КОНТРОЛИРУЕМЫЙ ЗАЩИЩЁННЫЙ УДАЛЁННЫЙ ДОСТУП

Платформа управления информационной безопасностью "Эгида"

Руководство администратора

2024

Содержание

Обозначения и сокращения....4

1 Введение....5

1.1 Область применения....5

1.2 Краткое описание возможностей....5

1.3 Состав и квалификация персонала подсистемы....6

2 Общее описание подсистемы....7

2.1 Комплекс управления средствами оценки состояния....7

2.2 Комплекс оценки состояния....8

3 Установка и настройка программных средств подсистемы....9

4 Администрирование подсистемы....10

4.1.1 Модель администрирования....10

4.1.2 Периодические работы, выполняемые СА....10

4.1.3 Периодические работы, выполняемые АБИ....11

4.1.4 Непериодические работы, выполняемые СА....14

4.1.5 Непериодические работы, выполняемые АБИ....29

5 Работа с интерфейсом Системы....31

5.1 Модуль управления событиями ИБ....31

5.1.1 Роли пользователя....31

5.1.2 События....31

5.1.3 Сущность событие....32

5.1.4 Задачи....33

5.2 Оценка соответствия....34

Приложение А (обязательное) Установка серверной части приложения....35

А.1 Общие положения по установке СУБД и конфигурации БД.....35

А.2 Установка компонентов систем.....38

Установка и настройка компонента API.....38

Проверка статуса модуля путём выполнения следующей команды: systemctl status egida_ api.service.....40

5.2.1 Установка и настройка компонента ACMS.....41

- Запуск модуля путём выполнения следующей команды: systemctl start egida_acms.service.....42
- Проверка статуса модуля путём выполнения следующей команды: systemctl status egida_ acms.service.....42

5.2.2 Установка и настройка компонента Orchestratrion service.....43

c. Запуск модуля путём выполнения следующей команды: systemctl start egida_orchestration.service.....44

5.2.3 Конфигурация веб сервера для функционала API Gateway по маршрутизации запросов к компонентам системы (nginx).....45

5.2.4 Конфигурация веб сервера для предоставления файлов веб приложения (nginx).....47

Обозначения и сокращения

АБИ	–	Администратор безопасности информации
АРМ	–	Автоматизированное рабочее место
АС	–	Администратор системы
ИБ	–	Информационная безопасность
МЭ	–	Межсетевое экранирование
ОС	–	Операционная система
ПО	–	Программное обеспечение
ПЗУД	–	Подсистема защищённого удалённого доступа
ПОС	–	Подсистема оценки состояния
Платформа	--	Платформа управления информационной безопасностью "Эгида"
СА	–	Системный администратор
Система	-	Система управления Платформой
СУБД	–	Система управления базами данных
УРМ	–	Удаленное рабочее место
ACL	–	Access Control List
AD	–	Active Directory
DNS	–	Domain Name System
HTTPS	–	HyperText Transfer Protocol Secure
IP	–	Internet Protocol
VPN	–	Virtual Private Network

1 Введение

1.1 Область применения

Данное руководство предназначено для администраторов платформы управления информационной безопасностью "Эгида" (далее - Платформа).

Руководство содержит в себе перечень сведений и действий, необходимых для установки, настройки и эксплуатации комплексов Платформы.

Данный документ не заменяет собой официальной документации, поставляемой с программным обеспечением производителя, а также находящейся на официальном сайте компании производителя.

1.2 Краткое описание возможностей

Платформа предоставляет следующие возможности:

– проведение процедуры оценки состояния УРМ в соответствии с установленными требованиями корпоративной политики ИБ;

– выявление нарушений (несоответствий требованиям установленной корпоративной политики ИБ) на устройствах пользователей защищенного удаленного доступа (УРМ);

– предотвращение целевого доступа к ресурсам корпоративной сети в случае несоответствия устройств пользователей защищенного удаленного доступа (ПЗУД) требованиям установленной корпоративной политики ИБ;

– уведомление пользователей и администраторов о нарушениях, выявленных в рамках прохождения процедуры оценки состояния.

– управление событиями информационной безопасности

– архивирование событий ИБ

– ведение статистики ИБ

– предоставление отчетности

– проведение оценки соответствия узлов ИС в соответствии с установленным набором требований, в том числе с учетом требований регуляторов (ФСТЭК, ФСБ, РКН и т.д.) и различных стандартов (PCI, CIS и т.д)

– предоставляет информационную панель по событиям информационной безопасности

1.3 Состав и квалификация персонала

Квалификация и знания специалистов, ответственных за администрирование Платформы, должны быть достаточными для выполнения своих функций в рамках модели администрирования.

2 Общее описание

Платформа включает в свой состав следующие комплексы:

– комплекс управления средствами оценки состояния;

– комплекс оценки состояния;

– платформу управления событиями.

2.1 Комплекс управления средствами оценки состояния

Комплекс управления средствами оценки состояния предназначен для:

– предоставления возможности настройки проверок, выполняемых на УРМ в рамках процедуры оценки состояния оборудования пользователей УРМ;

– предоставления возможности просмотра статуса выполнения оценки состояния устройств в интерфейсе управления средств оценки состояния;

– предоставления возможности настройки правил МЭ на шлюзе удаленного доступа ПЗУД для ограничения/разрешения доступа к ресурсам корпоративной сети, пользователям, проходящим процедуру оценки состояния;

– предоставления возможности создания пользовательских скриптов, выполняемых на удаленных машинах пользователей, производящих процедуру оценки состояния;

– предоставления возможности назначения выполнения различного перечня проверок на разные устройства, группы устройств (распределение устройств по группам и назначение разного перечня проверок на каждую из групп).

– предоставления возможности просмотра информации о выявленных нарушениях на пользовательских устройствах в интерфейсе управления средств оценки состояния, включая:

- имя устройства;
- название проверки, которую не удалось успешной пройти;

- время, в которое было выявлено несоответствие;
- статус подключения УРМ (подключен/отключен);
- статус оценки состояния.

Комплекс управления средствами оценки состояния состоит из следующих компонентов:

– сервер управления ИнфоЗонт Эгида Аргус (далее – Сервер управления);

– сервер СУБД PostgreSQL (далее – Сервер СУБД).

2.2 **Комплекс оценки состояния**

Комплекс оценки состояния выполняет следующие функции:

– осуществление автоматизированной проверки соответствия фактической конфигурации УРМ целевой конфигурации установленным в политиках ИБ;

– принятие решений и управление доступом УРМ ко внутренней (доверенной) сети;

– предоставление возможности исправления конфигурации УРМ в автоматизированном режиме;

– ограничение доступа в инфраструктуру для УРМ, не соответствующих требованиям установленной политики ИБ

– регистрация событий, связанных с прохождением оценки соответствия УРМ.

Комплекс оценки состояния состоит из следующих компонентов:

– агент оценки состояния ИнфоЗонт Эгида Аргус (далее – Агент оценки состояния).

– оркестратор агентов ИнфоЗонт Эгида Аргус (далее – Оркестратор);

– агент управления конфигурациями ИнфоЗонт Эгида Аргус (далее – Агент управления конфигурациями);

– брокер ИнфоЗонт Эгида Аргус (далее – Брокер);

3 Установка и настройка программных средств

Установка и настройка программных средств Платформы осуществляется в следующем порядке:

1) Установка серверной части приложения:
2) Установка и настройка компонента API:
3) Установка и настройка компонента ACMS;
4) Установка и настройка компонента Orchestratrion service;
5) Конфигурация веб сервера для функционала API Gateway по маршрутизации запросов к компонентам системы (nginx);
6) Конфигурация веб сервера для предоставления файлов веб приложения (nginx).

Подробное описание установки и настройки программных средств Платформы приведено в приложении А.

4 Администрирование

4.1.1 Модель администрирования

Модель администрирования Платформы предполагает наличие двух выделенных ролей администраторов:

– Системный администратора (далее – СА);

– Администратор безопасности информации (далее – АБИ).

Работы, выполняемые при администрировании подсистемы, подразделяются на следующие:

– периодические работы;

– непериодические работы.

4.1.2 Периодические работы, выполняемые СА

Периодические работы по администрированию Платформы, выполняемые СА, приведены в таблице ниже (Таблица 4 .1).

Таблица 4.1 – Периодические работы по администрированию Платформы, выполняемые СА

№ п/п	Описание обязанностей	Периодичность	Пункт описания
1.	Проведение процедуры резервного копирования конфигурационных файлов оборудования	Еженедельно	4.1.2.1.1

4.1.2.1 Проведение процедуры резервного копирования конфигурационных файлов оборудования

Резервное копирование может осуществляться вручную, либо автоматизировано (с использованием специализированных скриптов).

Резервное копирование в ручном режиме осуществляется с помощью команды pg_dumpall:

```
postgress@root:/ pg_dumpall > pg_base.bak
```

Для экономии дискового пространства рекомендуется использовать сжатие полученного файла:

```
postgress@root:/ pg_dumpall | gzip  > pg_base.gzip
```

Для автоматизированного создания резервных копий используются скрипты, доступные в официальной документации к PostgreSQL на веб ресурсе: https://wiki.postgresql.org/wiki/Automated_Backup_on_Linux.

4.1.3 Периодические работы, выполняемые АБИ

Периодические работы по администрированию ПЛАТФОРМЫ, выполняемые АБИ, приведены в таблице ниже (Таблица 4 .2).

Таблица 4.2 – Периодические работы по администрированию ПЛАТФОРМЫ, выполняемые АБИ

№ п/п	Описание обязанностей	Периодичность	Пункт описания
1.	Подготовка и сохранение резервных копий данных, их периодическая проверка и уничтожение;	ежеквартально	4.1.3.1
2.	Периодическое практическое тестирование защищенности системы	ежегодно	4.1.3.2

4.1.3.1 Подготовка и сохранение резервных копий данных, их периодическая проверка и уничтожение

Резервное копирование основных настроек веб интерфейса осуществляется при резервном копировании БД ПЛАТФОРМЫ средствами СУБД. Данный раздел необходим в случае, если необходимо зарезервировать набор правил для оперативной работы с правилами без прерывания работы ПЛАТФОРМЫ.

Резервное копирование групп правил УРМ осуществляется в разделе «Оценка соответствия» - «Правила» - «Группы правил» (Рисунок 1).

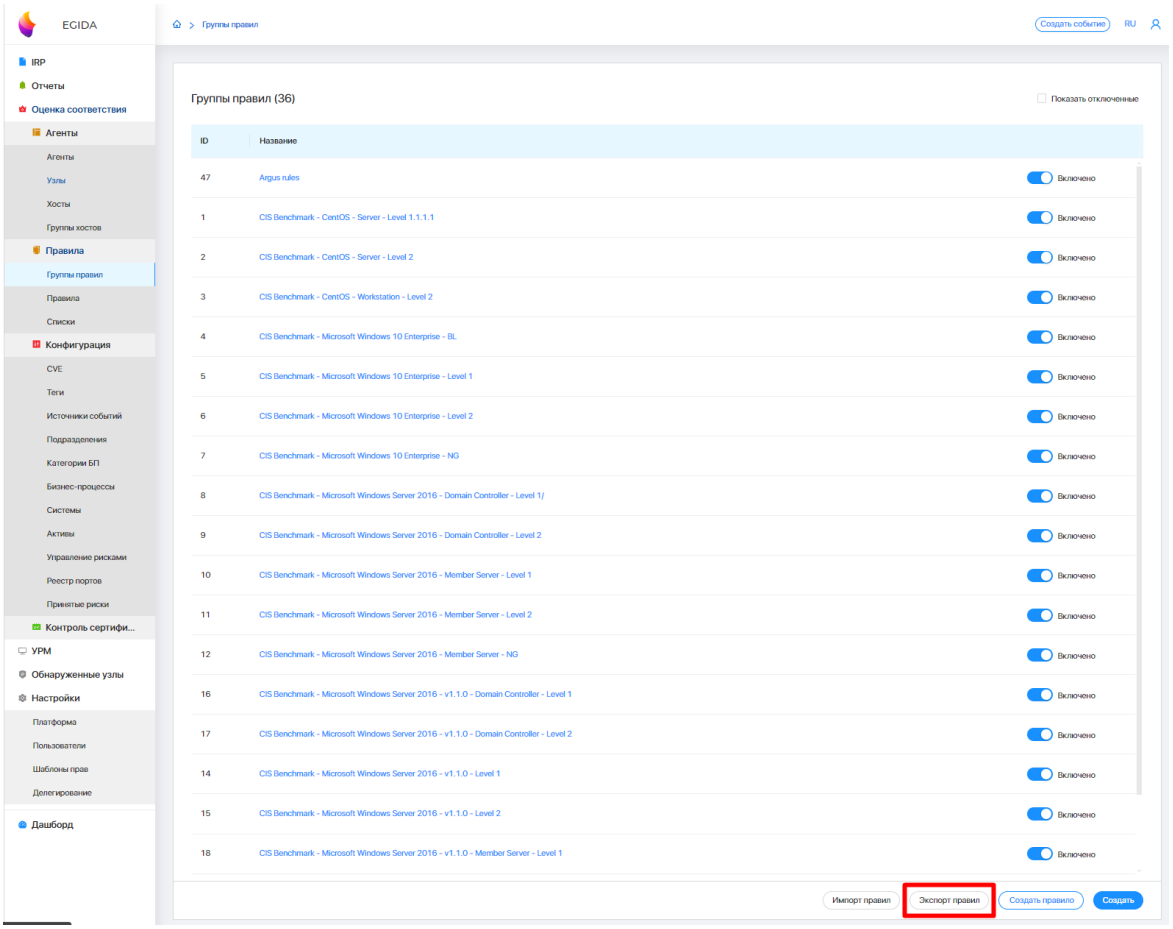


Рисунок 1 - Группы правил

Для создания резервной копии необходимо в правом нижнем углу нажать кнопку «экспорт правил». Затем выбрать необходимые правила, которые необходимо экспортировать и кликнуть по кнопке «скачать» (Рисунок 2). Указать файл, в котором будет сохранена резервная копия.

