее сообщение.

3.10.6.2. Редактирование пользовательского шаблона условий

Для редактирования в ПК «Efros ACS» доступны только пользовательские шаблоны условий.

Для редактирования шаблона условий администратору ACS необходимо:

- 1) Выбрать в блоке полей «Конструктор условий» страницы «Условия» (см. рис. 136) тип шаблона «Существующий».
- 2) Выбрать в отобразившемся поле «Шаблоны» наименование требуемого шаблона. В полях страницы отобразятся данные выбранного шаблона (рис. 141).
- 3) Внести необходимые изменения в поля «Название», «Описание» и в набор условий. Правила заполнения полей приведены в п.п. 3.10.6.1.
- 4) Нажать кнопку «Сохранить».

Будет запущен процесс проверки уникальности шаблона условий по названию, заполненности всех обязательных полей и корректности выбранных пар атрибут-значение.

При обнаружении незаполненных обязательных полей рядом с первым из таких полей отобразится всплывающая подсказка «Обязательное поле», в случае обнаружения в списке дубликата шаблона или некорректно заданных условий в верхней части страницы отобразится соответствующее сообщение. Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Сохранить».

Если проверки завершились без обнаружения ошибок, то внесенные изменения будут сохранены.



Внесенные в шаблон условий изменения применяются во всех наборах политик, в которых шаблон условий включен.

В журнал событий ПК «Efros ACS» будет внесено соответствующее сообщение.

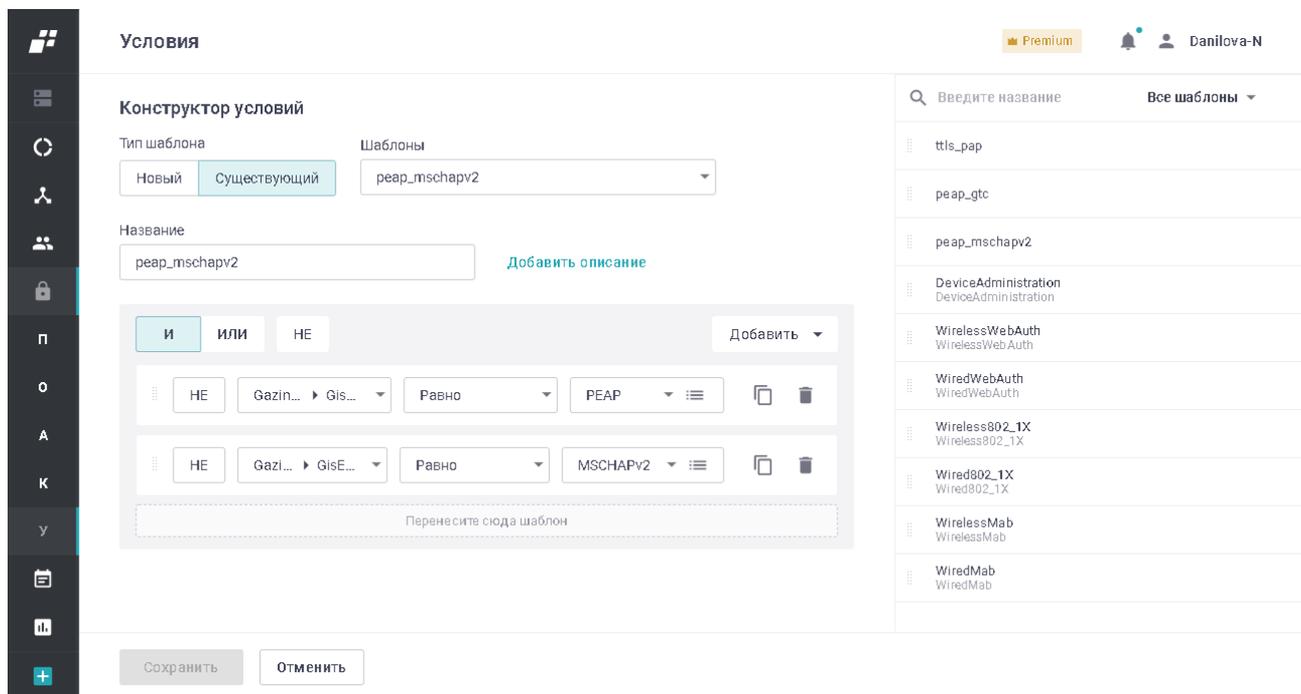


Рисунок 143 – Рисунок 141 – Страница редактирования шаблона условий

3.11 Просмотр и выгрузка журналов событий ПК «Efros ACS»

3.11.1. Общие сведения

Для выполнения функции по просмотру и выгрузке журналов событий ПК «Efros ACS» необходимо выбрать в панели главного меню приложения ссылку «Журнал событий».

В панели раскроется список ссылок на журналы событий:

- «TACACS+» – для перехода на страницу просмотра зафиксированных в ПК «Efros ACS» событий, связанных с работой пользователей с устройствами, использующими протокол TACACS+;
- «RADIUS» – для перехода на страницу просмотра зафиксированных в ПК «Efros ACS» событий, связанных с работой пользователей с устройствами, использующими протокол RADIUS;
- «Система» – для перехода на страницу просмотра зафиксированных в ПК «Efros ACS» системных событий.

По умолчанию журналы содержат записи о событиях за последние 3 месяца¹¹. Пользователь имеет возможность:

- просмотреть все записи журналов;
- выполнить поиск данных (см. п. 3.2.2);
- включить/отключить нажатием кнопки «Live-режим» (👁) в журналах событий «TACACS+» и «RADIUS» режим автоматического обновления списка событий (внешний вид кнопки: «👁» – режим выключен, «👁» – режим включен). При выключенном режиме списки обновляются только вручную при переходе по страницам ПК «Efros ACS» или по нажатию клавиши F5 клавиатуры;
- выполнить в журналах событий «TACACS+» и «RADIUS» фильтрацию данных (см. п. 3.2.4);
- выбрать интервал дат фиксации события (см. п. 3.2.3);
- выгрузить записи журнала (с учетом заданных правил поиска и фильтрации) в файл формата CSV или XLSX;
- выбрать состав отображаемых в интерфейсе приложения колонок таблиц журналов (см. п. 3.2.5).

Сортировка данных в таблицах журналов по умолчанию производится по убыванию значений в столбце «Дата и время». Пользователь имеет возможность задать другой тип сортировки, выбрав заголовок требуемого столбца таблицы. В заголовке отобразится знак «↓», сортировка всех строк таблицы будет выполнена по убыванию значений выбранного столбца. Для изменения направления сортировки необходимо повторно выбрать заголовок столбца. В заголовке отобразится знак «↑».

3.11.2. Просмотр журнала событий «TACACS+»

При выборе в панели главного меню ссылки «TACACS+» открывается страница «Журнал событий: TACACS+», приведенная на рис. 142.

Страница содержит вкладки:

- «Аутентификация» – содержит сообщения о событиях, связанных с попытками аутентификации пользователей (результаты проверки подлинности пользователей);
- «Авторизация» – содержит сообщения о событиях, связанных с попытками авторизации пользователей (результаты попыток пользователей выполнить команды на устройствах);

¹¹ Срок хранения записей журналов хранится в конфигурационном файле ПК «Efros ACS» и может быть изменен

— «Аудит» – содержит сообщения о событиях, связанных с работой пользователей на устройствах после получения доступа к ним.

Состав и описание доступных для просмотра данных зафиксированных событий для всех вкладок журнала приведен в таблице 40.

 Состав данных, отображаемых в интерфейсе приложения, зависит от выбранного состава отображаемых в интерфейсе приложения колонок таблиц журналов (по кнопке «»).

