

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

Описание применения

Аннотация

Данный документ представляет собой описание применения для программного комплекса централизованного управления контролем доступа к сетевым устройствам ПК «Efros ACS» (далее – ПК «Efros ACS»). Документ содержит сведения о назначении ПК «Efros ACS», области его применения, применяемых методах, классе решаемых задач, ограничениях для применения, минимальной конфигурации технических средств.

Степени важности примечаний:



Важная информация
Указания, требующие особого внимания.



Дополнительная информация
Указания, позволяющие упростить работу с программным комплексом.

Содержание

1.	Назначение	5
1.1.	Назначение программы	5
1.2.	Структура ПК «Efros ACS»	5
1.3.	Функциональные возможности программы	5
1.4.	Роли и аутентификация пользователей	8
2.	Условия применения	10
3.	Описание задачи	12
3.1.	Управление доступом на сетевых устройствах, поддерживающие на клиентском уровне протоколы TACACS+ и/или RADIUS	13
3.2.	Централизованное управление учетными данными и настройками ПК «Efros ACS»	13
3.3.	Поддержка двухуровневой иерархии серверов	13
3.4.	Управление отказоустойчивостью	14
3.5.	Поддержка служб каталогов для аутентификации пользователей (FreeIPA и AD DS)	14
3.6.	Множественный ввод комплекса в домен	15
3.7.	Ведение журнала системных событий	15
3.8.	Создание шаблонов отчетов, формирование отчетов на основе данных из системных журналов событий	15
3.9.	Авторизация сетевых устройств (Endpoints) по MAC-адресам	16
3.10.	Авторизация устройств с использованием расширяемого протокола аутентификации EAP	16
3.11.	Гибкая конфигурация службы выполнения команд на АСО	16
3.12.	Регистрация фактов доступа к АСО	17
3.13.	Поддержка ролевой модели администраторов комплекса	17
3.14.	Объединение в группы учетных записей пользователей АСО	17
3.15.	Объединение в группы сетевых устройств	18
3.16.	Экспорт журналов событий в ПК «Ankey SIEM»	18
3.17.	Экспорт журналов в файловую систему в виде CSV или XLSX	18
3.18.	Получение списка сетевых устройств из ПК «Efros CI»	18
3.19.	Импорт пользователей АСО и списка сетевых устройств из ПО «Cisco ACS»	19

3.20. Контроль состояния комплекса и работоспособности основных служб	19
4. Входные и выходные данные	20
4.1. Входные данные	20
4.1.1. Настройки работы протоколов	20
4.1.2. Данные учетных записей пользователей	20
4.1.3. Данные учетных записей АСО	22
4.1.4. Данные записей клиентского оборудования	22
4.1.5. Настройки подключения для интеграции с ПК «Ankey SIEM»	23
4.1.6. Настройки подключения для интеграции с ПК «Efros CI»	23
4.1.7. Настройки подключения для интеграции с доменной службой AD	24
4.1.8. Настройка подключения для интеграции со службами каталогов данных по протоколу LDAP	25
4.1.9. Файлы экспорта из ПК «Cisco ACS»	26
4.1.10. Данные SSL-сертификатов	26
4.1.11. Настройки подключения объектов доступа по EAP	27
4.2. Выходные данные:	28
4.2.1. Файлы запроса на сертификаты	28
4.2.2. Файлы журналов событий	28
Перечень сокращений	29

1. Назначение

1.1. Назначение программы

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 (далее - 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. Структура ПК «Efros ACS»

ПК «Efros ACS» является высокопроизводительным и гибко-настраиваемым сервером контроля доступа и представляет собой единую серверную платформу с возможностью конфигурирования параметров при помощи веб-интерфейса.

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.

1.3. Функциональные возможности программы

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 подчиненными серверами);
- управление отказоустойчивостью;
- поддержка служб каталогов для аутентификации пользователей (FreeIPA и AD DS);
- поддержка множественного ввода комплекса в домен;
- ведение журнала системных событий;

- создание шаблонов отчетов, формирование отчетов на основе данных из системных журналов событий;
- авторизация сетевых устройств (Endpoints) по MAC-адресам;
- авторизация устройств с помощью расширяемого протокола аутентификации EAP;
- гибкая конфигурация службы выполнения команд на активном сетевом оборудовании (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»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 «Efros ACS».
- 5) Управление экспортом и импортом данных.