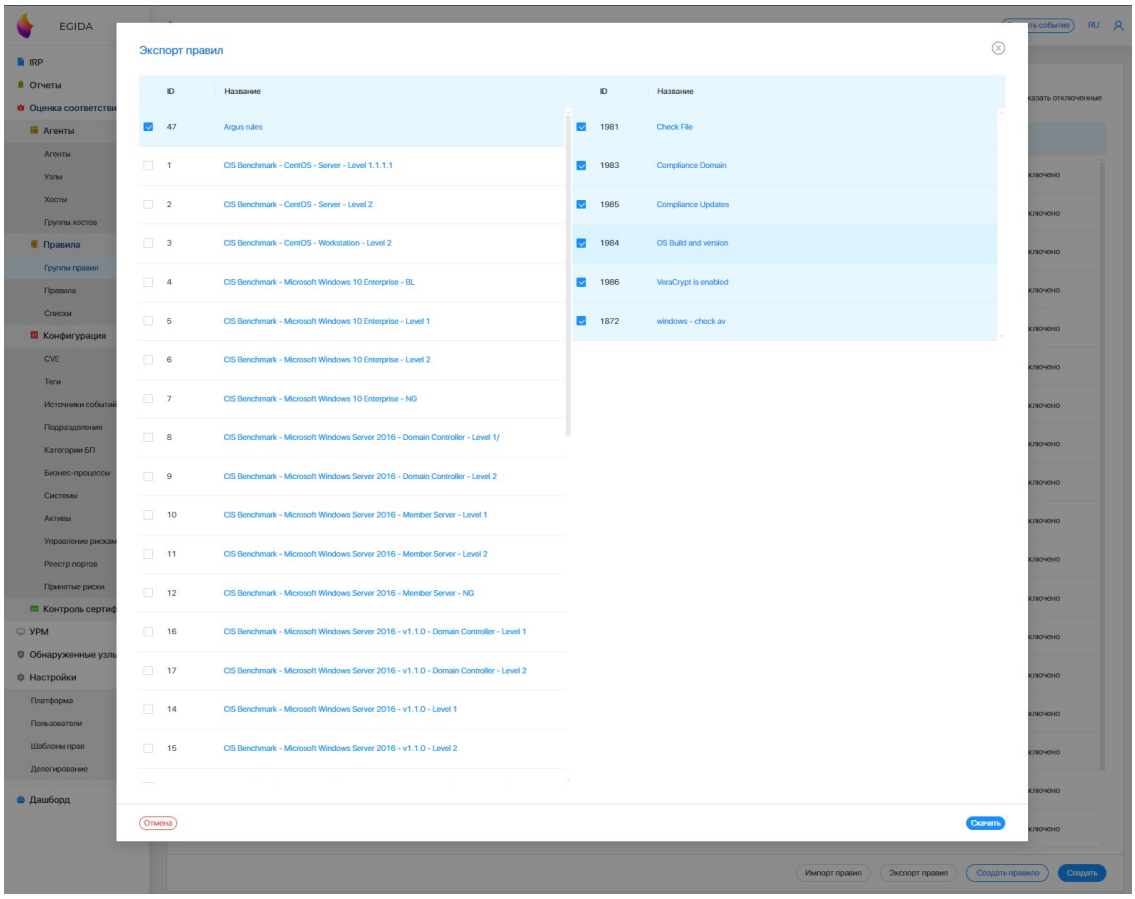


Рисунок 2 – Экспорт правил

Для восстановления правил из резервной копии необходимо воспользоваться кнопкой «Импорт правил», и указать файл-источник созданной ранее резервной копии.

Примечание: Резервная копия правил не защищается платформой. Защищать резервную копию необходимо при помощи ACL, файлового или дискового шифрования надежными алгоритмами шифрования.

4.1.3.2 Периодическое практическое тестирование защищенности системы

Для проверки защищенности системы предлагается использовать стороннее ПО в виде сканеров уязвимостей.

Для проверки защищенности необходимо запустить сканер уязвимостей указав адрес, на котором запущен веб-сервис комплекса управления. Помимо

этого, необходимо удостовериться, что парольная политика соответствует заявленной, периодичность проверок агентов установлена в соответствии с установленной политикой в е.

4.1.4 Непериодические работы, выполняемые СА

Непериодические работы по администрированию ПЛАТФОРМЫ, выполняемые СА, приведены в таблице ниже (Таблица 4 .3).

Таблица 4.3 – Непериодические работы по администрированию ПЛАТФОРМЫ, выполняемые СА

№ п/п	Описание обязанностей	Пункт описания
1	2	3
1.	Первоначальная настройка Egida Аргус, внесение изменений в настройки, настройка групп УРМ, настройка подключений к точкам управления	4.1.4.1
2.	Документирование произведенных настроек	4.1.4.2
3.	Проведение проверок актуальности документации	4.1.4.3
4.	Восстановление работоспособности	4.1.4.4
5.	Редактирование правил и групп доступа	4.1.4.5
6.	Управление разрешениями УРМ	4.1.4.6
7.	Управления ролями и полномочиями пользователей	4.1.4.7

4.1.4.1 Первоначальная настройка Egida Аргус, внесение изменений в настройки, настройка групп УРМ, настройка подключений к точкам управления

Первоначальная настройка Egida Аргус включает в себя настройку работы модулей УРМ, первичное конфигурирование Платформы и настройку подключений к точкам управления сетевым траффиком.

4.1.4.1.1 Настройка УРМ

В разделе «УРМ» web-интерфейса управления Egida Аргус необходимо выбрать раздел «Настройка УРМ» и сконфигурировать периодичность проведения проверок.

Рекомендованные значения уже установлены по умолчанию (Рисунок 3).

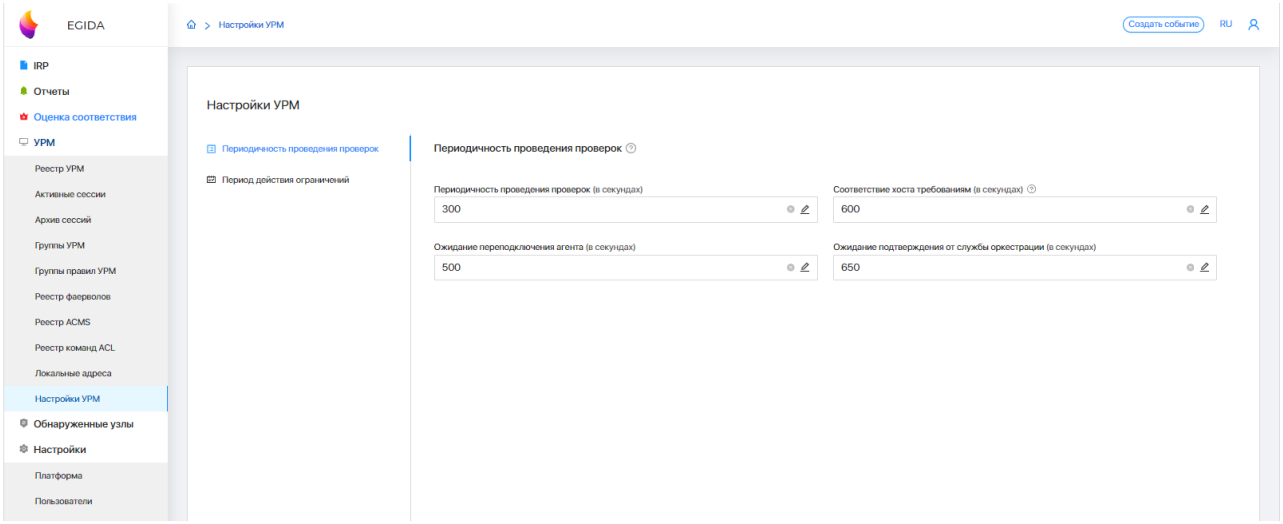


Рисунок 3 – Периодичность проведения проверок

Сокращение периодичности проведения проверок может повлиять на пропускную способность сетевого канала и на производительность УРМ. Увеличение указанных периодов может привести к снижению уровня защищенности внутренней сети компании.

Периодичность проведения проверок (стандартное значение: 300) – период проведения анализа соответствия требованиям по безопасности.

Соответствие хоста требованиям (стандартное значение: 600) – период, в рамках которого хост считается надежным, в случае если от него не получено отчета. Не рекомендуется ставить это значение меньше, чем 2 периода проведения проверок.

Ожидание повторного подключения агента (стандартное значение: 500) – период, в рамках которого система резервирует состояние агента в случае, если подключение было прервано.

Ожидание подтверждения от службы оркестрации (стандартное значение: 650) – отражает период в рамках которых ACMS может ожидать получение решения от службы оркестрации.

В разделе «УРМ» - «Локальные Адреса» необходимо установить какие диапазоны сетей выделены как локальные.

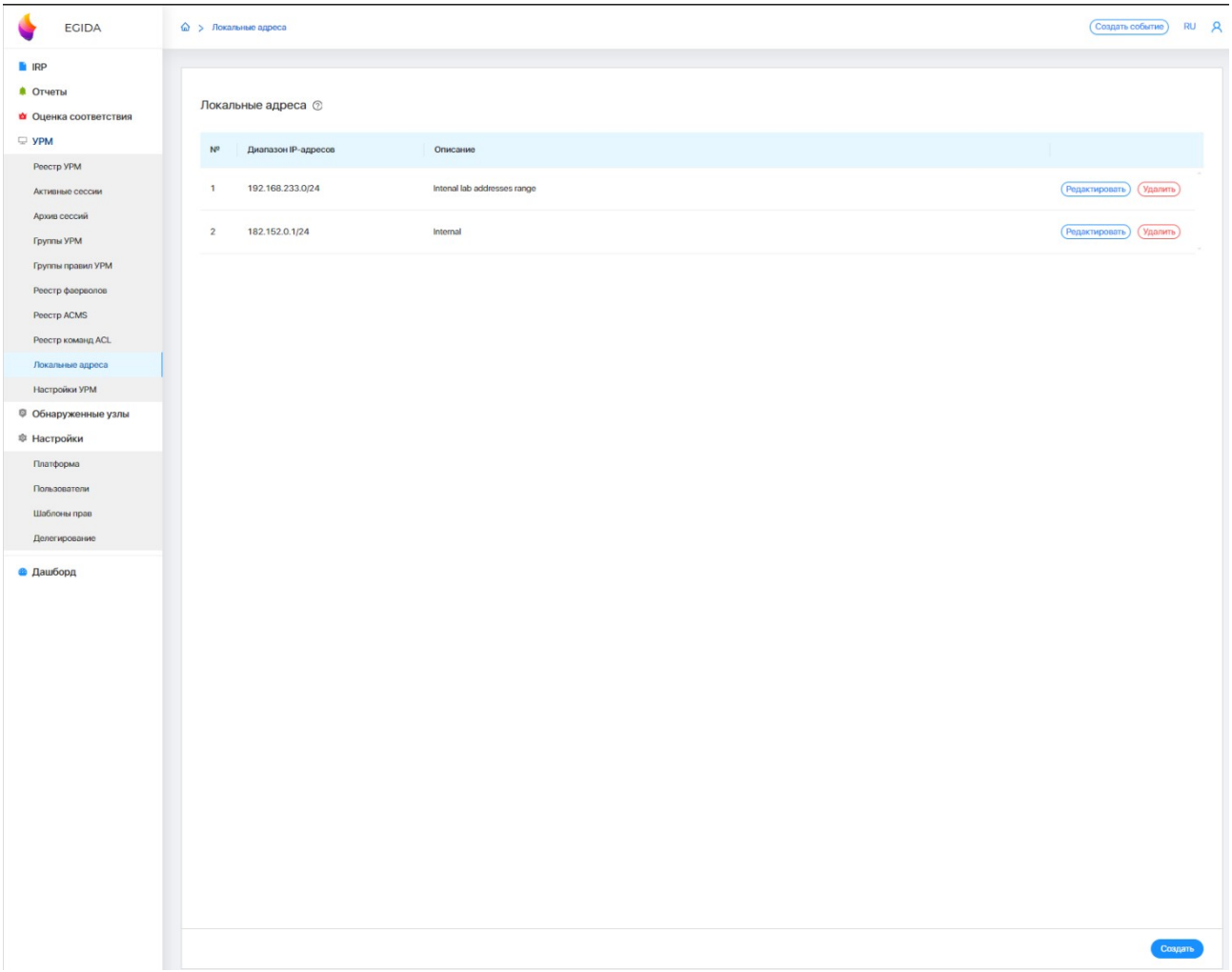


Рисунок 4 – Локальные адреса

Для добавления нового пула адресов, необходимо нажать кнопку «Создать», находящую в правом нижнем углу окна консоли управления, затем в появившемся окне редактирования указать IP-сеть (Рисунок 5). Маска сети, при этом, указывается в бит-формате.