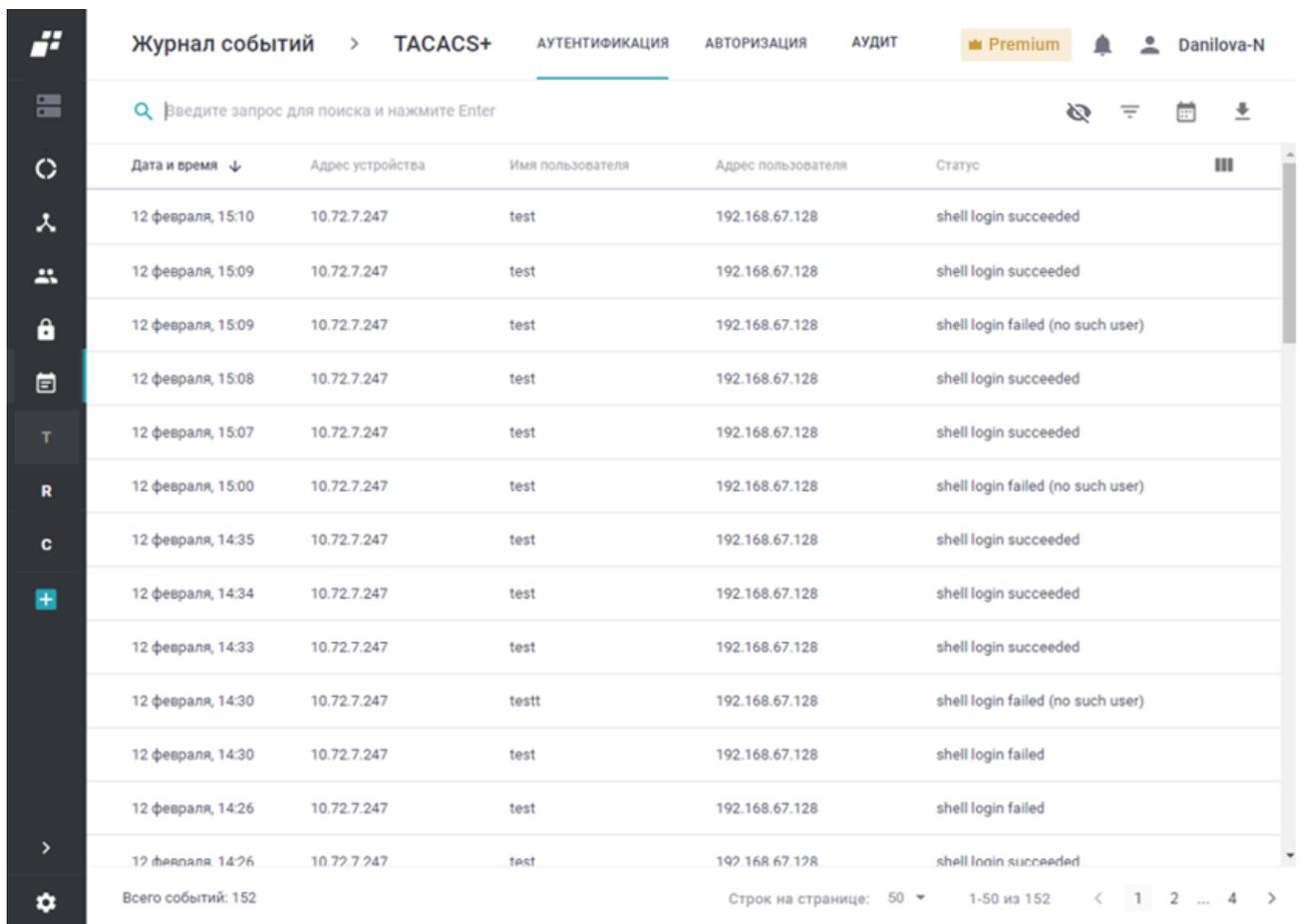


Рисунок 144 – Рисунок 142 – Страница «Журнал событий: TACACS+»

Таблица 40 – Состав и описание данных для каждой записи вкладок журнала событий «TACACS+»

Столбец	Описание
Вкладка «Аутентификация»	
Дата и время	Дата и время фиксации события

Столбец	Описание
IP-адрес устройства	IP-адрес устройства, доступ к которому пытался получить пользователь
Пользователь	Логин пользователя
Интерфейс устройства	Название интерфейса устройства
IP-адрес пользователя	IP-адрес ЭВМ, с которого была осуществлена попытка доступа
Действие	Выполненное действие. Текст столбца зависит от настройки протокола TACACS+. Например: «shell login» – попытка аутентификации
Статус	Статус попытки аутентификации. Текст столбца зависит от настройки протокола TACACS+. Например: «succeeded» – успешное выполнение действия
Вкладка «Авторизация»	
Дата и время	Дата и время фиксации события
IP-адрес устройства	IP-адрес устройства, на котором пользователь пытался выполнить команду
Пользователь	Логин пользователя
Интерфейс устройства	Тип интерфейса устройства
IP-адрес пользователя	IP-адрес ЭВМ, с которого была осуществлена попытка выполнения команды
Действие	Выполненное действие
Статус	Статус попытки выполнения команды. Текст столбца зависит от настройки протокола TACACS+. Например: «permit» – успешная попытка
Команда	Выполняемая на устройстве команда
Аргументы	Аргументы, с которыми команда выполнялась
Вкладка «Аудит»	
Дата и время	Дата и время фиксации события

Столбец	Описание
IP-адрес устройства	IP-адрес устройства, на котором пользователь выполнил команду
Пользователь	Логин пользователя
Интерфейс устройства	Название интерфейса устройства
IP-адрес пользователя	IP-адрес ЭВМ, с которого была выполнена команда
Тип сеанса	Значения: — «start» – начало сеанса работы с устройством; — «stop» – окончание сеанса работы с устройством
Идентификатор сеанса	Порядковый номер, присвоенный сеансу работы с устройством в начале его выполнения
Часовой пояс	Часовой пояс на устройстве
Служба выполнения команд	Значения: «shell», «slip», «ppp», «arap», «tty-daemon» и т.д.
Уровень доступа	Уровень доступа – определяет, какие команды могут выполнять пользователи после входа в сетевое устройство (возможные значения – 1 и 15)
Команда	Выполняемая на устройстве команда
Причина отключения	Причина, по которой сеанс был прерван, используется с записями «stop». Возможные значения: – 1 – User Request; – 2 – Lost Carrier; – 3 – Lost Service; – 4 – Idle Timeout; – 5 – Session Timeout; – 6 – Admin Reset; – 7 – Admin Reboot; – 8 – Port Error; – 9 – NAS Error; – 10 – NAS Request;

Столбец	Описание
	<ul style="list-style-type: none">– 11 – NAS Reboot;– 12 – Port Unneeded;– 13 – Port Preempted;– 14 – Port Suspended;– 15 – Service Unavailable;– 16 – Callback;– 17 – User Error;– 18 – Host Request
Расширенная причина отключения	Расширение атрибута причины отключения. Параметр специфичен для конкретного устройства, значение зависит от производителя
Продолжительность аутентификации	Продолжительность аутентификации в секундах
Продолжительность сеанса	Продолжительность сеанса в секундах
Время завершения сеанса	Дата и время завершения сеанса работы с устройством

3.11.3. Просмотр журнала событий «RADIUS»

При выборе в панели главного меню ссылки «RADIUS» открывается страница «Журнал событий: RADIUS», приведенная на рис. 143. Страница содержит вкладки:

- «Аутентификация» – содержит сообщения о событиях, связанных с попытками аутентификации пользователей (результаты проверки подлинности пользователей);
- «Аудит» – содержит сообщения о событиях, связанных с работой пользователей на устройствах после получения доступа к ним.

Состав и описание доступных для просмотра данных зафиксированных событий для всех вкладок журнала приведен в таблице 41.