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

Управление настройками ПК «Efros ACS» включает:

- ведение списка корневых и серверных сертификатов, создание запросов на сертификаты;
- 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;
- настройку подключения к внешним источникам данных (серверам LDAP, AD DS);
- настройку подчиненных серверов;
- настройку отказоустойчивости (создание кластеров);
- настройку парольной политики;
- активацию/сброс лицензии.

Подробное описание операций, выполняемых администраторами при настройке параметров работы ПК «Efros ACS» с использованием веб-интерфейса ПК «Efros ACS», приведено в документе «Программный комплекс централизованного управления контролем доступа к сетевым устройствам «Efros ACS». Руководство пользователя».

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 (далее - 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.

1.4. 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 и REST-интерфейсу 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;
- инициализация клиентских сертификатов – с правом доступа только к странице инициализации клиентских сертификатов сетевых пользователей ПК «Efros ACS».

Для разделения доступа администраторов программного комплекса 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 перечислении 1 данных (без возможности внесения изменений).
 - 3) «CER 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).

 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 применения

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 поддерживает 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.

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 AD DS), не доступны функциональные возможности управления подчиненными серверами, формирования отчетов (раздел «Отчеты») и выпуска клиентских сертификатов (в разделе «Сертификаты» подраздел «Клиентские», отсутствует роль «CER Администратор» (см. п. 1.4)).

3. Описание задачи

ПК «Efros ACS» решает следующие задачи:

- 1) Управление доступом к сетевым устройствам, поддерживающим на клиентском уровне протоколы TACACS+ и (или) RADIUS.
- 2) Централизованное управление учетными данными и настройками ПК «Efros ACS».
- 3) Поддержка двухуровневой иерархии серверов.
- 4) Управление отказоустойчивостью.
- 5) Поддержка служб каталогов для аутентификации пользователей (FreeIPA и AD DS).
- 6) Множественный ввод в домен комплекса.
- 7) Ведение журнала системных событий.
- 8) Создание шаблонов отчетов, формирование отчетов на основе данных из системных журналов событий.
- 9) Авторизация сетевых устройств (Endpoints) по MAC-адресам.
- 10) Авторизация устройств с использованием расширяемого протокола аутентификации EAP.
- 11) Гибкая конфигурация службы выполнения команд на АСО.
- 12) Регистрация фактов доступа к АСО.
- 13) Поддержка ролевой модели администраторов комплекса.
- 14) Объединение в группы учетных записей пользователей АСО.
- 15) Объединение в группы сетевых устройств.
- 16) Экспорт журналов событий в ПК «Ankey SIEM».
- 17) Экспорт журналов в файловую систему в виде CSV или XLSX.
- 18) Получение списка сетевых устройств из ПК «Efros CI».
- 19) Импорт пользователей АСО и списка сетевых устройств из ПО «Cisco ACS».
- 20) Контроль состояния комплекса и работоспособности основных служб.

3.1. Управление доступом на сетевых устройствах, поддерживающие на клиентском уровне протоколы TACACS+ и/или RADIUS

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

Управление доступом к сетевым устройствам обеспечивается 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 секретной последовательности;
- созданием правила доступа путем сопоставления пользователю сетевого устройства.

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

3.2. Централизованное управление учетными данными и настройками ПК «Efros ACS»

В ПК «Efros ACS» реализована возможность централизованного управления посредством единого веб-интерфейса. Консоль позволяет производить следующие действия:

- 1) Управление настройками ПК «Efros ACS».
- 2) Управление администраторами.
- 3) Управление пользователями.
- 4) Управление группами пользователей.
- 5) Управление сетевым оборудованием.
- 6) Управление группами сетевого оборудования.
- 7) Управление установкой правил доступа к сетевому оборудованию.
- 8) Управление экспортом и импортом данных.

Управление доступно администратору с ролью «Администратор ACS».

3.3. Поддержка двухуровневой иерархии серверов

В ПК «Efros ACS» с лицензией Premium доступна функция ведения списка серверов, подчиненных главному серверу. Главный сервер может быть только один.

Раздел «Настройки системы» главного сервера (первого уровня) содержит раздел «Управление подчиненными серверами» со списком подчиненных серверов (второго уровня). Поддерживается до 7 подчиненных серверов.