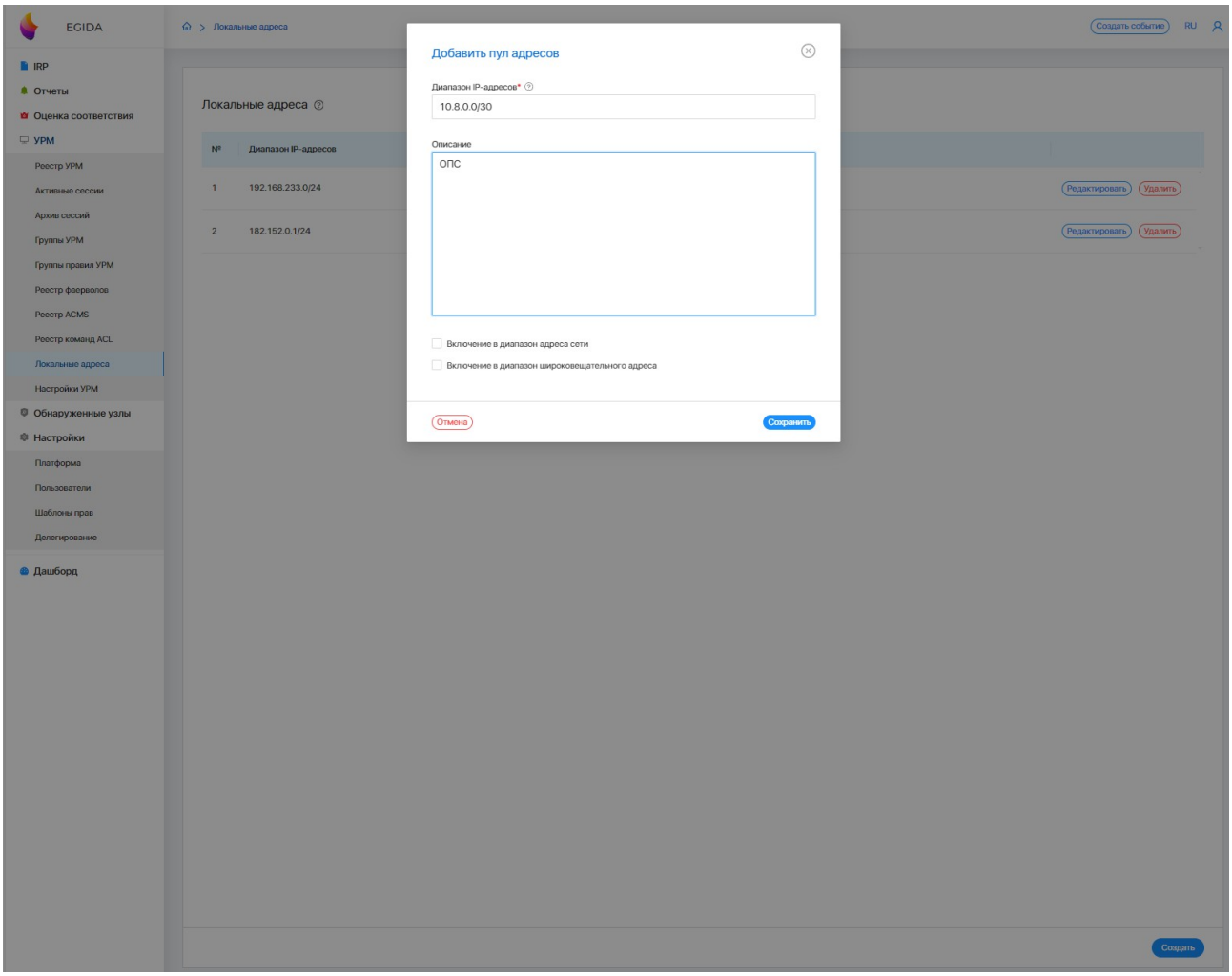


Рисунок 5 – Добавление пула адресов

Примечания:

- Пул ip адресов выделяемых VPN шлюзом не должен попадать в пул локальных адресов.
- В рамках взаимодействия между VPN шлюзом и локальной сетью не должна применяться технология NAT.
- Все подключения узла не из локальных пулов адресов рассматриваются как УРМ. В этом случае подключаемый АРМ автоматически регистрируется как устройство УРМ.

4.1.4.1.2 Заведение УРМ

УРМ в системе заводятся автоматизировано. В случае если подключение УРМ осуществляется не из пула локальных адресов. Ручного добавления УРМ в систему не предусмотрено.

4.1.4.1.3 Заведение агента ACMS

ACMS – Access Control Management Service – приложение ответственное за взаимодействие с точкой управления траффиком (Шлюз, FW)

ACMS регистрируется в системе автоматически. Добавляется в раздел «Реестр ACMS» после первого успешного подключения к серверу.

4.1.4.1.4 Конфигурирование подключения к точке управления траффиком (ACMS)

На данном этапе происходит настройка ACMS, включающая в себя конфигурирование зон ответственности каждого ACMS и настройку связи между ACMS и точкой управления траффиком.

Конфигурирование осуществляется в разделе меню «УРМ» - «Реестр фаерволов» (Рисунок 6).

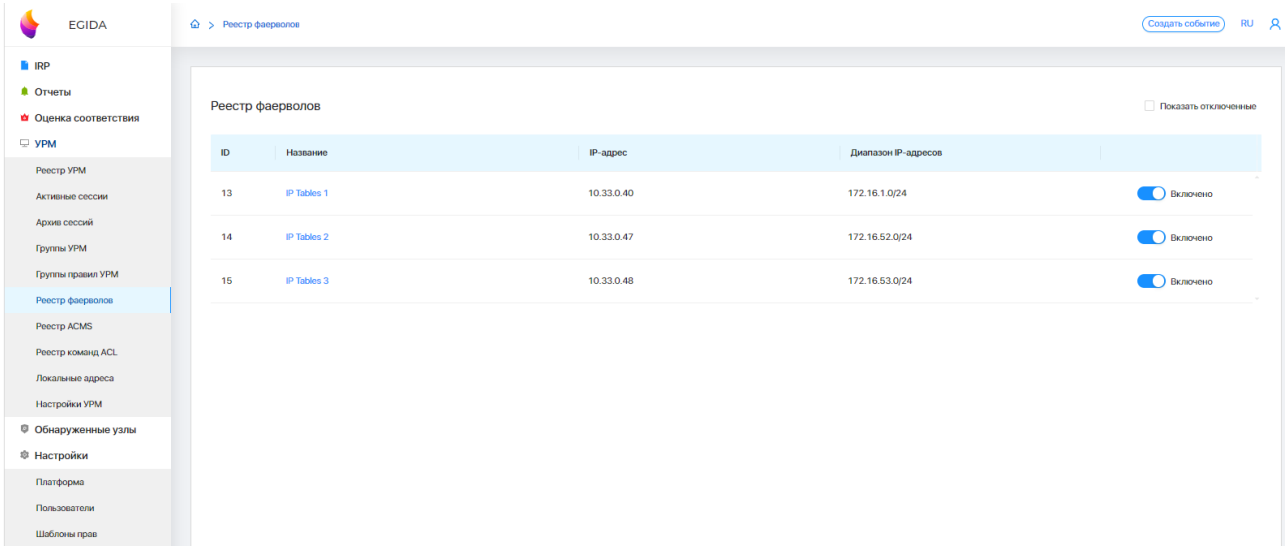


Рисунок 6 – Реестр фаерволов

Для управления точкой управления трафиком, необходимо нажать кнопку «создать» в правом нижнем углу экрана, далее заполнить поля, в соответствии с запросом формы.

В пункте «диапазон ip-адресов» указать адреса, которые считаются УРМ и для которых данная точка является единой точкой маршрутизации между VPN шлюзом и сетью компании.

Команда инициализации фаервола должна содержать инструкцию, в которой будет сконфигурировано базовое состояние этой точки управления траффиком. Одной из первых команд должна быть команда очистки всех разрешающих правил для наиболее корректной работы системы. Выполняется при каждом соединении с точкой управления траффиком. Скрипт необходим на случай восстановления состояния из-за перебоев и/или потери связи с точкой управления или ACMS.

Для корректного заведения точки управления траффиком обязательным является назначение ответственного ACMS для конкретной точки управления (Рисунок 7). Один ACMS может управлять только одной точкой управления траффиком.

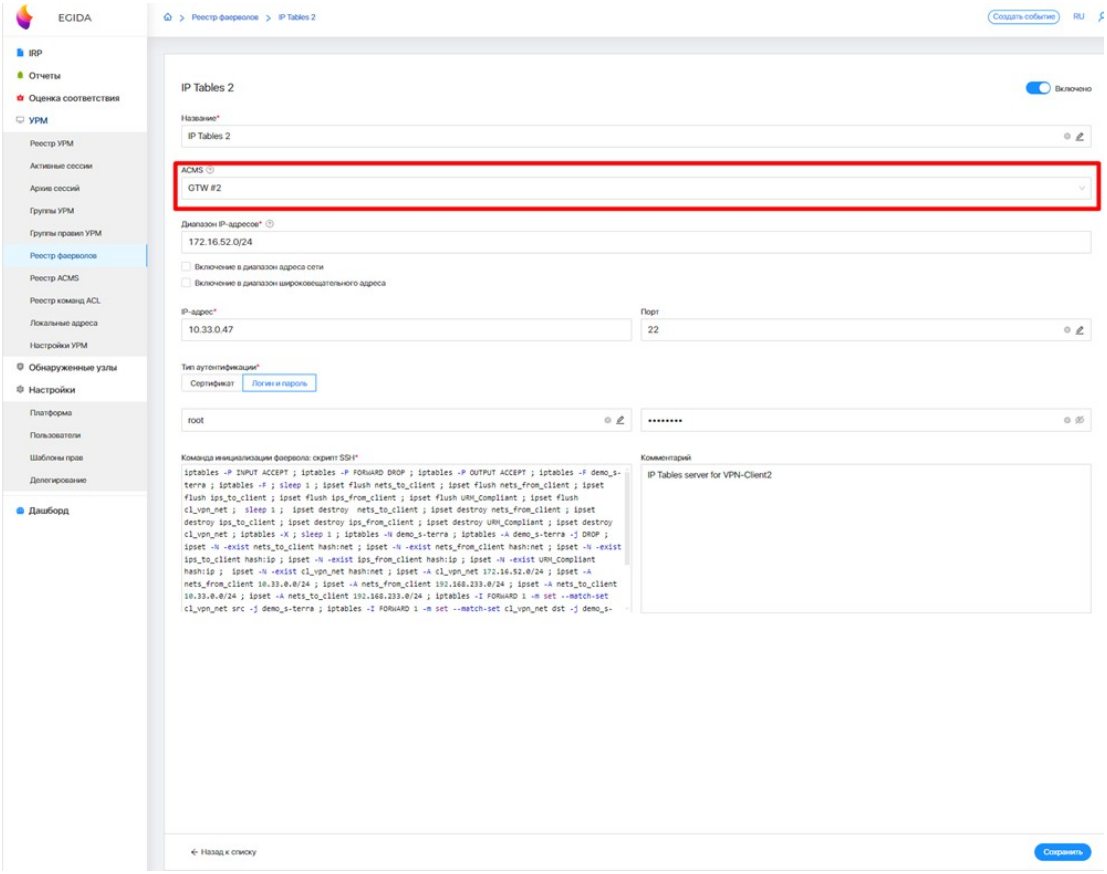


Рисунок 7 – назначение ACMS

4.1.4.1.5 Управление доступом УРМ

Для осуществления управления доступом УРМ предусмотрены команды ACL. Они доступны в разделе «УРМ» - «Реестр команд ACL» (Рисунок 8).