 Состав данных, отображаемых в интерфейсе приложения, зависит от выбранного состава отображаемых в интерфейсе приложения колонок таблиц журналов (по кнопке «»).

Дата и время	IP-адрес устройства	Пользователь	Тип ответа	Тип аутентификации	Тип EAP	Адрес пользователя	Идентификатор устройства
13 октября, 20:55:26	10.72.2.161	petrov	Access-Accept	MS-CHAP	PEAP		
13 октября, 20:52:04	10.72.2.161	petrov	Access-Reject	MS-CHAP	PEAP		
13 октября, 20:46:02	10.72.2.161	petrov	Access-Reject	MS-CHAP	PEAP		
12 октября, 18:19:16	10.72.2.184	Senab16S	Access-Reject	PAP			
12 октября, 18:19:08	10.72.2.184	user	Access-Accept	PAP			
12 октября, 18:08:34	10.72.2.184	Senab16S	Access-Reject	PAP			
12 октября, 18:06:57	10.72.2.184	Senab16S	Access-Reject	PAP			
12 октября, 18:06:51	10.72.2.184	user	Access-Accept	PAP			
12 октября, 18:06:44	10.72.2.184	user	Access-Reject	PAP			
12 октября, 18:05:37	10.72.2.184	Senab16S	Access-Reject	PAP			
12 октября, 18:05:30	10.72.2.184	Senab16S	Access-Reject	PAP			
12 октября, 18:05:24	10.72.2.184	user	Access-Accept	PAP			
12 октября, 18:04:14	10.72.2.184	user	Access-Reject	PAP			

Рисунок 145 – Рисунок 143 – Страница «Журнал событий: RADIUS»

Таблица 41 – Состав и описание данных для каждой записи вкладок журнала событий «RADIUS»

Столбец	Описание
Вкладка «Аутентификация»	
Дата и время	Дата и время фиксации события
IP-адрес устройства	IP-адрес устройства, доступ к которому пытался получить пользователь
Пользователь	Логин пользователя
Тип ответа	Значения: — «Accept» – доступ к устройству разрешен; — «Reject» – доступ к устройству не разрешен
Тип аутентификации	Указывается тип, с помощью которого проводится аутентификация по протоколу RADIUS. Возможные значения: — LDAP – аутентификация пользователя, хранящегося в службе каталогов (например, Active Directory);

Столбец	Описание
	— EAP – аутентификация клиентского устройства с помощью одного из методов EAP (например, PEAP).
Тип EAP	Указывается метод аутентификации с использованием EAP
Сообщение	Поясняющий текст
IP-адрес пользователя	IP-адрес ЭВМ, с которого была осуществлена попытка доступа
Тип службы	Указывает тип запрашиваемой или предоставляемой службы, например: <ul style="list-style-type: none">– Login;– Framed;– Callback-Login;– Callback-Framed;– Outbound;– Administrative;– NAS-Prompt;– Authenticate Only;– Callback-NAS-Prompt
Тип интерфейса	Тип физического порта устройства, через который подключается пользователь, например: <ul style="list-style-type: none">– Asynchronous;– Synchronous;– ISDN-Synchronous;– ISDN-Asynchronous (V.120);– ISDN-Asynchronous (V.110);– Virtual;– Ethernet
Интерфейс устройства	Название интерфейса устройства
Идентификатор устройства	Идентификатор устройства

Столбец	Описание
Корневые сертификаты	Название корневого сертификата, на основании которого выпущен использованный для аутентификации клиентский сертификат
Клиентские сертификаты	Название использованный для аутентификации клиентского сертификата
Тип аутентификации EAP	Тип аутентификации EAP, по которому произведена аутентификации
Имя оборудования	Имя оборудования
Политики доступа	Название политики доступа, по которой получен доступ к устройству
Сценарий доступа	Сценарий доступа
Правило аутентификации	Название правила аутентификации, по которому выполнена аутентификация
Правило авторизации	Название правила авторизации, по которому выполнена авторизация
Источник данных	Локальный или название внешней системы (LDAP-источника)
Тип источника данных	Локальный или LDAP
Вкладка «Аудит»	
Начало сеанса	Дата и время фиксации события
IP-адрес устройства	IP-адрес устройства, на котором пользователь выполнил команду
Пользователь	Логин пользователя
Интерфейс устройства	Название интерфейса устройства
Тип интерфейса	Тип физического порта устройства, через который подключается пользователь (примеры см. выше)
Обновление сеанса	Дата и время последнего обновления сеанса работы с устройством
Интервал обновления	Интервал обновления сеанса в секундах
IP-адрес пользователя	IP-адрес ЭВМ, с которого была осуществлена попытка доступа

Столбец	Описание
Тип аутентификации	Индикация того, что пользователь уже прошел аутентификацию с помощью протокола RADIUS, собственно устройства или иным способом. Возможные значения: <ul style="list-style-type: none">— RADIUS;— Local (локальная аутентификация);— Remote (удаленная аутентификация)
Завершение сеанса	Дата и время завершения сеанса работы с устройством
Продолжительность сеанса	Продолжительность сеанса в секундах
Идентификатор сеанса	Порядковый номер, присвоенный сеансу работы с устройством в начале его выполнения. Стартовая и конечная запись для данной сессии имеют одинаковые значения идентификатора сеанса
Уникальный идентификатор сеанса	Дополнительный идентификатор сеанса
Область	Область
Входящий трафик	Размер входящего трафика
Исходящий трафик	Размер исходящего трафика
Сервер	Имя сервера
Клиент	Имя клиента
Причина отключения	Причина отключения
Тип службы	Тип службы
Тип пакетного протокола	Тип пакетного протокола
Адрес пользователя IPv6	IPv6-адрес ЭВМ, с которого была осуществлена попытка доступа
Префикс IPv6	Префикс сети IPv6, используемый для маршрутизации
Идентификатор интерфейса IPv6	Идентификатор интерфейса IPv6, используемый для идентификации сетевого интерфейса
Делегированный префикс IPv6	Делегированный префикс IPv6

3.11.4. Просмотр журнала событий «Система»