Администраторы ACS имеют возможность ведения списка подчиненных серверов (добавление/удаление/редактирование). Для каждого подчиненного сервера отдельно формируется список пользователей, имеющих к нему доступ. При этом каждому пользователю отдельно назначаются права доступа к подчиненному серверу: полный доступ (администратор ACS) или только просмотр (администратор RO). Так пользователь, имеющий права администратора RO на главном сервере, может иметь полные права администратора ACS на подчиненном сервере.

В панели главного меню веб-приложения ПК «Efros ACS» расположено поле выбора настраиваемого в текущий момент времени сервера. При переходе на подчиненный сервер управляющие элементы меню и страниц ПК «Efros ACS» доступны или не доступны в зависимости от прав пользователя на соответствующем сервере.

3.4. Управление отказоустойчивостью

В ПК «Efros ACS» с лицензией Premium доступна функция управления отказоустойчивостью.

Администраторы ACS имеют возможность создавать/удалять кластеры для повышения отказоустойчивости в работе ПК «Efros ACS». При возникновении ошибки в работе и сбое какой-либо службы или всего сервера, все службы ПК «Efros ACS» (а также подключения к домену, если они были) перемещаются на другой узел, находившийся в «спящем» режиме, и продолжают работу до восстановления работоспособности вышедшего из строя узла, кластер при этом переводится в состояние «FAILED». При восстановлении работоспособности узла происходит согласование узлов кластера, службы ПК «Efros ACS» и кластер продолжают работать в штатном режиме.

3.5. Поддержка служб каталогов для аутентификации пользователей (FreeIPA и AD DS)

Функция создания учетных записей на основе доменной службы включает:

- 1) Настройку подключения к AD DS/FreeIPA.
- 2) Загрузку учетных записей из доменной службы в локальную БД для ускорения конфигурации.
- 3) Проверку корректности соединения.

На основе учетных записей из доменной службы создаются учетные записи локальных пользователей. Таким образом, пользователь, заведенный в домене, может иметь доступ на АСО.

Аналогичным образом реализована поддержка доменных групп пользователей, в результате целая группа может быть сконфигурирована для доступа на АСО. Актуальность доменных записей в БД ПК «Efros ACS» поддерживается периодической проверкой их состояний во внешней системе AD в соответствии с заданным параметром настройки «Частота обновления».

3.6. Множественный ввод комплекса в домен

В ПК «Efros ACS» с лицензией Premium доступна функция множественного ввода комплекса в домен. При лицензии Standard домен может быть только один.

Страница «Настройки системы» главного сервера (первого уровня) содержит подраздел «Внешние источники данными», необходимо выбрать вкладку «Active Directory» и выполнить настройку подключения.

Администраторы ACS имеют возможность ведения списка подключений к домену. При наличии лицензии Premium создание новых подключений к доменам не ограничено.

3.7. Ведение журнала системных событий

ПК «Efros ACS» содержит журнал событий, который хранит аудит действий администраторов ПК и сообщения о работе модулей ПК:

- 1) В журнале «Система» реализована регистрация активности администраторов ПК: авторизация, создание сущностей, удаление и т.д. Журнал представлен в едином списке, поддерживающем разделение по типу важности сообщения: «Инфо», «Предупреждение», «Ошибка».
- 2) В журнале событий «TACACS+», «RADIUS» производится регистрация фактов доступа пользователей к активному сетевому оборудованию.

Для каждого вида журнала доступна сортировка, поиск и фильтрация, а также функция экспорта. Журнал доступен администраторам ПК «Efros ACS».

3.8. Создание шаблонов отчетов, формирование отчетов на основе данных из системных журналов событий

В ПК «Efros ACS» реализована возможность создания шаблонов отчетов, формирования на их основе неперiodических и периодических отчетов.

Отчеты формируются путем выборки событий системных журналов событий по заданным в шаблоне параметрам.

Шаблоны и сформированные на их основе отчеты хранятся в разных списках ПК «Efros ACS» и доступны администраторам ACS и RO.

3.9. Авторизация сетевых устройств (Endpoints) по MAC-адресам

В ПК «Efros ACS» реализована возможность авторизации сетевых устройств (Endpoints) по MAC-адресам. Возможность обеспечивается добавлением сетевого устройства в список «Конечные точки сети» ПК «Efros ACS» с указанием его MAC-адреса и статуса устройства – «Активен».