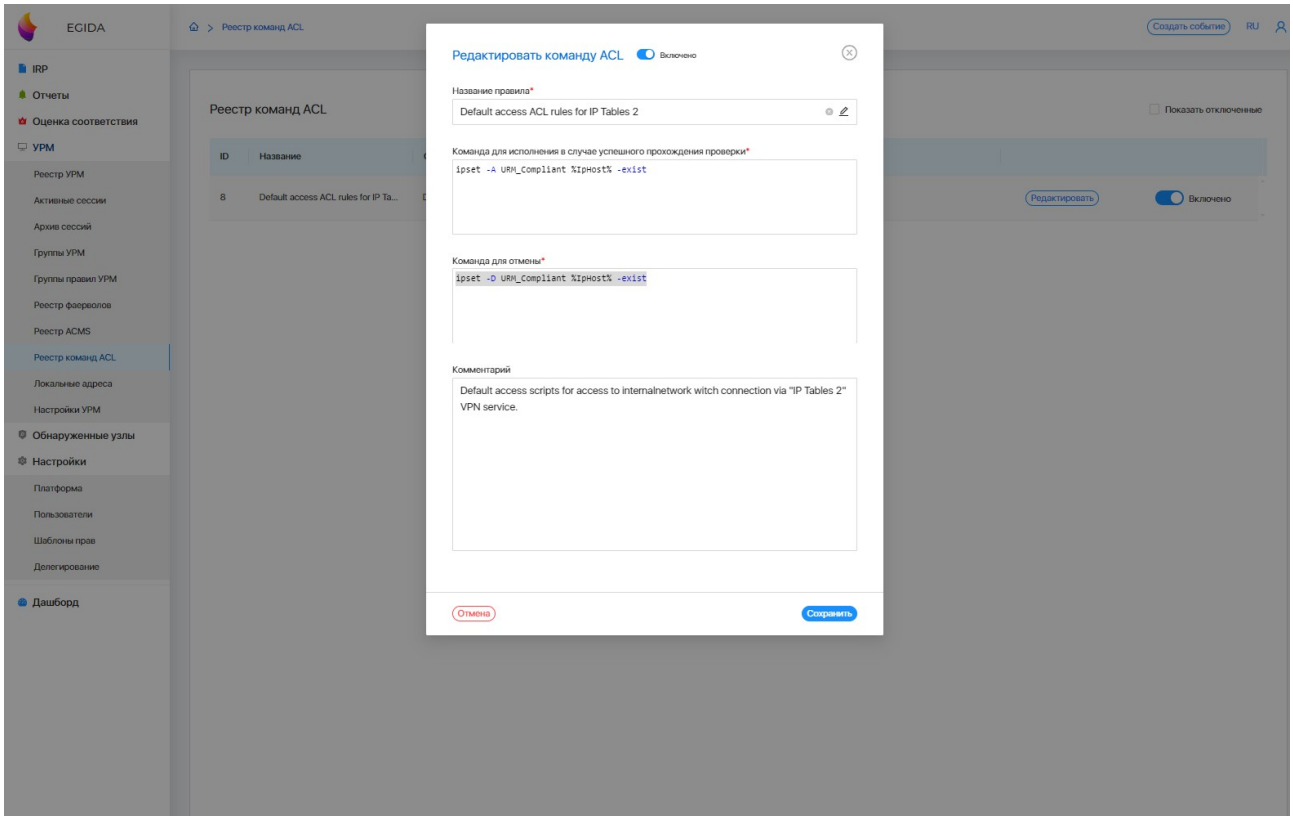


Рисунок 8 – Реестр команд ACL

В данном меню доступны для редактирования наборы команд, которые будут выполняться в случае исполнения требований к конфигурации, а также команды, которые призваны инвертировать эти действия.

Команда должны быть написана в синтаксисе целевой управляемой системы при подключении через SSH.

Предусмотрены переменные.

%IpHost% - заменится ip адресом УРМ

Примечание: «Команда исполнения» и «команда отмены» должны иметь ровно противоположные результаты исполнения.

4.1.4.1.6 Создание групп УРМ

Управление доступом УРМ осуществляется при помощи групп УРМ. Для формирования группы необходимо перейти в раздел «УРМ» - «Группы

УРМ», создать группу. Перейдя в детальный просмотр созданной Группы УРМ (Рисунок 9), во вкладке «состав группы» необходимые добавить требуемые УРМ в эту группу.

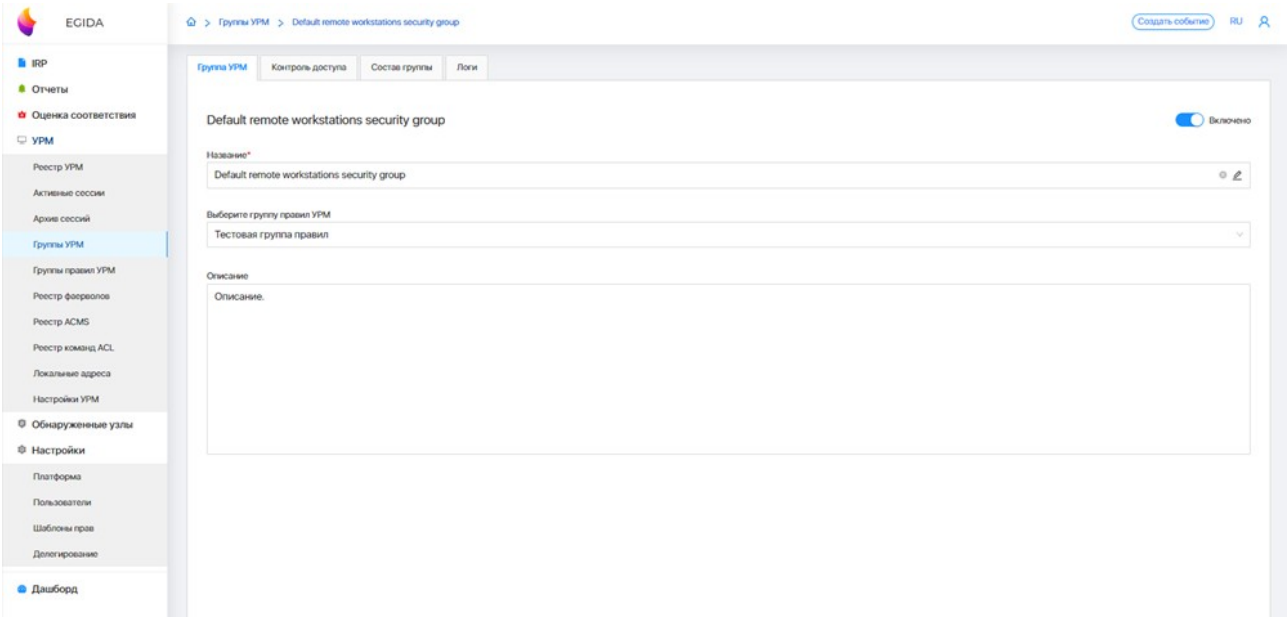


Рисунок 9 – Просмотр группы УРМ

На вкладке «контроль доступа» необходимо добавить набор правил из стандартной поставки ПО:

- проверка наличия/отсутствия определённого установленного ПО;
- проверка наличия/отсутствия определённых запущенных служб;
- проверка наличия/отсутствия определённых значений в реестре;
- проверка выполнения обновления ОС (Windows);
- проверка шифрования диска (Bitlocker)
- проверка выполнения обновления антивирусных баз (Kaspersky).

Помимо предустановленных скриптов доступно создание собственных скриптов проверки. Процедура описана в разделе 4.1.4.5.

Данные правила будут добавлены в число обязательных проверок, в случае успешного прохождения проверки соответствия УРМ стандартам ИБ на каждом конкретном шлюзе. Это позволяет создать разные конфигурации доступа в зависимости от точки подключения.

4.1.4.2 Документирование произведенных настроек

После каждого регламентированного изменения конфигурации, СА необходимо выполнить обновление файла эталонных настроек.

Поддержание документации в актуальном состоянии необходимо как дополнительное средство обнаружения нерегламентированных изменений в конфигурации компонентов комплекса.

4.1.4.3 Проведение проверок актуальности документации

После каждого регламентированного изменения конфигурации, СА требуется произвести сравнение фактической конфигурации с эталонной конфигурации хранящейся в файле эталонных настроек.

Поддержание документации в актуальном состоянии необходимо как дополнительное средство обнаружения нерегламентированных изменений в конфигурации компонентов комплекса.

4.1.4.4 Восстановление работоспособности

Восстановление работоспособности возможно с помощью восстановления состояния системы из ранее созданных резервных копий. Резервные копии, созданные в соответствии с данным руководством, будут содержать файл с описанием процесса восстановления сгенерированные СУБД.

4.1.4.5 Редактирование правил и групп доступа

Процесс управления доступами описан в разделах 4.1.4.1.3 - 4.1.4.1.4.

Процедура создания пользовательских правил:

В меню «Оценка соответствия» - «Правила» - «Правила» (Рисунок 10), в правом нижнем углу экрана нажать на кнопку «Создать».

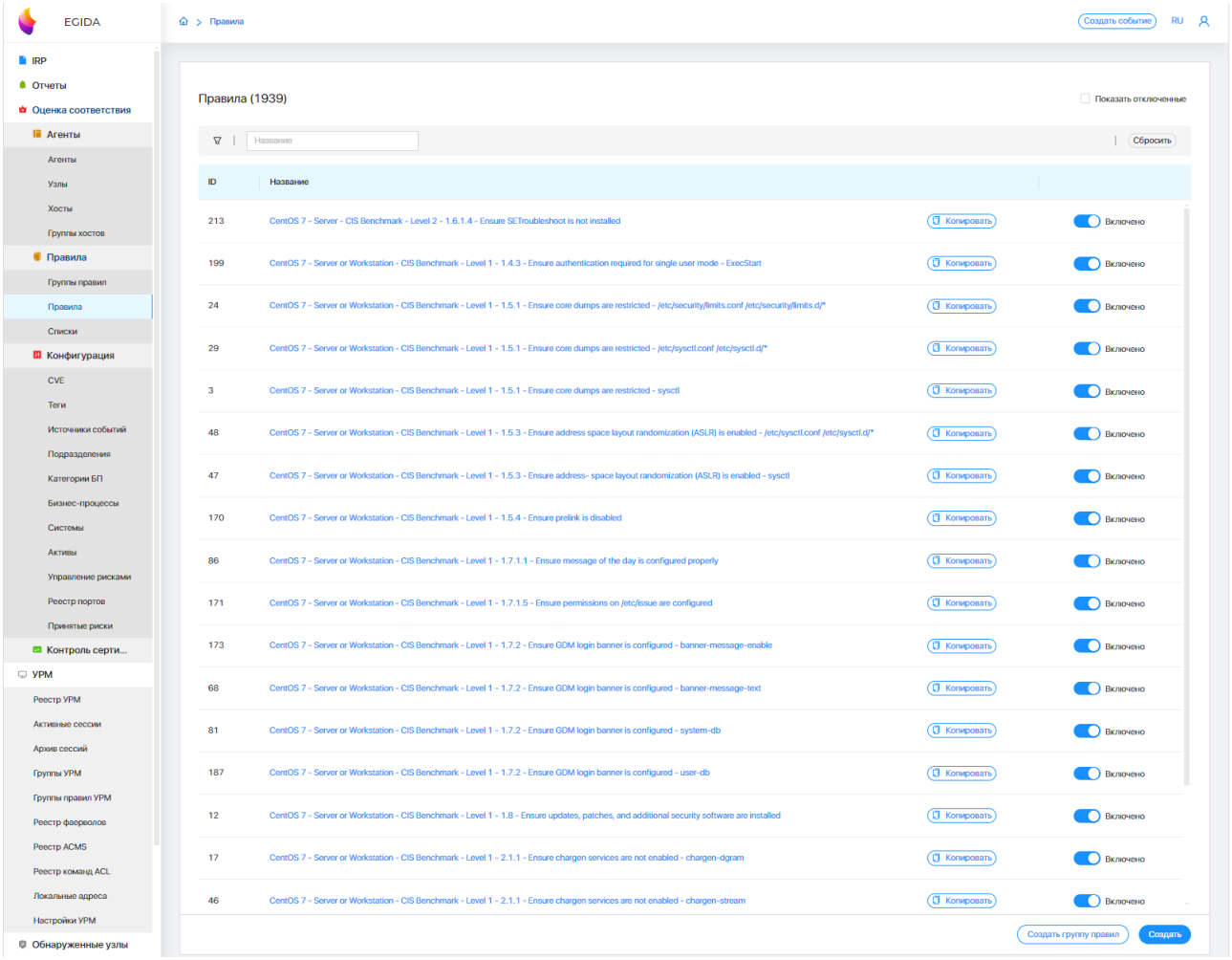


Рисунок 10 – Правила оценки соответствия

- В появившемся окне (Рисунок 11) необходимо выбрать тип скрипта над полем «Скрипт». Для ОС Windows необходимо выбрать Powershell, для linux - shell. Скрипт пишется в соответствии с выбранным типом скрипта. Скрипты на выходе должны выводить объекты вида ключ-значение.