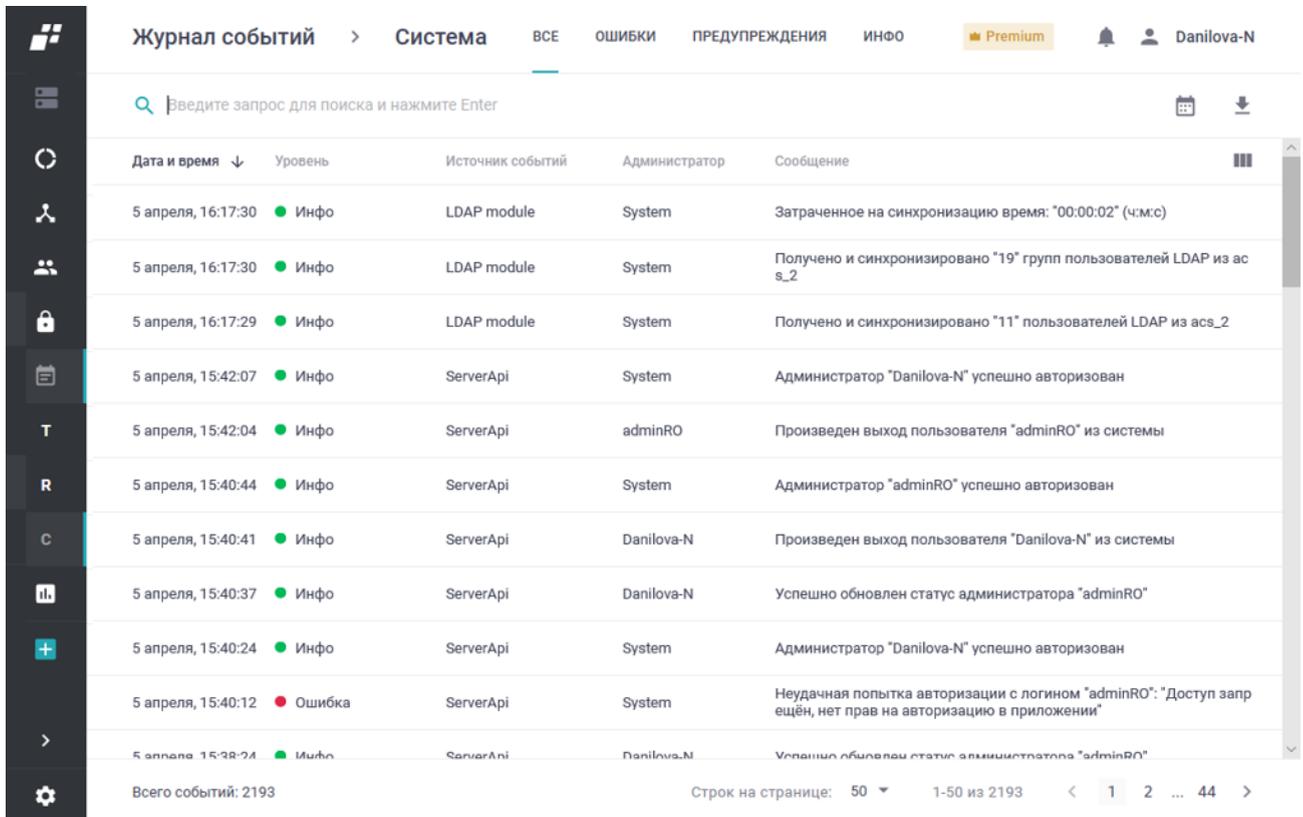
При выборе в панели главного меню ссылки «Система» открывается страница «Журнал событий: Система», приведенная на рис. 144.

Страница содержит вкладки с данными событий, зафиксированных за последние три месяца в ПК «Efros ACS» при работе служб и приложения:

- «Все» – содержит сообщения обо всех событиях;
- «Ошибки» – содержит сообщения обо всех событиях типа «Ошибка»;
- «Предупреждения» – содержит сообщения обо всех событиях типа «Предупреждение»;
- «Инфо» – содержит сообщения обо всех событиях типа «Информационное».

Состав и описание доступных для просмотра данных зафиксированных событий для всех вкладок журнала одинаков и приведен в таблице 42.

 Состав данных, отображаемых в интерфейсе приложения, зависит от выбранного состава отображаемых в интерфейсе приложения колонок таблиц журналов (по кнопке «»).



Дата и время ↓	Уровень	Источник событий	Администратор	Сообщение
5 апреля, 16:17:30	Инфо	LDAP module	System	Затраченное на синхронизацию время: "00:00:02" (ч:м:с)
5 апреля, 16:17:30	Инфо	LDAP module	System	Получено и синхронизировано "19" групп пользователей LDAP из acs_2
5 апреля, 16:17:29	Инфо	LDAP module	System	Получено и синхронизировано "11" пользователей LDAP из acs_2
5 апреля, 15:42:07	Инфо	ServerApi	System	Администратор "Danilova-N" успешно авторизован
5 апреля, 15:42:04	Инфо	ServerApi	adminRO	Произведен выход пользователя "adminRO" из системы
5 апреля, 15:40:44	Инфо	ServerApi	System	Администратор "adminRO" успешно авторизован
5 апреля, 15:40:41	Инфо	ServerApi	Danilova-N	Произведен выход пользователя "Danilova-N" из системы
5 апреля, 15:40:37	Инфо	ServerApi	Danilova-N	Успешно обновлен статус администратора "adminRO"
5 апреля, 15:40:24	Инфо	ServerApi	System	Администратор "Danilova-N" успешно авторизован
5 апреля, 15:40:12	Ошибка	ServerApi	System	Неудачная попытка авторизации с логином "adminRO": "Доступ запрещён, нет прав на авторизацию в приложении"
5 апреля, 15:38:24	Инфо	ServerApi	Danilova-N	Успешно обновлен статус администратора "adminRO"

Всего событий: 2193

Строк на странице: 50 1-50 из 2193 < 1 2 ... 44 >

Рисунок 146 – Рисунок 144 – Страница «Журнал событий: Система»

Таблица 42 – Состав и описание данных для каждой записи вкладок журнала событий «Система»

Столбец	Описание
Дата и время	Дата и время фиксации события
Уровень	Тип события: «Ошибка», «Предупреждение» или «Информационное»
Источник события	Название подсистемы ПК «Efros ACS», по результатам работы которой зафиксировано событие
Администратор	Логин пользователя, действия которого привели к фиксированию события, либо значение «System», если событие зафиксировано в результате автоматической работы ПК «Efros ACS»
Сообщение	Поясняющий текст

3.11.5. Экспорт журналов в файлы формата CSV и XLSX

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

- 1) Перейти на страницу выгружаемого журнала.
- 2) Выбрать вкладку, данные которой необходимо выгрузить.
- 3) Выполнить, при необходимости, поиск и фильтрацию данных журнала.
- 4) Нажать над таблицей журнала кнопку «Экспорт журнала» (↓). Откроется окно настройки параметров выгрузки, приведенное на рис. 145. В заголовке окна отображается общее количество выгружаемых записей.
- 5) Ввести название файла, который будет сформирован в результате выгрузки.
- 6) Указать установкой переключателя формат файла.
- 7) Нажать кнопку «СКАЧАТЬ».

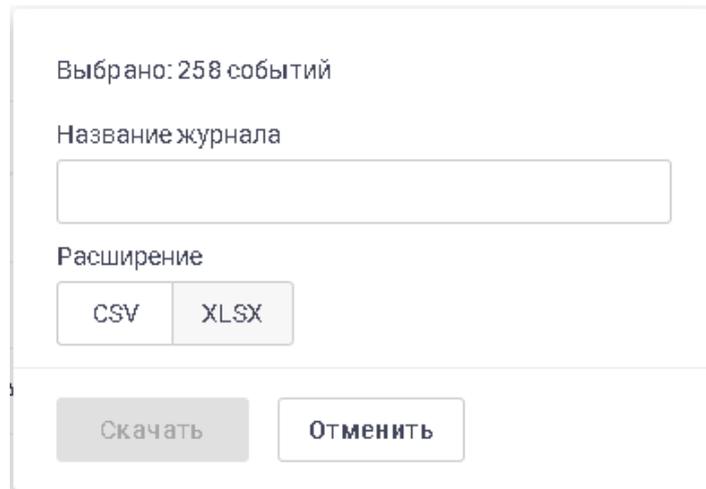


Рисунок 147 – Рисунок 145 – Окно настройки параметров выгрузки

После завершения процесса выгрузки записей – файл с записями событий сохранен локально на ЭВМ, в верхней части страницы отобразится сообщение «Файл <имя файла> успешно создан и экспортирован».

Для просмотра файла с выгруженными данными необходимо нажать ссылку в нижней части страницы браузера.

 В файл выгружаются данные всех колонок вкладки, вне зависимости от текущей настройки отображаемых колонок в интерфейсе приложения!

3.12 Отчеты ПК «Efros ACS»

Для выполнения функций по работе с отчетами ПК «Efros ACS» необходимо выбрать в панели главного меню приложения ссылку «Отчеты». Откроется страница «Отчеты» с активной вкладкой «Шаблоны».

Отчеты в ПК «Efros ACS» формируются на основе созданных ранее шаблонов отчетов. Список шаблонов доступен администраторам ACS и администраторам RO для просмотра и редактирования во вкладке «Шаблоны» (см. п. 3.12.1). Список сформированных отчетов доступен пользователям для просмотра во вкладке «Результаты» (см. п. 3.12.2).