3.10. Авторизация устройств с использованием расширяемого протокола аутентификации EAP

В ПК «Efros ACS» реализована возможность авторизации сетевых устройств по протоколу EAP – по учетной записи устройства во внешней системе: через LDAP, один из контроллеров домена, через сетевых пользователей. Возможность обеспечивается следующими функциями ПК «Efros ACS»:

- 1) Ведение списка корневых и серверных сертификатов, создание запросов на сертификаты.
- 2) Ведение списка шаблонов клиентских сертификатов.
- 3) Ведение списка клиентских сертификатов, создаваемых на основе созданных ранее в ПК «Efros ACS» шаблонов.
- 4) Настройка доступа ПК «Efros ACS» в сеть: настройка параметров доступа, включение/отключение доступа, выбор серверного сертификата.
- 5) Настройка подключения к внешним источникам данных: ввод данных сервера аутентификации, к которому выполняется подключение, проверка статуса подключения.

3.11. Гибкая конфигурация службы выполнения команд на АСО

Гибкая конфигурация службы выполнения команд на АСО в ПК «Efros ACS» обеспечивается следующими функциями:

- 1) Ведение списка настроенных политик доступа пользователей к контролируемым устройствам с возможностью формирования списка разрешенных и запрещенных для выполнения команд с заданными аргументами.
- 2) Назначение прав доступа пользователей и групп пользователей к АСО и группам АСО.
- 3) Настройка службы выполнения команд для отдельных пользователей и групп пользователей с возможностью:
 - включения/отключения и выбора пароля (при включении) привилегированного режима для управления устройством;

- разрешение/запрет выполнения команд по умолчанию на устройстве;
- выбора набора команд, разрешенных или запрещенных пользователю для выполнения на АСО.

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

3.12. Регистрация фактов доступа к АСО

Регистрация фактов доступа к активному сетевому оборудованию производится с помощью сервера управления доступом. Фиксирование записей о фактах доступа производится в журнале событий «TACACS+», «RADIUS».

3.13. Поддержка ролевой модели администраторов комплекса

Для администратора ПК «Efros ACS» можно установить одну из ролей:

- 1) «Администратор RO» – администратор имеет права на доступ в ПК «Efros ACS» и чтение данных. Для поля «Роль администратора» задается роль «Только на чтение».
- 2) «Администратор ACS» – администратор обладает полным доступом к ПК «Efros ACS». Для поля «Роль администратора» задается роль «Полный доступ».
- 3) «Администратор CER» – 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 получения доступа к ПК «Efros ACS» в соответствии с выбранной ролью, при создании администратора атрибут «Статус пользователя» должен быть установлен в значение «Активен».

3.14. Объединение в группы учетных записей пользователей АСО

В ПК «Efros ACS» поддерживается функция объединения в группы учетных записей пользователей АСО. Объединение производится выбором в состав группы учетных записей в момент создания или редактирования группы пользователей. Для созданной группы пользователей возможна конфигурация доступа группы к АСО.

3.15. Объединение в группы сетевых устройств

В ПК «Efros ACS» поддерживается функция, позволяющая произвести следующие операции:

- 1) Создание группы сетевых устройств.
- 2) Сопоставление пользователю или группе пользователей группы сетевых устройств.

Операцию сопоставления возможно произвести в момент создания или редактирования пользователя, или группы пользователей.

3.16. Экспорт журналов событий в ПК «Ankey SIEM»

В ПК «Efros ACS» реализованы следующие журналы событий, доступные для выгрузки в ПК «Ankey SIEM»:

- 1) «TACACS+. Аутентификация, авторизация, отчетность».
- 2) «RADIUS. Аутентификация, отчетность».
- 3) «Система. Все, ошибки, предупреждения, инфо».

Выгрузка журналов событий в ПК «Ankey SIEM» реализована как функция интеграции данных между программными комплексами. Функция включает настройку подключения к ПК «Efros ACS» и учетной записи, под которой будет производиться выгрузка данных. Формат передачи данных определен разработчиками ПК «Ankey SIEM» и поддерживается ПК «Efros ACS».

3.17. Экспорт журналов в файловую систему в виде CSV или XLSX

В ПК «Efros ACS» реализована возможность выгрузки в файлы формата CSV и XLSX журнала системных событий и журналов событий, зафиксированных ПК «Efros ACS» по протоколам TACACS+ и RADIUS. Выгрузка осуществляется администраторами ПК «Efros ACS». При выгрузке предоставляется возможность настройки выгружаемых данных средствами журнала: поиск и фильтрация данных.