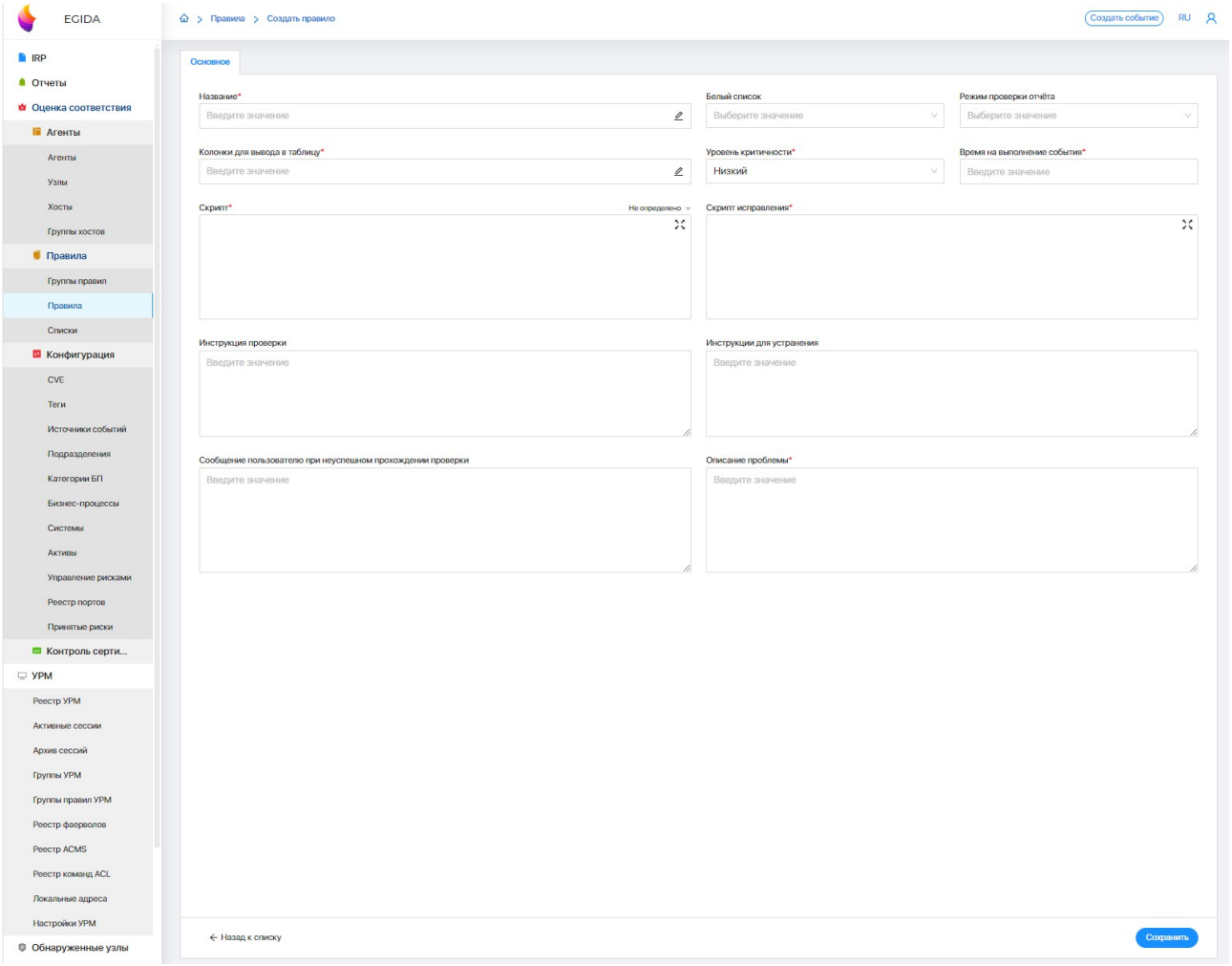


Рисунок 11 – Создание правила оценки состояния

- В поле «колонки для вывода в таблицу», указываются Ключи, которые участвуют в проверке, через “;” (Рисунок 12).

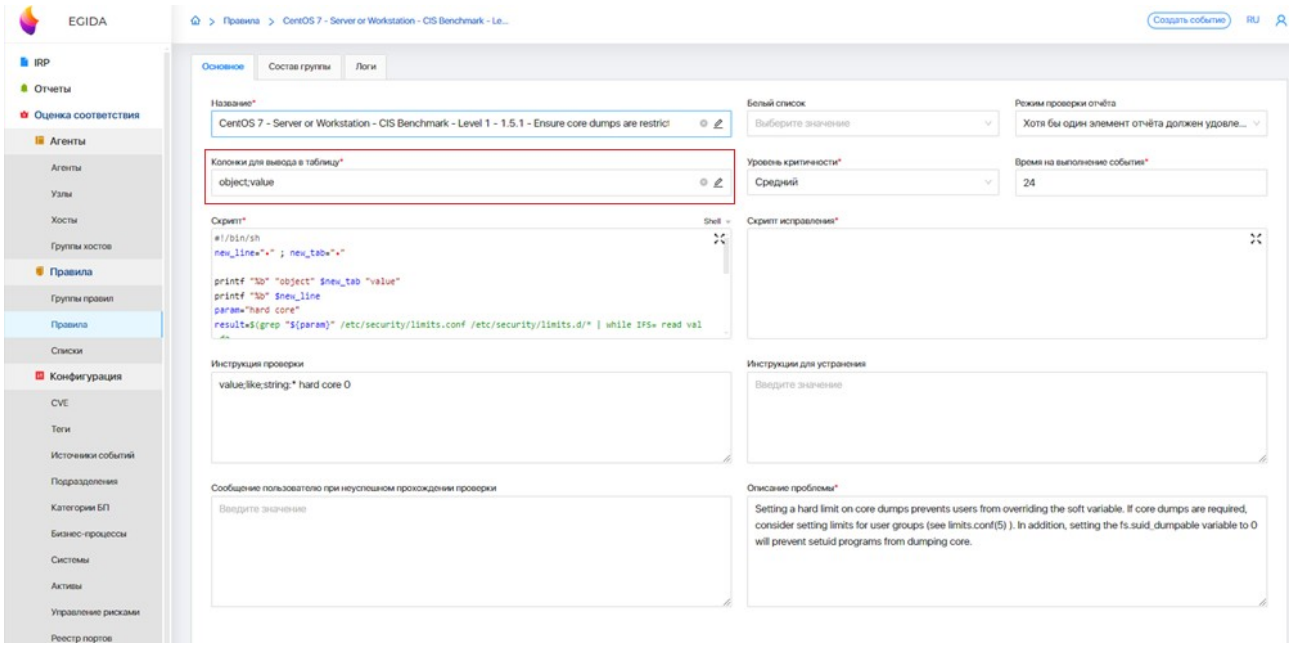


Рисунок 12 – Указание ключей для вывода в таблицу

- В поле «Инструкция проверки» (Рисунок 13) вносится выражение, которое проверяет соответствие заданным значениям. Значения могут быть строковыми или числовыми. Возможные операторы сравнения: >; >=; <; <=; =; like.

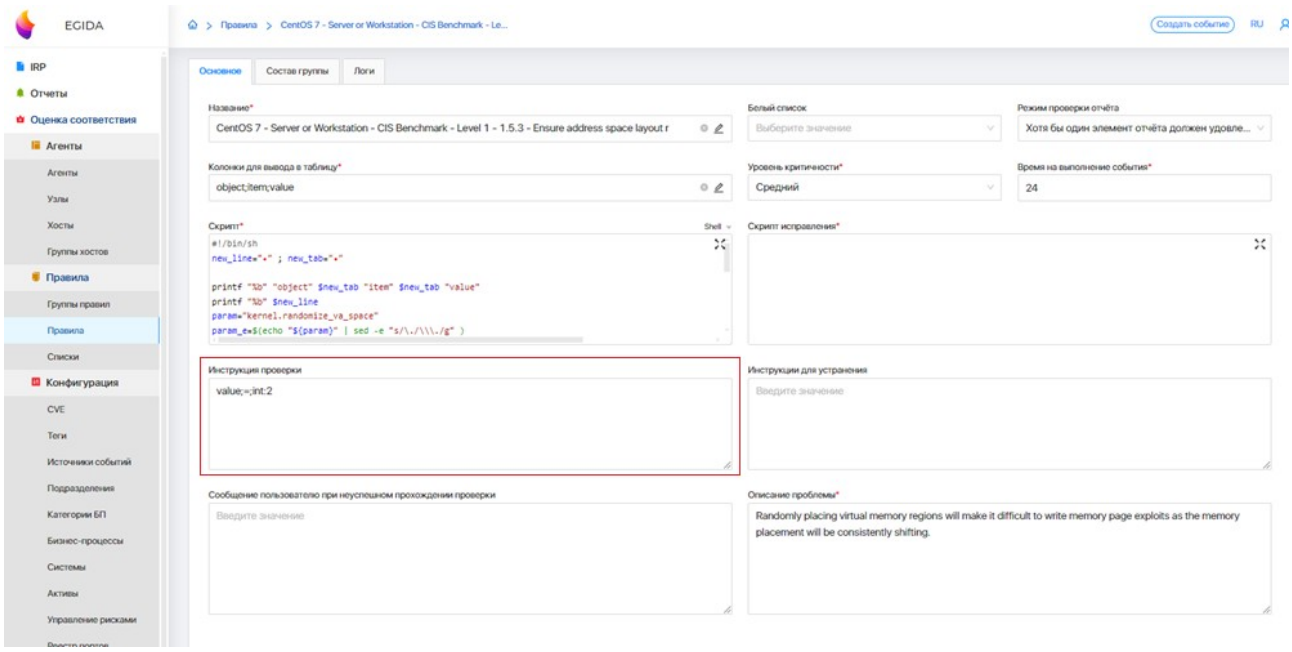


Рисунок 13 – Инструкция проверки

Скрипт устранения – скрипт, который выполнится при попытке агента в автоматическом режиме выполнить устранение проблемы.

Если все условия из поля «инструкция проверки» принимают значение «истина», тогда правило считается выполненным успешно.

4.1.4.6 Управление разрешениями УРМ

Управление разрешениями УРМ осуществляется в разделе «УРМ» - «Реестр команд ACL».

Для создания нового правила необходимо нажать на кнопку «создать». Далее необходимо заполнить соответствующие поля в появившемся окне (Рисунок 14). Обязательным является указание команды отмены, инвертирующей команду для исполнения.

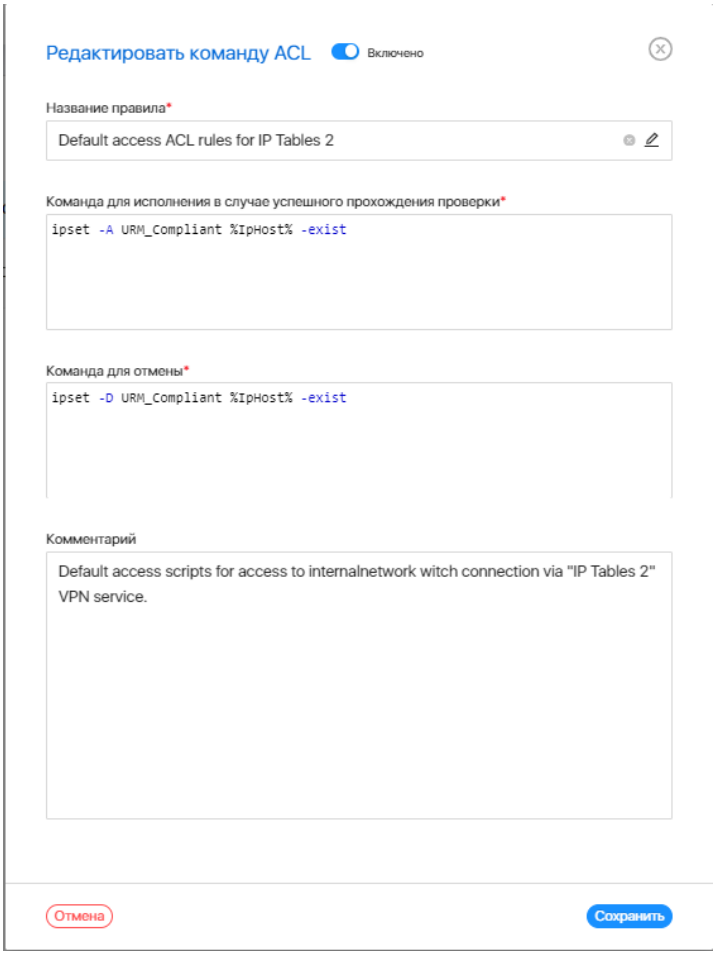


Рисунок 14 – Управление разрешениями УРМ

Команды указываются в соответствии с синтаксисом целевой управляемой системы при подключении SSH.