3.12.1. Шаблоны отчетов

Вкладка «Шаблоны» (рис. 146) содержит список созданных ранее шаблонов, по которым формируются отчеты ПК «Efros ACS». Создавать шаблоны имеют право администраторы ACS и администраторы RO. Созданные шаблоны доступны для просмотра, редактирования и удаления.

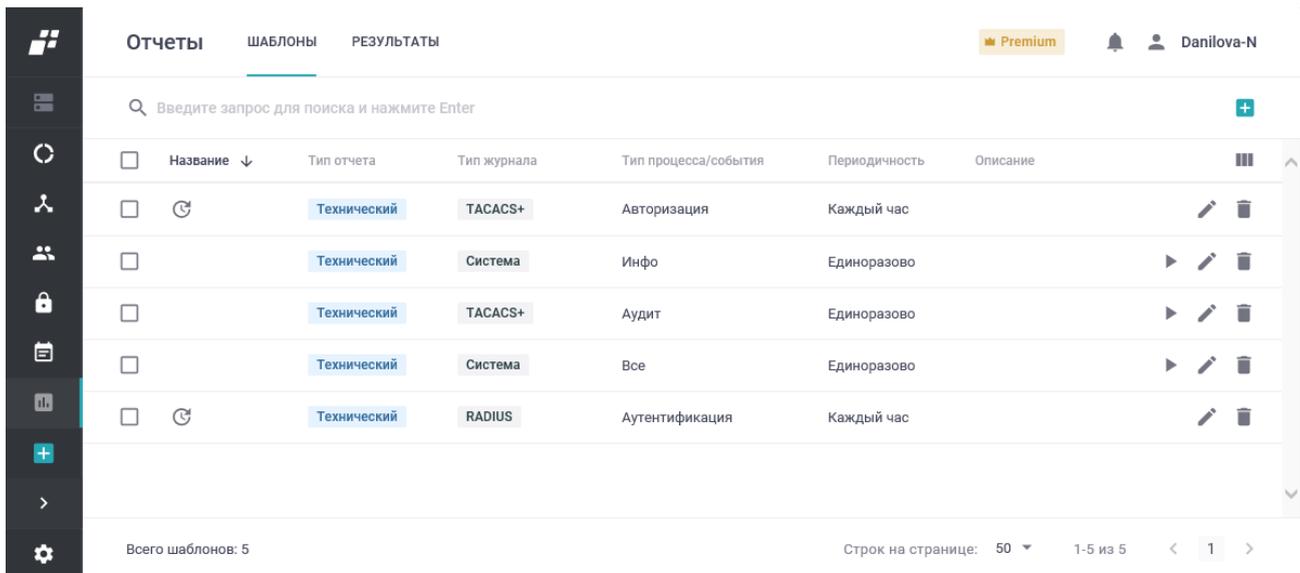


Рисунок 148 – Рисунок 146 – Страница «Отчеты». Вкладка «Шаблоны»

Примечание. После установки ПК «Efros ACS» список шаблонов отчетов пуст, на странице отображается сообщение «В системе нет шаблонов отчетов» и кнопка «Добавить» () для перехода на страницу создания нового шаблона отчета.

Для каждого шаблона отчета отображаются данные:

- название шаблона;
- тип журнала событий ПК «Efros ACS», на основе данных из которого отчет будет формироваться;
- тип процесса/события – вкладка журнала событий ПК «Efros ACS»;
- периодичность формирования отчетов по шаблону: «Единоразово» (далее – непериодические отчеты) или «Каждый час», «Каждый день», «Каждую неделю», «Каждый месяц» (для отчетов, для которых в шаблоне настроена соответствующая периодичность формирования (далее – периодические отчеты));
- описание шаблона.

Над таблицей располагаются:

- поле поиска. Правила поиска приведены в п. 3.2.2
- кнопка «Добавить» () – для перехода на страницу добавления нового шаблона отчета.

В таблице также доступны следующие кнопки:

- «Сформировать отчет» () – для запуска вручную процесса формирования отчета (кнопка доступна только для непериодических отчетов);

- «Изменить» (✎) – для перехода на страницу редактирования шаблона;
- «Удалить» (🗑) – для удаления соответствующего шаблона.

Сортировка данных в таблице шаблонов по умолчанию производится по убыванию значений в столбце «Название». Пользователь имеет возможность задать другой тип сортировки, выбрав заголовок требуемого столбца таблицы. В заголовке отобразится знак «↓», сортировка всех строк таблицы будет выполнена по убыванию значений выбранного столбца. Для изменения направления сортировки необходимо повторно выбрать заголовок столбца. В заголовке отобразится знак «↑».

3.12.1.1. Добавление нового шаблона отчета

Для добавления нового шаблона отчета пользователю необходимо:

- 1) Нажать над таблицей шаблонов отчетов кнопку «Добавить» (+). Откроется окно добавления шаблона отчета, приведенное на рис. 146.
- 2) Заполнить поле «Название», добавить, при необходимости, описание шаблона, нажав кнопку «Добавить описание» и заполнив отобразившееся поле «Описание», либо установить флаг в поле «Автоматическая генерация».

i При установке флага «Автоматическая генерация» поля «Название» и «Описание» станут недоступны для редактирования, после сохранения параметров шаблона (нажатия кнопки «Добавить») в зависимости от выбранного языка при установке программного комплекса имя отчета будет создано автоматически в формате: «Отчет/Report № N, ДД.ММ.ГГГГ» (где N - порядковый номер создаваемого отчета, ДД.ММ.ГГГГ – текущая дата), поле «Описание» останется пустым.

← Новый шаблон Premium Danilova-N

Название ?

Добавить описание Автоматическая генерация

Обязательное поле

Основные настройки

Тип журнала ?

TACACS+ RADIUS Система

Добавить Отменить

Рисунок 149 – Рисунок 147 – Окно добавления шаблона отчета

- 3) Выбрать в поле «Тип журнала» нажатием кнопки тип журнала событий ПК «Efros ACS», на основе данных из которого будет формироваться отчет по шаблону.
- 4) После выбора типа журнала:
 - «TACACS+» или «RADIUS» на странице добавится поле «Процесс» для выбора вкладки журнала соответственно: «Аутентификация», «Авторизация», «Аудит» или «Аутентификация», «Аудит». После выбора одной из вкладок на странице добавятся поля для ввода параметров формирования отчета;
 - «Система» на странице добавится поле «Тип события» для выбора вкладки журнала «Все», «Ошибка», «Инфо», «Предупреждение» и дополнительные поля ввода параметров формирования отчета (состав дополнительных полей не зависит от типов событий).

Состав и описание дополнительных полей страницы для типа журнала «TACACS+» приведены в таблице 43, «RADIUS» – в таблице 44, «Система» – в таблице 45.

- 5) Для неперiodических отчетов:
 - выбрать – вид отчета «Динамический» или «Статический»;
 - задать для выбранного вида временные параметры формирования отчета;
 - заполнить остальные поля страницы, переключатель «Периодический отчет» при этом оставить в выключенном состоянии.
- 6) Для периодических отчетов:
 - перевести переключатель «Периодический отчет» в положение «» (включено);
 - задать в добавившихся полях периодичность формирования отчетов по шаблону.
- 7) Нажать кнопку «Добавить».