3.18. Получение списка сетевых устройств из ПК «Efros CI»

В ПК «Efros ACS» реализован импорт АСО из ПК «Efros CI». Данные включают в себя наименование, IP-адрес устройства и т.д.

Функция включает настройку правил подключения к ПК «Efros CI», проверку корректности соединения и импорта списка устройств.

3.19. Импорт пользователей АСО и списка сетевых устройств из ПО «Cisco ACS»

В ПК «Efros ACS» получение списка сетевых устройств из ПО «Cisco ACS» реализовано как функция импорта файлов данных. Формат файлов передачи данных определен разработчиками ПО «Cisco ACS» и реализован в двух видах:

- 1) Файл экспорта со списком пользователей.
- 2) Файл экспорта со списком сетевых устройств.

Функция импорта позволяет произвести выбор данных для загрузки в ПК «Efros ACS» из загруженного списка экспорта ПО «Cisco ACS».

3.20. Контроль состояния комплекса и работоспособности основных служб

Контроль текущего состояния комплекса и служб протоколов реализован как набор основных параметров, отображаемых в веб-интерфейсе:

- 1) «Общая информация» – содержит визуализированные данные о состоянии системы, о системе, о базе данных.
- 2) «Пользователи и устройства» – содержит визуализированные данные о пользователях, устройствах и группах.
- 3) «Состояние служб и модулей» – содержит данные о статусе служб и модулей.
- 4) «Журнал аварийных сигналов» – содержит данные за текущие сутки о наличии аварийных сигналов ПК «Efros ACS».

4. Входные и выходные данные

4.1. Входные данные

Входные данные вводятся в поля страниц веб-интерфейса или через запросы REST-интерфейса ПК «Efros ACS».

Состав и описание входных данных зависят от выполняемых функций ПК «Efros ACS».

4.1.1. Настройки работы протоколов

Описание параметров, вводимых для настройки работы ПК «Efros ACS» с сервисами протоколов TACACS+ и RADIUS, приведены в таблице 2.

Таблица 2 – Параметры настройки протоколов

Параметр	Описание
Для протокола «TACACS+»	
Используемый порт	Числовой параметр – номер порта сервера ПК «Efros ACS» для протокола TACACS+. По умолчанию – 49
Количество серверных процессов	Два числовых параметра – минимальное и максимальное количество процессов для службы TACACS+. По умолчанию – 1 и 10
Для протокола «RADIUS»	
Прослушивание пакетов аутентификации	Два параметра: <ul style="list-style-type: none">– IP-адрес прослушиваемых серверов;– номер порта прослушивания пакетов аутентификации. По умолчанию прослушиваются все сервера в сети (задано значение «*») и порт прослушивания - 1812
Прослушивание пакетов учета	Два параметра: <ul style="list-style-type: none">– IP-адрес прослушиваемых серверов;– номер порта прослушивания пакетов учета. По умолчанию прослушиваются все сервера в сети (задано значение «*») и порт прослушивания - 1813

4.1.2. Данные учетных записей пользователей

Описание параметров, используемых при работе с учетными записями пользователей ПК «Efros ACS» (сетового пользователя и администратора), приведены в таблице 3.

Таблица 3 – Состав и описание параметров пользователя ПК «Efros ACS»

Параметр	Описание
Тип пользователя	Одно значение из списка (тип добавляемого пользователя): «Пользователь» или «Администратор»
Логин	Текстовый параметр (до 50 символов) Если пользователь является: <ul style="list-style-type: none">– локальным пользователем ПК «Efros ACS», то параметр задается путем ввода логина вручную;– пользователем из внешней системы (LDAP), то параметр задается путем выбора логина из списка пользователей LDAP

Параметр	Описание
Пароль	Текстовый параметр. Задается в ПК «Efros ACS» только для локальных пользователей. Пароль должен соответствовать требованиям, заданным при настройке парольной политики ПК «Efros ACS»
Описание	Текстовый параметр (до 250 символов). Если пользователь является: – локальным пользователем ПК «Efros ACS», то параметр задается путем ввода текста описания вручную; – пользователем из внешней системы (LDAP), то параметр задается автоматически после выбора логина пользователя
Роль администратора	Параметр устанавливается только для администратора. Одно из значений переключателя: – «Полный доступ» – администратору назначается роль «ACS Администратор»; – «Только просмотр» – администратору назначается роль «RO Администратор»; – «Выпуск сертификатов» – администратору назначается роль «CER Администратор»
Статус пользователя	Одно из значений переключателя: – «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»
Список доступных устройств	Параметр устанавливается только для пользователя. Список формируется путем множественного выбора из списка устройств ПК «Efros ACS»
Список групп, в которые пользователь входит	Параметр устанавливается только для пользователя. Список формируется путем множественного выбора из списка групп пользователей ПК «Efros ACS»

Описание параметров, используемых для настройки службы выполнения команд для пользователя, приведены в таблице 4.