4.1.4.7 Управления ролями и полномочиями пользователей

Управление пользователями осуществляется в меню «Настройки» - «Пользователи».

При первичной настройке обязательно необходимо создать пользователя с полномочиями АС. Встроенная учетная запись не предназначена для эксплуатации системы. Встроенный пользователь должен быть отключен после создания АС Платформы.

Создать пользователя можно нажав на кнопку «Добавить» в правом нижнем углу окна «Пользователи». Далее необходимо заполнить поля формы создания пользователей (Рисунок 15). Обязательным свойствами являются: имя пользователя, подразделение, e-mail. Также имеется возможность создать Подразделение в справочнике «Настройки» - «Подразделения» и затем указать данное подразделение для создаваемого пользователя.

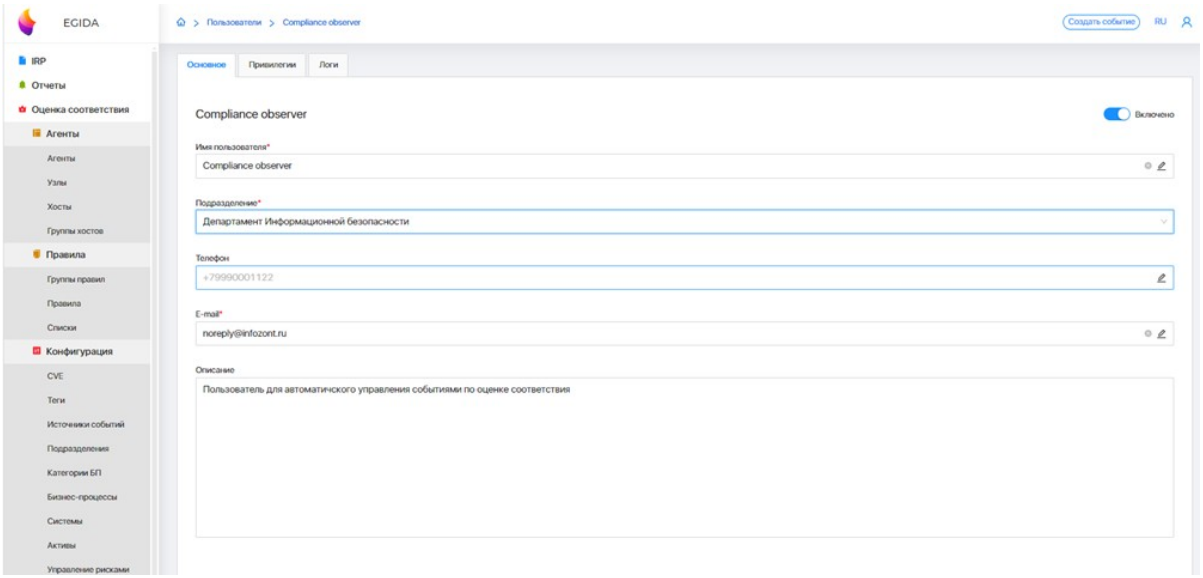


Рисунок 15 – Создание пользователя Платформы

В окне детального просмотра свойств пользователя на вкладке «права», в правом верхнем углу необходимо выбрать одну из предустановленных ролей:

- «Пользователь УРМ» - для пользователей, которые могут осуществлять просмотр интерфейсов управления УРМ;
- «Администратор УРМ» - для администраторов, осуществляющих управление настройками подключения к ACMS.

4.1.5 Непериодические работы, выполняемые АБИ

Непериодические работы по администрированию Платформы, выполняемые АБИ, приведены в таблице ниже (Таблица 4 .4).

Таблица 4.4 – Непериодические работы по администрированию комплекса защищенного удаленного доступа, выполняемые АБИ

№ п/п	Описание обязанностей	Пункт описания
1	2	3
1.	Поддержание системы в рамках утвержденной политики безопасности	4.1.5.1
2.	Создание и поддержание в актуальном состоянии пользовательских учётных записей	4.1.5.2
3.	Отслеживание информации об уязвимостях системы и своевременное принятие мер	4.1.5.3

4.1.5.1 Поддержание системы в рамках утвержденной политики безопасности

После каждого регламентированного изменения конфигурации АБИ производит сравнение фактической конфигурации на соответствие требованиям

безопасности установленным внутренним нормативными документами в области ИБ.

В качестве профилактической меры АБИ должен проверять назначенные на группы УРМ группы правил УРМ, установленные периодичности проверок.

Поддержание конфигурации в актуальном состоянии необходимо как дополнительное средство обнаружения нерегламентированных изменений в конфигурации компонентов комплекса.

4.1.5.2 Создание и поддержание в актуальном состоянии пользовательских учётных записей

АБИ должен проверять актуальность учетных записей, активных в системе. Своевременное удаление учетных записей из комплекса снижает риски несанкционированных изменений в Платформы.

Управление учетными записями осуществляется в разделе веб-интерфейса Платформы «Настройки» - «Пользователи» (см. раздел 4.1.4.7).

4.1.5.3 Отслеживание информации об уязвимостях системы и своевременное принятие мер

АБИ должен просматривать информационные письма об обнаруженных уязвимостях от лицензиара, и выполнять инструкции, приложенные к информационным письмам.

В случае обнаружения АБИ уязвимостей, необходимо сообщить лицензиару об уязвимости

5 Работа с интерфейсом Системы

5.1 Модуль управления событиями ИБ

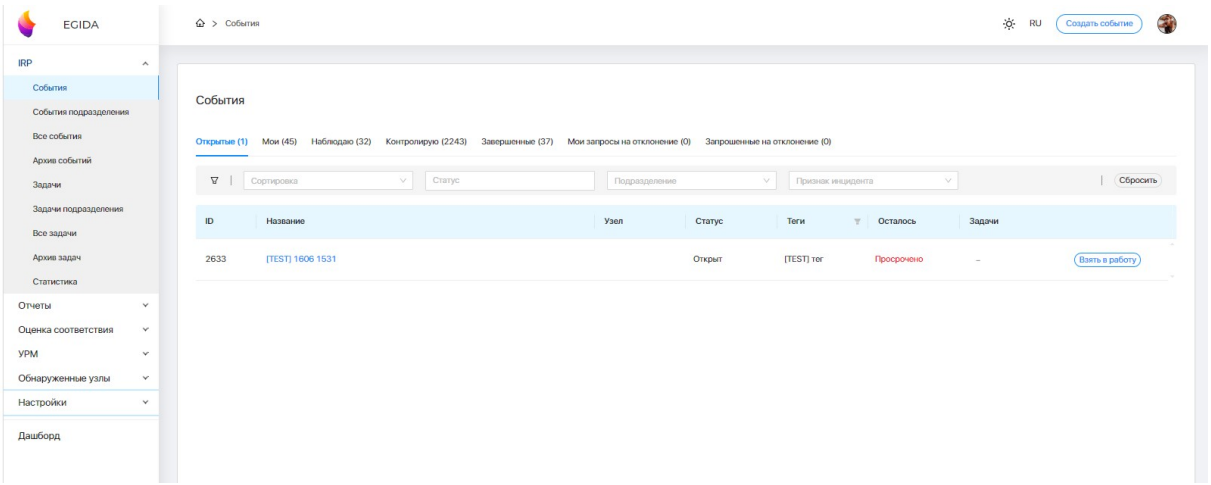


Рисунок 16. Общий вид раздела IRP

Модуль управления событиями (далее - МУС) представляет собой платформу управления задачами. Основой парадигмой является принцип контроля и неотказуемости.

Принцип контроля – каждая задача должна проверяться контролером перед закрытием

Принцип неотказуемости – каждое действие с событием или задачей регистрируется системой.

5.1.1 Роли пользователя

В МУС пользователь может выступать в следующих ролях
- Ответственный – пользователь, который может просматривать все сведения о событии, управлять им и завершать задачу. Может быть назначена только одному пользователю в одном событии
- Соисполнитель – пользователь, который получает все полномочия «ответственного», но не несет ответственность за результат. В одном событии может быть множество пользователей
- Контролирующий – пользователь, который принимает результат выполненных работ по событию. Контролирующий может закрыть событие.
- Наблюдатель – не имеет полномочий для редактирования, внесения изменений в событие но имеет возможность просматривать его

5.1.2 События

В разделе события существуют несколько вкладок
Вкладка «открытые» - список всех событий назначенных на подразделение к которому относится пользователь.

Вкладка «Мои» - список событий, в которых пользователь участвует в роли «Ответственный» или «соисполнитель»
Вкладка «Наблюдаю» - список событий, в которых пользователь участвует в роли «Наблюдатель»
Вкладка «Контролирую» - в этом разделе находятся события требующие контроля от пользователя
Вкладка «Завершенные» - события которые были завершены и находятся на контроле у пользователя с ролью «Контролирующий»
Вкладка «Мои запросы на отклонение» - список событий, которые по каким либо причинам стали не актуальны, Ответственный или соисполнитель могут создать запрос Контролирующему на закрытие события
Вкладка «Запросы на отклонение» - список входящих запросов на отклонение.

5.1.3 Сущность событие

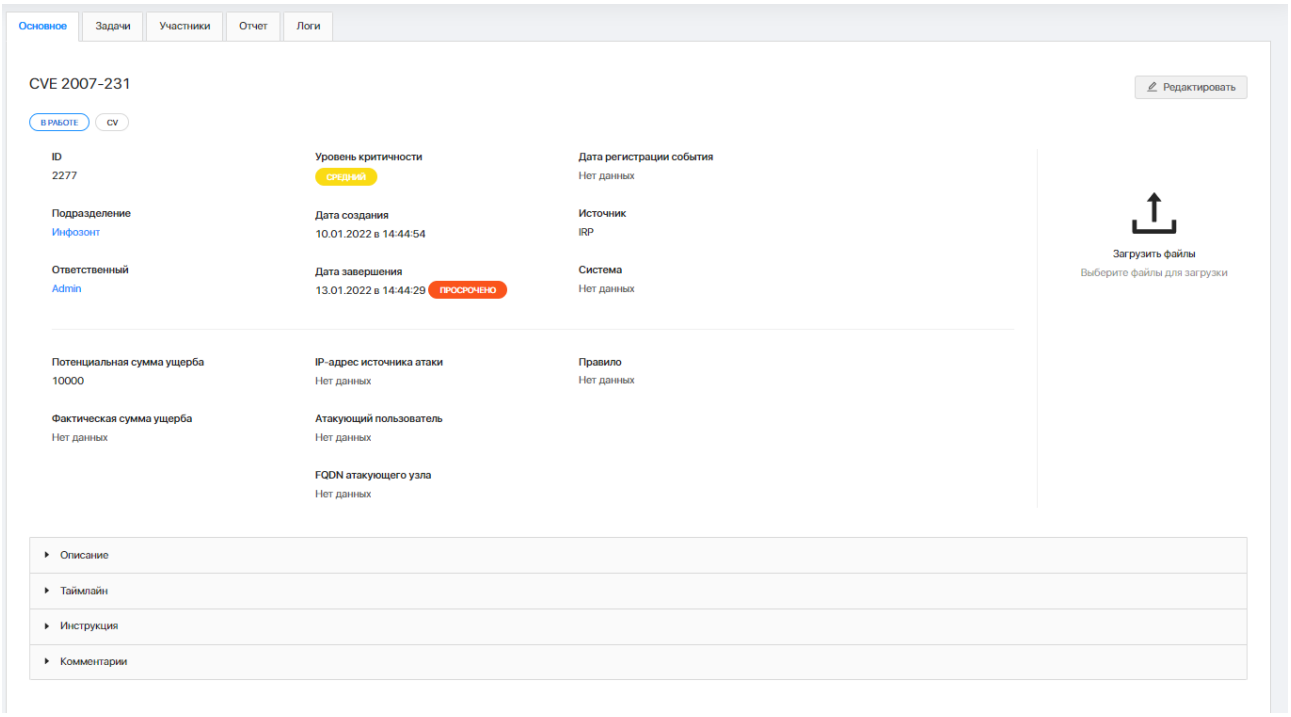


Рисунок 17. Общий вид События

Событие может быть создано двумя способами:
1) автоматизировано, на базе правил. Если одно или несколько правил ПОС в режиме информирования выдают отрицательный результат. В этом случае будет создано события с параметрами, настроенным в правиле ПОС.