Таблица 43 – Состав и описание дополнительных полей страницы создания шаблона для типа журнала «TACACS+»

Столбец	Описание
Тип журнала «TACACS+». Процесс «Аутентификация»	
Группа полей «Дополнительные настройки»	
Вид отчета	Поле с кнопками «Динамический», «Статический» для выбора требуемого вида отчета: статические отчеты формируются на заданный промежуток дат и времени, динамические отчеты – на

Столбец	Описание
	<p>заданный период времени. Интервалы времени задаются в поле «Дата фиксации события» (см. ниже).</p> <p>ВНИМАНИЕ: Для периодических отчетов (см. ниже поле «Периодичный отчет») вид отчета не выбирается, Поле «Вид отчета» скрыто!</p>
Дата фиксации события	<p>Поле отображается только для неперiodических отчетов.</p> <p>Для динамических отчетов – поле со списком для выбора периода фиксации событий – сегодня, вчера, за последние 7 дней или за последние 30 дней.</p> <p>Для статических отчетов – два поля для ввода начальной и конечной дат периода фиксации событий.</p> <p>Даты также можно выбрать в окне выбора периода (см. п. 3.2.3), которое открывается по нажатию кнопки «Выбрать период» .</p> <p>Примечание. В окне отсутствует панель быстрого выбора периода</p>
Устройство	Поле со списком для выбора адреса сетевого оборудования, на котором аутентифицировался пользователь
Пользователь	Поле со списком для выбора пользователя, выполнявшего команду на сетевом устройстве
Статус	<p>Поле со списком для выбора статуса доступа пользователя к сетевому оборудованию. Состав значений списка зависит от настройки протокола TACACS+.</p> <p>Например: «permit» – успешная попытка</p>
Группа полей «Необходимо добавить отчет» В	<p>Содержит кнопки для выбора дополнительных данных, которые должны быть отражены в отчете:</p> <p>«Адрес пользователя» – адрес указанного пользователя;</p> <p>«Интерфейс устройства» – интерфейс устройства</p>
Переключатель «Периодичный отчет»	<p>Переключатель с двумя положениями «» (выключено) или «» (включено). По умолчанию установлен в положение «выключено», обязательным для выбора является вид отчета (см. выше поле «Вид отчета».)</p> <p>После включения переключателя отображаются дополнительные поля задания периодичности формирования отчетов по шаблону (см. ниже)</p>

Столбец	Описание
Группа полей задания периодичности формирования отчетов	<p>Содержит поле «Периодичность» – поле со списком для выбора типа периодичности: каждый час, каждый день, каждую неделю, каждый месяц. От выбранного типа зависит состав остальных полей группы.</p> <p>Если выбран тип периодичности:</p> <ul style="list-style-type: none"> — «Каждый час», то доступны поля для выбора интервала часов в сутках и интервала дат формирования отчетов; — «Каждый день», то доступны поля для выбора времени запуска и интервала дат формирования отчетов; — «Каждую неделю», то доступны поля для выбора времени запуска, дня недели и интервала дат формирования отчетов; — «Каждый месяц», то доступны поля для выбора времени запуска, интервала дат формирования отчетов и числа месяца. <p>ВНИМАНИЕ: Поле «Дата окончания» не может содержать дату, предшествующую дате в поле «Дата начала», поле «Время окончания» не может содержать время, предшествующее времени в поле «Время начала»</p>
Тип журнала «TACACS+». Процесс «Авторизация»	
Вид отчета, Дата фиксации события	<p>Поле «Вид отчета» содержит кнопки «Динамический», «Статический» для выбора требуемого вида отчета.</p> <p>Правила заполнения полей см. выше для процесса «Аутентификация»</p>
Устройство	Поле со списком для выбора адреса сетевого оборудования, на котором аутентифицировался пользователь
Статус	Статус для выбора статуса попытки выполнения команды на устройстве, возможен выбор одного из трех вариантов: «Все», «Разрешено», «Запрещено»
Пользователь	Поле со списком для выбора пользователя, выполнявшего команду на сетевом устройстве
Команда	Переключатель с двумя положениями «  » (выключено) или «  » (включено). По умолчанию установлен в положение «выключено», в отчет отбираются все события авторизации без учета выполненных на устройстве команд.

Столбец	Описание
	После включения переключателя отображаются дополнительные поля для ввода команд и аргументов. Для добавления новой команды необходимо нажать кнопку «Добавить команду» (+) справа от поля «Аргументы».
Группа полей «Необходимо добавить в отчет»	Содержит кнопки для выбора дополнительных данных, которые должны быть отражены в отчете: — «Адрес пользователя» – адрес указанного пользователя; — «Интерфейс устройства» – интерфейс устройства
Переключатель «Периодичный отчет» и группа полей задания периодичности формирования отчетов	см. выше описание полей для процесса «Аутентификация»
Тип журнала «TACACS+». Процесс «Аудит»	
Вид отчета, Дата фиксации события	Поле «Вид отчета» содержит кнопки «Динамический», «Статический» для выбора требуемого вида отчета. Правила заполнения полей см. выше для процесса «Аутентификация»
Устройство	Поле со списком для выбора адреса сетевого оборудования, на котором аутентифицировался пользователь
Пользователь	Поле со списком для выбора пользователя, выполнявшего команду на сетевом устройстве
Тип сеанса	Поле со списком для выбора типа события. Доступны значения: «start» – начало сеанса работы с устройством; «stop» – окончание сеанса работы с устройством
Причина отключения	Поле со списком для выбора причины, по которой сеанс был прерван, используется с записями типа сеанса «stop». Возможные значения: — 1 – User Request; — 2 – Lost Carrier; — 3 – Lost Service; — 4 – Idle Timeout; — 5 – Session Timeout;

Столбец	Описание
	<ul style="list-style-type: none">— 6 – Admin Reset;— 7 – Admin Reboot;— 8 – Port Error;— 9 – NAS Error;— 10 – NAS Request;— 11 – NAS Reboot;— 12 – Port Unneeded;— 13 – Port Preempted;— 14 – Port Suspended;— 15 – Service Unavailable;— 16 – Callback;— 17 – User Error;— 18 – Host Request
Уровень доступа	<p>Поле для выбора одного из трех уровней доступа пользователя¹²</p> <p>Возможные значения:</p> <ul style="list-style-type: none">— Все;— Уровень доступа – 1;— Уровень доступа – 15. <p>В отчете будут отображены доступные для выполнения команды</p>
Команда	<p>Переключатель с двумя положениями «» (выключено) или «» (включено). По умолчанию установлен в положение «выключено», в отчет отбираются все события аудита без учета команд.</p> <p>После включения переключателя отображается дополнительное поле для ввода команды. Для добавления новой команды необходимо нажать кнопку «Добавить команду» () справа от поля «Команда»</p>
Группа полей «Необходимо добавить в отчет»	<p>Содержит кнопки для выбора дополнительных данных, которые должны быть отражены в отчете:</p> <ul style="list-style-type: none">— «Адрес пользователя» – адрес указанного пользователя;— «Интерфейс устройства» – интерфейс устройства;— «Расширенная причина отключения» – расширение атрибута причины отключения. Параметр специфичен для конкретного устройства, значение зависит от производителя;

¹² Уровень доступа определяет какие команды могут выполняться пользователем после входа в сетевое устройство

Столбец	Описание
	<ul style="list-style-type: none"> — «Идентификатор сеанса» – порядковый номер, присвоенный сеансу работы с устройством в начале его выполнения; — «Часовой пояс» – часовой пояс на устройстве; — «Служба выполнения команд» – значения: «shell», « slip», «rpp», « arar», «tty-daemon» и т.д; — «Продолжительность аутентификации» – продолжительность аутентификации в секундах; — «Продолжительность сеанса» – продолжительность сеанса в секундах; — «Начало действия» – данные о начале действия; — «Время завершения сеанса» – дата и время завершения сеанса работы с устройством; — «Причина» – информация, которая описывает событие, вызвавшее изменение системы
Переключатель «Периодичный отчет» и группа полей задания периодичности формирования отчетов	см. выше описание полей для процесса «Аутентификация»

Таблица 44 – Состав и описание дополнительных полей страницы создания шаблона для типа журнала «RADIUS»