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

Таблица 4 – Состав и описание параметров настройки службы выполнения команд для пользователя ПК «Efros ACS»

Параметр	Описание
Привилегированный режим	Одно значение из списка для включения/отключения и выбора пароля (при включении) привилегированного режима для управления устройством. Список содержит значения: – «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

Параметр	Описание
Пароль	Текстовый параметр. Задается только после выбора для привилегированного режима значения «Задать пароль». Пароль должен соответствовать требованиям, заданным при настройке парольной политики ПК «Efros ACS»
Выполнение команд по умолчанию	Одно из значений переключателя: – «Выполнять» – пользователю разрешено выполнение команд по умолчанию на устройстве; – «Не выполнять» – пользователю запрещено выполнение команд по умолчанию на устройстве
Наборы команд	Список наборов команд (разрешенных и запрещенных) формируется путем множественного выбора из списка наборов команд ПК «Efros ACS»
Время доступа на устройстве	Задается только после активации данного поля. Содержит следующие поля: – «Начало» - время начала работы на устройстве, задается в формате ММ.ЧЧ. – «Конец» - время окончания работы на устройстве, задается в формате ММ.ЧЧ.

4.1.3. Данные учетных записей АСО

Описание параметров, используемых при работе с учетными записями АСО в ПК «Efros ACS», приведены в таблице 5.

Таблица 5 – Состав и описание параметров АСО в ПК «Efros ACS»

Параметр	Описание
Название	Текстовый параметр (до 50 символов)
Описание	Текстовый параметр (до 250 символов)
IP-адрес или список подсетей	Текстовый параметр (IP-адрес или диапазон IP-адресов устройства)
Профиль сетевого оборудования	Поле со списком для выбора профиля сетевого оборудования из перечня заранее заведенных в разделе «Профили оборудования»
Группы	Список формируется путем множественного выбора из списка групп АСО ПК «Efros ACS»
Тип протокола	Для каждого типа протокола «TACACS+» и «RADIUS» указывается: – одно из значений переключателя «Включен»/ «Выключен» (протокол используется/не используется); – текстовый параметр – значение разделяемого ключа (указывается только для используемого протокола)

4.1.4. Данные записей клиентского оборудования

Описание параметров, используемых при работе с учетными записями клиентского оборудования (КО), аутентифицирующегося в сети по MAC-адресу учетной записи в ПК «Efros ACS», приведены в таблице 6.

Таблица 6 – Состав и описание параметров КО в ПК «Efros ACS»

Параметр	Описание
Название	Текстовый параметр (до 50 символов)
Описание	Текстовый параметр (до 250 символов)
MAC-адрес	Текстовый параметр (MAC-адрес устройства)
Список групп КО	Список формируется путем множественного выбора из списка групп КО ПК «Efros ACS»
Статус конечной точки сети	Одно из значений переключателя: – «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»

4.1.5. Настройки подключения для интеграции с ПК «Ankey SIEM»

Описание параметров, вводимых для настройки работы ПК «Efros ACS» с ПК «Ankey SIEM», приведены в таблице 7.

Таблица 7 – Параметры настройки работы ПК «Efros ACS» с ПК «Ankey SIEM»

Параметр	Описание
Служба «Ankey SIEM»	Одно из значений переключателя: – «Включена» – подключение к ПК «Ankey SIEM» включено; – «Выключена» – подключение к ПК «Ankey SIEM» выключено
Логин	Текстовый параметр (до 50 символов). Имя пользователя, под которым выполняются запросы из ПК «Ankey SIEM»
Пароль	Текстовый параметр. Пароль пользователя, под которым выполняются запросы из ПК «Ankey SIEM»

4.1.6. Настройки подключения для интеграции с ПК «Efros CI»

Описание параметров, вводимых для настройки работы ПК «Efros ACS» с ПК «Efros CI», приведены в таблице 8.