2) вручную, с помощью кнопки в правом верхнем углу. В этом случае пользователь может вручную задать все параметры события

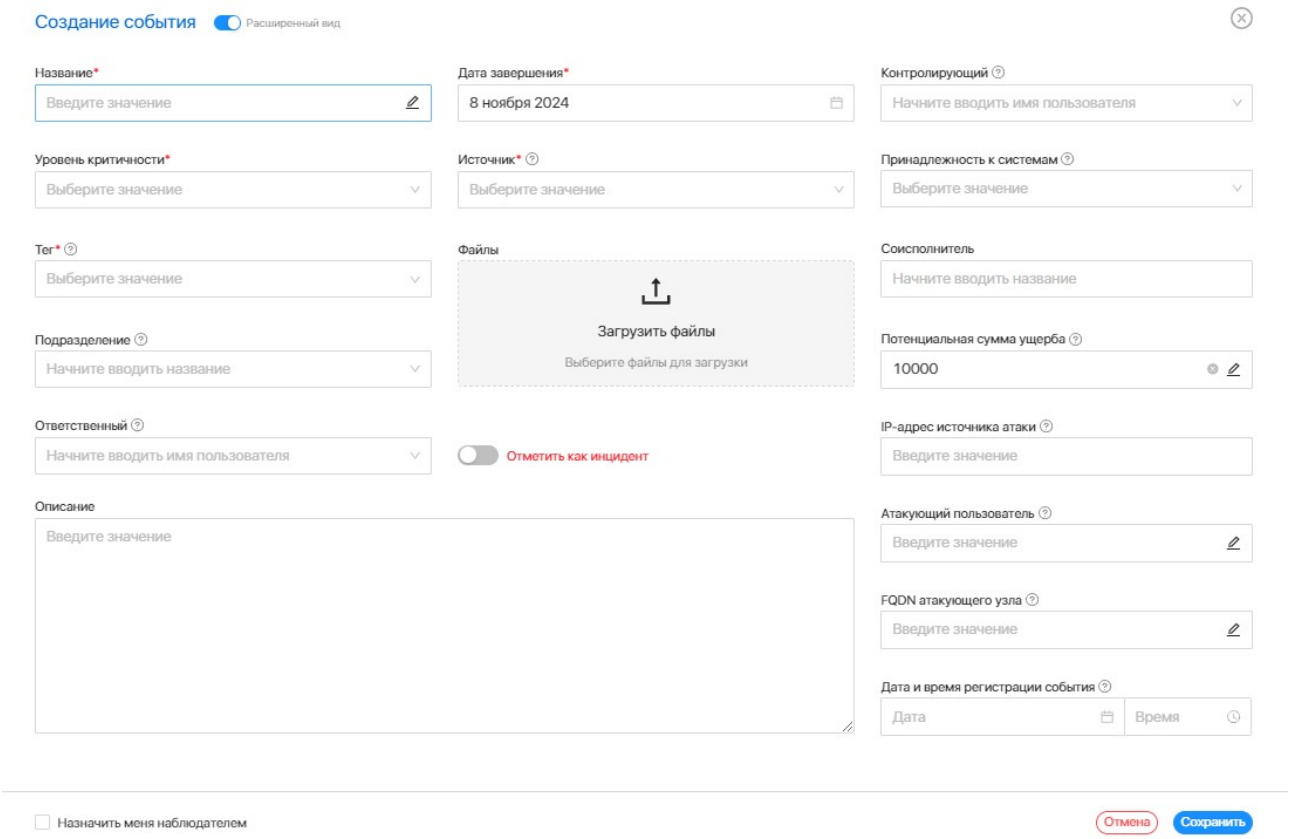


Рис 18. Ручное создание события.

События доступны к просмотру только пользователям подразделения, в которое назначено событие, руководителю подразделения и пользователю с правом просмотра «всех событий».

5.1.4 Задачи

Задача – дочерняя сущность События и неразрывно связана с ним.
Задача необходима в том случае, если нужно привлечь внешние подразделения, без раскрытия подробностей События.

Для создания задачи необходимо на вкладке «задачи» в Событии нажать на кнопку «Создать»

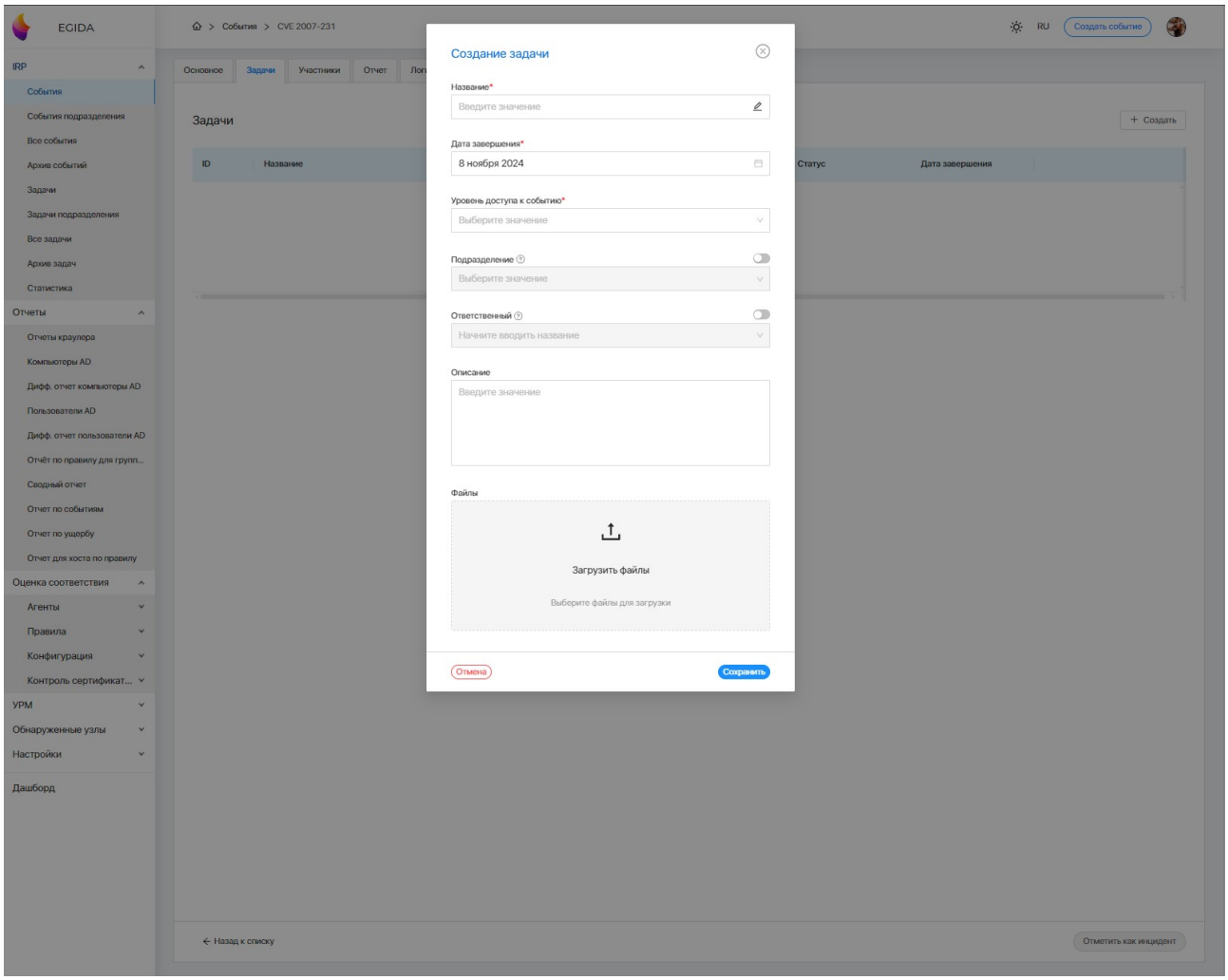


Рис 19. Окно создания задачи.

Заполните поля в форме.

Нельзя закрыть событие, в котором находятся открытые задачи.

5.2 Оценка соответствия

Модуль оценки соответствия позволяет производить оценку соответствия узлов ИС в двух режимах, в режиме информирования (оценка соответствия) и режиме управления (УРМ).
Режим управления описан выше, в разделе ПОС.
Режим информирования предназначен для проведения аудит узлов ИС в соответствии с требованиями, установленными в компании.
Требования к устанавливаются в разделе правила, аналогично ПОС (см раздел Редактирование правил и групп доступа)

Приложение А
(обязательное)
Установка серверной части приложения

А.1 Общие положения по установке СУБД и конфигурации БД

Все серверные компоненты в качестве системы управления базами данных используют решение PostgreSQL и рассчитаны на 13 мажорную версию и выше.

Конфигурация СУБД и БД должна осуществляться в соответствии с внутренними регламентами по администрированию (создание резервных копий, управление используемыми дисковыми пространствами) с учётом следующих рекомендаций:

- Для каждого компонента системы должные быть создавать отдельные пользователи для обеспечения сегрегации доступов.
- Должны быть прописаны правила подключения пользователей к базам данных с учётом сегрегации доступов (для каждого из компонентов выделяется отдельный пользователь, и для него должны быть предоставлен доступ на подключение только к тем БД, которые он использует).
- В случае, если СУБД находится на отдельном сервере от компонентов серверной инфраструктуры (для взаимодействия необходимо коммуникация по сети), рекомендуется настроить шифрование коммуникации с СУБД при помощи TLS (в том числе ограничить способы подключения для пользователей).

Остальные параметры СУБД и баз данных могут быть скорректированы на основании особенностей работы отдельных компонентов системы в рабочей инфраструктуре.

Общие положения по установке компонентов системы

Дистрибуция компонентов системы осуществляется путём передачи бинарных файлов или файлов документов отображаемым веб браузерами. Для сегрегации доступов приложений внутри хостовой операционной системы рекомендуется создавать отдельного пользователя с назначением ему соответствующих доступов. В соответствии с этим, существует рекомендация по используемым путям развёртывания, которая выглядит следующим образом:

1. В качестве корневой директории используется **/opt/egida/** (далее **%egida_root%**)
2. Внутри корневого каталога, упоминаемого в пункте *1*, идёт разделение на следующие директории:
    1. **%egida_root%/bin** - используется для размещения бинарных файлов компонентов системы. Для каждого из устанавливаемых компонентов системы внутри данного каталога создаётся директория по имени компонента (например **api**) (далее **%bin%**)
    2. **%egida_root%/etc** – используется для размещения файлов конфигурации компонентов системы. Для каждого из устанавливаемых компонентов системы внутри данного каталога создаётся директория по имени компонента (например **api**) (далее **%etc%**)
    3. **%egida_root%/varwww** – используется для размещения файлов, связанных с управлением системой через веб браузер
        - **%egida_root%/varwww/spa** - используется для хранения файлов веб приложения, отображаемых веб браузером (далее **%varwww-spa%**)
        - **%egida_root%/varwww/attachments** – используется для сохранения файлов- вложений, сохранённых в системе через веб интерфейс (далее **%varwww-attachments%**)
3. В качестве корневого каталога для файлов логов компонентов системы используется **/var/log/egida**. Для каждого из компонентов системы выделяется отдельная директория внутри корневого каталога логов по имени компонента (например **api**) (далее **%logs%**)

В случае, если в компании существует соглашение по дистрибуции и/или развёртыванию похожих систем, параметры каталогов могут быть изменены в соответствии с данным регламентом.

Большая часть серверных компонентов системы развёртывается при помощи системы управления службами в Linux systemd. Это позволяет настроить изоляцию переменных окружения для компонентов системы.