Столбец	Описание
Тип журнала «RADIUS». Процесс «Аутентификация»	
Группа полей «Дополнительные настройки»	
Вид отчета, Дата фиксации события	<p>Поле «Вид отчета» содержит кнопки «Динамический», «Статический» для выбора требуемого вида отчета.</p> <p>Правила заполнения полей см. выше в таблице 43 для процесса «Аутентификация» для типа журнала «TACACS+»</p>
Устройство	Поле со списком для выбора адреса сетевого оборудования, на котором аутентифицировался пользователь
Тип ответа	Поле для выбора тип ответа при попытке аутентификации пользователя на сетевом оборудовании. Возможные варианты: «Все», «Удачно», «Неудачно»

Столбец	Описание
Пользователь	Поле со списком для выбора пользователя, аутентифицирующегося на сетевом устройстве
Тип аутентификации	Поле со списком для выбора типа, с помощью которого проводится аутентификация по протоколу RADIUS
Тип TAP	Поле со списком для выбора метода аутентификации с использованием EAP
Группа полей «Необходимо добавить в отчет»	Содержит кнопки для выбора дополнительных данных, которые должны быть отражены в отчете: <ul style="list-style-type: none"> — «Адрес пользователя» – адрес указанного пользователя; — «Тип службы» – тип запрашиваемой или предоставляемой службы; — «Тип интерфейса» – тип физического порта устройства, через который подключается пользователь; — «Интерфейс устройства» – интерфейс устройства; — «Идентификатор устройства» – идентификатор устройства
Переключатель «Периодичный отчет» и группа полей задания периодичности формирования отчетов	см. выше в таблице 43 описание полей процесса «Аутентификация» для типа журнала «TACACS+»
Тип журнала «RADIUS». Процесс «Аудит»	
Группа полей «Дополнительные настройки»	
Вид отчета, Дата фиксации события	Поле «Вид отчета» содержит кнопки «Динамический», «Статический» для выбора требуемого вида отчета. Правила заполнения полей см. выше для процесса «Аутентификация» для типа журнала «TACACS+»
Устройство	Поле со списком для выбора адреса сетевого оборудования, на котором аутентифицировался пользователь
Тип аутентификации	Поле со списком для выбора типа, с помощью которого проводится аутентификация по протоколу RADIUS
Пользователь	Поле со списком для выбора пользователя, аутентифицирующегося на сетевом устройстве

Столбец	Описание
Тип интерфейса	Поле для выбора типа физического порта устройства, через который подключается пользователь
Группа полей «Необходимо добавить в отчет»	<p>Содержит кнопки для выбора дополнительных данных, которые должны быть отражены в отчете:</p> <ul style="list-style-type: none"> — «Адрес пользователя» – адрес указанного пользователя; — «Интерфейс устройства» – интерфейс устройства; — «Обновление сеанса» – обновление сеанса; — «Интервал обновления» – интервал обновления; — «Завершение сеанса» – завершение сеанса; — «Продолжительность сеанса» – продолжительность сеанса в секундах; — «Идентификатор сеанса» – порядковый номер, присвоенный сеансу работы с устройством в начале его выполнения; — «Уникальный идентификатор сеанса» – уникальный идентификатор сеанса; — «Область» – область; — «Входящий трафик» – входящий трафик; — «Исходящий трафик» – исходящий трафик; — «Сервер» – сервер; — «Клиент» – клиент; — «Причина отключения» – причина отключения; — «Тип службы» – тип службы; — «Тип пакетного протокола» – тип пакетного протокола; — «Адрес пользователя IPv6» – адрес пользователя IPv6; — «Префикс IPv6» – префикс IPv6; — «Делегированный префикс IPv6» – делегированный префикс IPv6; — «Идентификатор интерфейса IPv6» – идентификатор интерфейса IPv6
Переключатель «Периодичный отчет» и группа полей задания периодичности формирования отчетов	см. выше в таблице 43 описание полей процесса «Аутентификация» для типа журнала «TACACS+»

Таблица 45 – Состав и описание дополнительных полей страницы создания шаблона для типа журнала «Система»

Столбец	Описание
Тип журнала	«Система». Типы события «Все», «Ошибка», «Инфо», «предупреждение»
Группа полей «Дополнительные настройки»	
Вид отчета, Дата фиксации события	Поле «Вид отчета» содержит кнопки «Динамический», «Статический» для выбора требуемого вида отчета. Правила заполнения полей см. выше в таблице 43 для процесса «Аутентификация» для типа журнала «TACACS+»
Источник событий	Поле со списком для выбора подсистемы ПК «Efros ACS», по результатам работы которой зафиксированы включаемые в отчет события
Администратор	Поле со списком для выбора логина администратора, действия которого привели к фиксированию включаемых в отчет событий (если требуются системные события, то необходимо выбрать текст «System»)
Группа полей «Необходимо добавить в отчет»	Содержит кнопку «Сообщение» для добавления в отчет поясняющего событие текста из журнала событий
Переключатель «Периодичный отчет» и группа полей задания периодичности формирования отчетов	см. выше в таблице 43 описание полей процесса «Аутентификация» для типа журнала «TACACS+»

Будет запущен процесс проверки уникальности добавляемого шаблона отчетов по названию и заполненности всех обязательных полей.

При обнаружении незаполненных обязательных полей рядом с первым из таких полей отобразится всплывающая подсказка «Обязательное поле», в случае обнаружения в списке дубликата шаблона в верхней части страницы отобразится соответствующее сообщение. Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Добавить».

Если проверки завершились без обнаружения ошибок, то созданный шаблон будет добавлен в список шаблонов отчетов. В журнал событий ПК «Efros ACS» будет внесено соответствующее сообщение.

Если добавлен шаблон неперіодического отчета, то пользователь сможет сформировать по шаблону отчет, нажав в соответствующей строке таблицы шаблонов кнопку «Сформировать отчет» (▶). Периодические отчеты будут формироваться по созданному шаблону в соответствии с заданным в шаблоне расписанием.

3.12.1.2. Редактирование шаблона отчетов

Редактирование шаблонов отчетов выполняется администраторами ACS и администраторами RO. При редактировании для внесения изменений не доступны название и описание шаблона, а также поля группы «Основные настройки» (выбор типа журнала, процесса или события), остальные поля доступны для изменения, в том числе пользователь имеет возможность изменить тип отчета (периодический, неперіодический) и для неперіодических отчетов изменить вид отчета (динамический или статический).

Для редактирования администратору ACS необходимо выбрать в списке с помощью «мыши» название требуемого шаблона либо нажать в строке кнопку «Изменить» (✎). Откроется страница редактирования, которая содержит внесенные ранее данные. Состав элементов страницы и правила заполнения полей страницы аналогичны составу страницы добавления и правилам добавления шаблона отчетов (см. п.п. 3.12.1.1). Далее пользователю необходимо внести требуемые изменения и нажать кнопку «Сохранить».

При обнаружении незаполненных обязательных полей рядом с первым из таких полей отобразится всплывающая подсказка «Обязательное поле», а также в случае обнаружения в списке дубликата шаблона в верхней части страницы отобразится соответствующее сообщение. Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Сохранить».

Если проверки завершились без обнаружения ошибок, то внесенные изменения будут сохранены. В журнал событий ПК «Efros ACS» будет внесено соответствующее сообщение.

3.12.2. Список сформированных отчетов

Для просмотра сформированных отчетов пользователю необходимо перейти на странице «Отчеты» (см. рис. 146) на вкладку «Результаты» (рис. 148). Вкладка содержит список всех отчетов, сформированных по шаблонам отчетов на основе данных из журналов событий ПК «Efros ACS». Отчеты доступны для экспорта в файл формата CSV, XLSX или PDF, вывода на печать и удаления.

Для каждого отчета отображаются данные:

- дата и время формирования;
- название отчета;
- тип журнала событий ПК «Efros ACS», на основе данных из которого отчет сформирован;
- тип процесса/события – вкладка журнала событий ПК «Efros ACS»;
- описание (из шаблона отчета).