Таблица 8 – Параметры настройки работы ПК «Efros ACS» с ПК «Efros CI»

Параметр	Описание
IP адрес или dns имя сервера	Текстовый параметр. dns-имя или IP-адрес домена установки ПК «Efros CI», с которым настраивается соединение
Порт	Числовой параметр. Номер порта сервера ПК «Efros ACS» для взаимодействия с ПО «Efros CI». По умолчанию – 20000
Логин	Текстовый параметр. Имя пользователя, под которым выполняется подключение к ПО «Efros CI»
Пароль	Текстовый параметр. Пароль пользователя, под которым выполняется подключение к ПО «Efros CI»

4.1.7. Настройки подключения для интеграции с доменной службой AD

Описание параметров, вводимых для настройки работы ПК «Efros ACS» с доменной службой AD, приведены в таблице 9.

Таблица 9 – Параметры настройки работы ПК «Efros ACS» с доменной службой AD

Параметр	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. По умолчанию содержит одну строку для ввода данных одного сервера. Для добавления новой строки в поле необходимо нажать кнопку «Добавить» (+)
Группа полей «Ввод в домен».	
Поля группы активны только после успешного создания подключения (после сохранения введенных выше параметров по нажатию кнопки «СОХРАНИТЬ» без появления сообщений об ошибках). Справа от заголовка группы отображается текущий статус ввода ПК «Efros ACS» в домен: «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»). По умолчанию в списке не выбрана ни одна группа

4.1.8. Настройка подключения для интеграции со службами каталогов данных по протоколу LDAP

Описание параметров, вводимых для настройки работы ПК «Efros ACS» с внешними каталогами данных, приведены в таблице 10.

Таблица 10 – Параметры настройки работы ПК «Efros ACS» с внешними каталогами данных

Параметр	Описание
Имя соединения	Имя нового соединения
Статус	Одно из значений переключателя: – «Вкл.» – подключение к каталогам включено; – «Выкл.» – подключение к каталогам выключено
Группа полей «Основные настройки»	
Тип источника	Содержит кнопки выбора типа подключаемого LDAP-сервера: – «Active Directory»; – «FreeIPA». По умолчанию выбран тип «Active Directory»
Домен	Текстовый параметр. Имя домена, где размещена служба каталогов, с которой настраивается соединение (до 50 символов)
IP-адрес	Текстовый параметр. IP-адрес домена, где размещена служба каталогов, с которой настраивается соединение (до 50 символов)
База пользователей	Поля для ввода фильтра запрашиваемых данных в БД LDAP-сервера (пользователей и групп пользователей). По умолчанию поля не заполнены и поиск данных выполняется в полной базе LDAP-сервера
База групп	
Использовать SSL	Одно из значений переключателя: – «Вкл.» – подключение к LDAP-серверу выполняется с использованием протокола SSL; – «Выкл.» – подключение к LDAP-серверу выполняется без использования протокола SSL
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.»
Частота обновления	Числовой параметр. Интервал запроса из ПК «Efros ACS» на обновление данных в AD (в часах). По умолчанию – 1 и с периодичностью в один час выполняется обновление данных
Группа полей «Авторизация»	
Логин	Текстовый параметр. Имя пользователя, под которым выполняется подключение к AD (до 50 символов). Допустимый формат, например, для пользователя с именем «acs», зарегистрированного на сервере TOR: – acs; – TOR\acs; – acs@tor.ru
Пароль	Текстовый параметр. Пароль пользователя, под которым выполняется подключение к AD
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

Параметр	Описание
	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»	

4.1.9. Файлы экспорта из ПК «Cisco ACS»

В ПК «Efros ACS» импорт пользователей АСО и списка сетевых устройств выполняется из файлов формата CSV размером до 50 Мб, сформированных в ПО «Cisco ACS».

4.1.10. Данные SSL-сертификатов

Корневые сертификаты добавляются в ПК «Efros ACS» путем импорта из файла формата .pem. При импорте указываются текстовые параметры корневого сертификата в ПК «Efros ACS»: название (до 50 символов) и описание (до 250 символов).

Серверные сертификаты добавляются в ПК «Efros ACS» либо автоматически после привязки к созданному ранее в ПК «Efros ACS» запросу сертификата, либо путем импорта уже имеющегося в организации серверного сертификата в БД ПК «Efros ACS» (аналогично импорту корневых сертификатов).

При привязке серверного сертификата выполняется импорт сертификата из файла формата .pem, при этом указывается название сертификата в ПК «Efros ACS» (до 50 символов), а также указывается тип использования сертификата:

- «WEB-консоль» – для установки доверенного соединения при доступе к веб-приложению ПК «Efros ACS».

При привязке или импорте серверного сертификата автоматически определяется соответствующий ему корневой сертификат.

Описание параметров, указываемых при создании запроса сертификата, приведены в таблице 11.

Таблица 11 – Состав и описание параметров запроса сертификата

Параметр	Описание
Название	Текстовый параметр (до 50 символов)
Данные субъекта	
Общее имя, Организация, Подразделение, Город, Область	Текстовые параметры (до 50 символов)







Параметр	Описание
Страна	Текстовый параметр (2 символа)
Альтернативное имя (SAN)	Список альтернативных имен. Каждому имени соответствует его тип: «DNS», «IP-адрес», «URL ресурса» или «Директория» и значение параметра

4.1.11. Настройки подключения объектов доступа по EAP

Настройки доступа в сеть подключенных к ПК «Efros ACS» устройств с использованием расширяемого протокола аутентификации EAP, приведены в таблице Таблица 12.

Таблица 12 – Параметры настройки доступа в сеть подключенных к ПК «Efros ACS» устройств с использованием расширяемого протокола аутентификации EAP

Параметр	Описание
Тип EAP	Выбор типа аутентификации EAP из выпадающего списка
Время ответа на EAP пакет	Числовой параметр. Время хранения данных аутентификатора между запросами и ответами на EAP-пакеты (в секундах). По истечении заданного интервала времени данные удаляются. Допустимые значения: от 1 до 600
Максимальное кол-во открытых сессий	Числовой параметр. Максимально допустимое количество одновременно открытых сессий обмена данными. Допустимые значения: от 1 до 4096
Настройки TLS	
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
Версия TLS	Выбор минимальной и максимальной версии TLS из списка
Кэширование	Переключатель с двумя положениями: <ul style="list-style-type: none"> – «Включен» (☑) – при восстановлении сеанса из кэша копируются атрибуты сеанса: ID сессии и имя пользователя; – «Выключен» (☐) – при восстановлении сеанса атрибуты из кэша не копируются. Время хранения атрибутов сессии настраивается в поле «Время жизни кэша» (см. ниже)
Время жизни кэша	Поле для ввода времени хранения атрибутов сессии: ID сессии и имя пользователя (в часах). Допустимые значения: от 1 до 100. Поле отображается и доступно для редактирования только, если включен переключатель «Кэширование» (см. выше)
Проверять список отзыва сертификатов	Переключатель с двумя положениями: <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

Параметр	Описание
OCSP	Переключатель с двумя положениями: <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	Переключатель с двумя положениями: <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	Поле для ввода URL-адреса ответчика OCSP, которым должен заменяться URL-адрес ответчика. Поле отображается и доступно для редактирования только, если включен переключатель «Подменять URL-адреса ответчика» (см. выше)
Время ожидания ответа	Поле для ввода времени ожидания ответа OCSP-ответчика (в секундах). Допустимые значения: от 0 до 100
Игнорировать ошибки	Переключатель с двумя положениями: <ul style="list-style-type: none">– «Включен» () – клиенты с отозванными сертификатами смогут подключиться при недоступном ответчике OCSP;– «Выключен» () – при недоступном ответчике OCSP клиенты с отозванными сертификатами не смогут подключиться

4.2. Выходные данные:

4.2.1. Файлы запроса на сертификаты

Запросы на сертификаты создаются в ПК «Efros ACS» в соответствии с п. 4.10.1. В результате формируется файл формата .pem, который может быть экспортирован на локальную ЭВМ администратора и далее направлен в ответственную организацию для выпуска по нему серверного сертификата.

4.2.2. Файлы журналов событий

Выгрузка журнала системных событий и журналов событий, зафиксированных ПК «Efros ACS» по протоколам TACACS+ и RADIUS осуществляется по запросу администратора в файлы формата CSV и XLSX. Перед выгрузкой администратор возможность настроить выгружаемых данные средствами журнала: поиск и фильтрация данных.

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
ОС	—	Операционная система
ПК	—	Программный комплекс
СУБД	—	Система управления базами данных
ЭВМ	—	Электронно-вычислительная машина