<input type="checkbox"/>	Дата и время ↓	Название	Тип журнала	Тип процесса/события	Описание	
<input type="checkbox"/>	4 апреля, 23:59	Отчет №6, 18.03.2021	Система	Аутентификация		📄 🖨️ 🗑️
<input type="checkbox"/>	4 апреля, 23:00	Отчет №7, 19.03.2021	TACACS+	Авторизация		📄 🖨️ 🗑️
<input type="checkbox"/>	4 апреля, 22:00	Отчет №7, 19.03.2021	TACACS+	Авторизация		📄 🖨️ 🗑️
<input type="checkbox"/>	4 апреля, 21:00	Отчет №7, 19.03.2021	TACACS+	Авторизация		📄 🖨️ 🗑️
<input type="checkbox"/>	4 апреля, 20:00	Отчет №7, 19.03.2021	TACACS+	Авторизация		📄 🖨️ 🗑️
<input type="checkbox"/>	4 апреля, 19:00	Отчет №7, 19.03.2021	TACACS+	Авторизация		📄 🖨️ 🗑️
<input type="checkbox"/>	4 апреля, 18:00	Отчет №7, 19.03.2021	TACACS+	Авторизация		📄 🖨️ 🗑️
<input type="checkbox"/>	4 апреля, 17:00	Отчет №7, 19.03.2021	TACACS+	Авторизация		📄 🖨️ 🗑️
<input type="checkbox"/>	4 апреля, 16:00	Отчет №7, 19.03.2021	TACACS+	Авторизация		📄 🖨️ 🗑️

Всего отчетов: 156 Строк на странице: 50 1-50 из 156 < 1 2 ... 4 >

Рисунок 150 – Рисунок 148 – Страница «Отчеты». Вкладка «Результаты»

В таблице доступны следующие кнопки:

- «Экспортировать» (📄) – для экспорта данных отчета в файл формата CSV, XLSX или PDF;
- «Распечатать» (🖨️) – для вывода отчета на печать;
- «Удалить» (🗑️) – для удаления отчета.

Сортировка данных в таблице отчетов по умолчанию производится по убыванию значений в столбце «Название». Пользователь имеет возможность задать другой тип сортировки, выбрав заголовок требуемого столбца таблицы. В заголовке отобразится знак «↓», сортировка всех строк таблицы будет выполнена по убыванию значений

выбранного столбца. Для изменения направления сортировки необходимо повторно выбрать заголовок столбца. В заголовке отобразится знак «↑».

Для поиска в таблице требуемых записей необходимо ввести в поле поиска последовательность символов из данных искомой записи списка и нажать клавишу клавиатуры ENTER.

Для экспорта отчета в файл и просмотра отчета пользователю необходимо:

- нажать в строке требуемого отчета кнопку «Экспортировать» (↓);
- в открывшемся окне «Экспорт отчета» (рис. 149) ввести название файла (если поле «Название» не заполнить, то файлу будет присвоено название отчета), выбрать формат файла и нажать кнопку «Экспортировать»;
- выбрать в открывшемся стандартном окне (рис. 150) выполняемое с файлом действие (просмотреть, сохранить).

Для вывода отчета на печать пользователю необходимо нажать в строке требуемого отчета кнопку «Распечатать» (🖨️), задать в открывшемся стандартном окне настройки печати (выбрать принтер, параметры печати) и нажать кнопку «Печать».

Экспорт отчета

Название

Тип файла

CSV XLSX PDF

Экспортировать Отменить

Рисунок 151 – Рисунок 149 – Окно «Экспорт отчета»



Рисунок 152 – Рисунок 150 – Окно выбора действия с файлом

3.13 Завершение работы ПК «Efros ACS»

Для завершения работы ПК «Efros ACS» необходимо в заголовке текущей страницы ПК «Efros ACS» нажать кнопку «Выход» и закрыть вкладку используемого веб-браузера.

4 Сообщения пользователю

4.1 При запуске ПК «Efros ACS»

При выполнении запуска ПК «Efros ACS», при обнаружении ошибки, могут быть выведены следующие сообщения:

- «Логин или пароль не могут быть пустыми» – в случае, если в паре логин /пароль не задано хотя бы одно значение;
- «Неверный логин или пароль» – в случае, если введена неправильная пара логин /пароль;
- «Доступ запрещен, нет прав на авторизацию в приложении» – в случае, если пользователь внесен в список пользователей ПК «Efros ACS», но для него в учетной карточке установлен статус «Не активен»;
- «Не найден администратор с логином {логин_администратора}» – в случае, если в списке пользователей ПК «Efros ACS» не найдена учетная запись с указанным логином.

В первых двух случаях пользователю необходимо ввести корректные данные и повторить попытку запуска, в других случаях – необходимо обратиться к системному администратору ПК «Efros ACS».

Кроме того, после нескольких подряд неуспешных попыток запуска ПК «Efros ACS» учетная запись пользователя автоматически блокируется на заданный в подразделе «Общие настройки» ПК «Efros ACS» (см. п. 3.4.7) период времени. На странице выводится сообщение: «Администратор '{имя_пользователя}' заблокирован из-за превышения количества попыток ввода пароля на {количество_минут} мин».

Примечание. Количество неуспешных попыток запуска ПК «Efros ACS» также настраивается в подразделе «Общие настройки» ПК «Efros ACS» (см. п. 3.4.7).

Пользователь может повторить попытку запуска через указанный в сообщении период времени либо обратиться к администратору ACS для уточнения своих данных (логина и пароля) и разблокирования учетной записи.

4.2 При выполнении функции по фильтрации данных журнала событий

Если при заполнении в окне фильтрации данных журнала событий полей даты и времени интервала, за который должен быть сформирован отчет, начальное значение интервала превышает конечное значение, то поле ввода начального значения будет выделено красной линией, под линией отобразится соответствующее сообщение.

При этом пользователю необходимо выбрать корректные данные и продолжить действия по формированию отчета.

4.3 Перечень возможных сообщений пользователю при создании/редактировании записей списков ПК «Efros ACS»

Если при заполнении полей страниц создания/редактирования записей списков ПК «Efros ACS» не было заполнено хотя бы одно из обязательных полей или поле заполнено некорректно, то это поле будет выделено красной линией, под линией отобразится соответствующее сообщение. В этом случае пользователю необходимо заполнить поле корректно и продолжить работу с записью.

При попытке создать в списке ПК «Efros ACS» дубликат уже имеющейся записи в верхней части страницы добавления отобразится соответствующее сообщение. Пользователю необходимо корректно заполнить поля страницы и повторно нажать кнопку «ДОБАВИТЬ». Параметры записей, по которым не допускается наличие дубликатов в списках ПК «Efros ACS», приведены в таблице 46.

Таблица 46 – Параметры записей, по которым не допускается наличие дубликатов в списках ПК «Efros ACS»

Список ПК «Efros ACS»	Параметр записи
Пользователи	Логин пользователя/администратора
Группы пользователей	Наименование группы пользователей
Сетевое оборудование	Название и IP-адрес АСО
Конечная точка сети	Название и MAC-адрес КО
Группы устройств	Наименование группы АСО или КО
Политика доступа	Наименование политики доступа

Перечень сокращений

AD DS	—	Active Directory Services
LDAP	—	Lightweight Directory Access Protocol
RADIUS	—	Remote Authentication in Dial-In User Service
TACACS+	—	Terminal Access Controller Access Control System plus
АСО	—	Активное сетевое оборудование
БД	—	База данных
КО	—	Клиентское оборудование
ОС	—	Операционная система
ПК	—	Программный комплекс
СУБД	—	Система управления базами данных
ЭВМ	—	Электронно-вычислительная машина