А.2 Установка компонентов систем

Установка и настройка компонента API

Начальные требования

1. Установлен ASP.NET Core runtime 6-ой мажорной и наиболее высокой минорной версии на момент установки
2. В СУБД создан пользователь для компонента (например **egida_api_user**) и известны его параметры (имя, пароль, параметры целевого экземпляра СУБД)
3. Созданы необходимые БД в СУБД, упоминаемой в пункте *2*
    - база данных с основной конфигурацией системы (например **egida_global**), владельцем которой является пользователь из пункта *2*
    - база данных, содержащей отчёты оценки соответствия (например **egida_reports**), владельцем которой является пользователь из пункта *2*
    - база данных, содержащей конфигурацию модуля мониторинга сети (например **egida_networkanalysys**), владельцем которой является пользователь из пункта *2*
    - база данных, содержащей конфигурацию модуля мониторинга контроллеров домена (например **egida_ldap**), владельцем которой является пользователь из пункта *2*
4. В СУБД настроены политики подключения пользователя из пункта *2* к базам данных из пункта *3*
5. Определены целевые директории размещения бинарных файлов, файлов конфигурации и логов
6. Определена директория для размещения вложений, сохраняемых в системе при помощи веб интерфейса управления

Установка представляет из себя следующую последовательность шагов:

1. Копирование бинарных файлов компонента в директорию **%bin%** и установка соответствующих прав
2. Копирование файлов конфигурации компонента в директорию **%etc%/api/** и установка соответствующих прав

3. Создание директории **%logs%/api/** для файлов логов компонента и установка соответствующих прав
4. Актуализация параметров работы модуля *systemd* в файле конфигурации (пример находится в директории **/appendix/etc/api/ egida_api.service**)*:*
    a. Пользователь и группа, под которыми должен работать модуль компонента (параметры **User** и **Group** соответственно)
    b. Рабочая директория должна быть установлена в директорию, упоминаемой в шаге *1* (параметр **WorkingDirectory**)
    c. Файл переменных окружения должен быть установлен в соотвествии с расположением в директории, упоминаемой на шаге *2* (параметр **EnvrionmentFile**)
5. Актуализация параметров, хранящихся в файле переменных окружения для модуля *systemd* (пример находится в директории **/appendix/etc/api/egida_api.env**)
    a. Параметры подключения к БД, содержащей основную конфигурации системы (параметр **ConnectionStrrings__global**)
    b. Параметры подключения к БД, содержащей отчёты оценки соответствия (параметр **ConnectionStrrings__reports**)
    c. Параметры подключения к БД, содержащей конфигурацию модуля мониторинга сети (параметр **ConnectionStrrings__NetworkAnalysys**)
    d. Параметры подключения к БД, содержащей конфигурацию модуля мониторинга контроллеров домена (параметр **Ldap__ConnectionStrrings__main**)
    e. Параметры путей файлов логирования, в частности путь и имя файла внутреннего логирования и корневой директории файлов логов компонента, упоминаемой в шаге *3*, и (параметры **NLog__internalLogFile** и **NLog__variables__logDirectory** соответственно)
    Примечание: файл внутреннего логирования рекомендуется держать в директории логов компонента, хотя это и не обязательно
6. Конфигурация *systemd*

Создание файла-ссылки с настройкой модуля в *systemd* в директории **/etc/systemd/system/**

Сделать это можно при помощи следующей команды

ln -s %etc%/ api /egida_api.service /etc/systemd/system/ egida_api.service

....

Активация модуля путём выполнения следующей команды: systemctl daemon-reload && systemctl enable egida_api.service

Запуск модуля путём выполнения следующей команды: systemctl start egida_ api.service

Проверка статуса модуля путём выполнения следующей команды: systemctl status egida_ api.service

5.2.1 Установка и настройка компонента ACMS

Начальные требования

1. Установлен ASP.NET Core runtime 6-ой мажорной и наиболее высокой минорной версии на момент установки
2. В СУБД создан пользователь для компонента (например **egida_acms_user**) и известны параметры для его подключения (имя, пароль, параметры целевого экземпляра СУБД)
3. Созданы необходимые БД в СУБД, упоминаемой в пункте *2*
    - база данных с основной конфигурацией модуля управлением доступа УРМ на основании оценки соответствия (например **egida_acms**), владельцем которой является пользователь из пункта *2*
4. В СУБД настроены политики подключения пользователя из пункта *2* к базам данных из пункта *3*
5. Определены целевые директории размещения бинарных файлов, файлов конфигурации и логов

Установка

Установка представляет из себя следующую последовательность шагов:

1. Копирование бинарных файлов компонента в целевую директорию и установка соответствующих прав
2. Копирование файлов конфигурации компонента в целевую директорию и установка соответствующих прав
3. Создание директории для файлов логов компонента и установка соответствующих прав
4. Актуализация параметров работы модуля *systemd* в файле конфигурации (пример находится в директории **/appendix/etc/amcs /egida_acms.service**)*:*
    a. Пользователь и группа, под которыми должен работать модуль компонента (параметры **User** и **Group** соответственно)
    b. Рабочая директория должна быть установлена в директорию, упоминаемой в шаге *1* (параметр **WorkingDirectory**)
    c. Файл переменных окружения должен быть установлен в соответствии с расположением в директории, упоминаемой на шаге *2* (параметр **EnvrionmentFile**)

5. Актуализация параметров, хранящихся в файле переменных окружения для модуля *systemd* (пример находится в директории **/appendix/etc/amcs /egida_acms.env**)
    a. Параметры подключения к БД, содержащей основную конфигурации системы (параметр **Persistence__ConnectionStrrings__main**)
    b. Параметры путей файлов логирования, в частности путь и имя файла внутреннего логирования и корневой директории файлов логов компонента, упоминаемой в шаге *3*, и (параметры **NLog__internalLogFile** и **NLog__variables__logDirectory** соответственно)
    Примечание: файл внутреннего логирования рекомендуется держать в директории логов компонента, хотя это и не обязательно
6. Конфигурация *systemd*

- Создание файла-ссылки с настройкой модуля в systemd в директории /etc/systemd/system/
  Сделать это можно при помощи следующей команды
  ln -s %etc%/ acms /egida_acms.service /etc/systemd/system/ egida_acms.service
- Активация модуля путём выполнения следующей команды: systemctl daemon-reload && systemctl enable egida_ acms.service
- Запуск модуля путём выполнения следующей команды: systemctl start egida_acms.service
- Проверка статуса модуля путём выполнения следующей команды: systemctl status egida_ acms.service

5.2.2 Установка и настройка компонента Orchestratrion service

Начальные требования

1. Установлен ASP.NET Core runtime 6-ой мажорной и наиболее высокой минорной версии на момент установки
2. В СУБД создан пользователь для компонента (например **egida_orcherstration_user**) и известны его параметры (имя, пароль, параметры целевого экземпляра СУБД)
3. Созданы необходимые БД в СУБД, упоминаемой в пункте *2*
    - база данных с основной конфигурацией системы (например **egida_global**), с доступом на чтение и запись для пользователя из пункта *2*
    - база данных, содержащей отчёты оценки соответствия (например **egida_reports**), с доступом на чтение и запись для пользователя из пункта *2*
    - база данных, содержащей внутренние объекты компонента (например **egida_orchestration**), владельцем которой является пользователь из пункта *2*
4. В СУБД настроены политики подключения пользователя из пункта *2* к базам данных из пункта *3*
5. Определены целевые директории размещения бинарных файлов, файлов конфигурации и логов
6. Определена директория для размещения вложений, сохраняемых в системе при помощи веб интерфейса управления

Установка

Установка представляет из себя следующую последовательность шагов:

7. Копирование бинарных файлов компонента в целевую директорию и установка соответствующих прав
8. Копирование файлов конфигурации компонента в целевую директорию и установка соответствующих прав
9. Создание директории для файлов логов компонента и установка соответствующих прав
10. Актуализация параметров работы модуля *systemd* в файле конфигурации (пример находится в директории **/appendix/etc/ orchestration/egida_orchestration.service**)*:*
    a. Пользователь и группа, под которыми должен работать модуль компонента (параметры **User** и **Group** соответственно)

b. Рабочая директория должна быть установлена в директорию, упоминаемой в шаге *1* (параметр **WorkingDirectory**)
c. Файл переменных окружения должен быть установлен в соотвествии с расположением в директории, упоминаемой на шаге *2* (параметр **EnvrionmentFile**)

11. Актуализация параметров, хранящихся в файле переменных окружения для модуля *systemd* (пример находится в директории **/appendix/etc/orchestration/egida_orchestration.env**)
    a. Параметры подключения к БД, содержащей основную конфигурации системы (параметр **ConnectionStrings__global**)
    b. Параметры подключения к БД, содержащей отчёты оценки соответствия (параметр **ConnectionStrrings__reports**)
    c. Параметры подключения к БД, содержащей внутренние объекты службы оркестрации (параметр **ConnectionStrings__orchestration**)
    d. Параметры путей файлов логирования, в частности путь и имя файла внутреннего логирования и корневой директории файлов логов компонента, упоминаемой в шаге *3*, и (параметры **NLog__internalLogFile** и **NLog__variables__logDirectory** соответственно)
    Примечание: файл внутреннего логирования рекомендуется держать в директории логов компонента, хотя это и не обязательно
12. Конфигурация *systemd*
    a. Создание файла-ссылки с настройкой модуля в *systemd* в директории **/etc/systemd/system/**
    Сделать это можно при помощи следующей команды
    ln -s %etc%/ orchestration /egida_orchestration.service /etc/systemd/system/ egida_orchestration.service
    b. Активация модуля путём выполнения следующей команды:
    systemctl daemon-reload && systemctl enable egida_orchestration.service
    c. Запуск модуля путём выполнения следующей команды:
    systemctl start egida_orchestration.service

5.2.3 Конфигурация веб сервера для функционала API Gateway по маршрутизации запросов к компонентам системы (nginx)

Начальные требования

1. Установлен nginx последней стабильной версии
2. Выделена корневая директория для хранения файлов конфигураций (**%etc%**)
3. Согласован формат обращения к веб приложению (будет ли выделено ли отдельное DNS имя, будет ли использован TLS сертификат для защиты данных в транзите)
4. Развёрнуты компоненты API и ACMS и известны эндпоинты для взаимодействия с ними

Конфигурация

Конфигурация веб сервера представляет из себя выполнение следующих шагов:

- Копирование файлов конфигурации nginx в директорию **%etc%/nginx/egida_api**
- Установка прав на чтение для директории **%etc%/nginx/** группе **www-data**
- **Актуализация эндпоинтов компонентов API и ACMS в файле %etc%/nginx/egida_api. egida_api_backends.conf**
- В случае, если для API был выделен отдельное DNS имя (например api.**egida.contoso.com**), необходимо актуализировать в файле **%etc%/nginx/egida_api** параметр server_name. Например: server_name api.egida.contoso.com;
- Актуализация путей сохранения фалов логов доступа сервера nginx в параметрах **access_log** и **error_log**
- Создание файла-ссылки для импорта конфигурации веб-сервера для проксироваия запросов API к приложениям. Сделать это можно при помощи следующей команды ln -s %etc%/nginx/egida_api/egida_api_gateway.conf /etc/nginx/sites-enabled/egida_spa.conf
- Применение конфигурации веб-сервера nginx Сделать это можно при помощи следующей команды /sbin/nginx –s reload

5.2.4 Конфигурация веб сервера для предоставления файлов веб приложения (nginx)

Начальные требования

- Установлен nginx последней стабильной версии
- Выделена корневая директория для хранения файлов конфигураций (**%etc%**)
- Выделена корневая директория для хранения файлов, связанных с управлением системой через веб браузер (**%varwww-spa%**)
- Согласован формат обращения к веб приложению (будет ли выделено ли отдельное DNS имя, будет ли использован TLS сертификат для защиты данных в транзите)
- Сконфигурирован API Gateway для маршрутизации запросов к компонентам системы

Конфигурация

Конфигурация веб сервера представляет из себя выполнение следующих шагов:

1. Копирование файлов, связанных с управлением системой через веб браузер в директорию **%varwww-spa%**
2. Установка прав для директории **%varwww-spa%** прав для чтения группе **www-data**
   Сделать это можно при помощи следующей команды:
   chown -R root:www-data **%varwww-spa%** && chmod find **%varwww-spa%** . -type f -exec chmod 644 {} + && find **%varwww-spa%** -type d -exec chmod 755 {} +
3. Копирование файлов конфигурации nginx в директорию **%etc%/nginx/**
4. Установка прав для директории **%etc%/nginx/** для чтения для группы **www-data**
5. Установка корня директории предоставляемых файлов (параметр root) на директорию **%varwww-spa%**
   Пример: root /opt/egida/varwww/spa;
6. В случае, если для веб интерфейса программного комплекса было выделено отдельное DNS имя (например egida.contoso.com), необходимо переопределить имя виртуального сервера в файле **%etc%/nginx/egida_spa.conf** (имя параметра **server_name**).
   Пример: server_name egida.contoso.com;
7. Актуализация адресов приложений API для осуществления функции обратного проксирования запросов на API
   - В сегменте **location /api/** в свойство **proxy_pass** необходимо выставить схему и адрес развёртывания API. Например:

location /api/ {

proxy_pass https://api-egida.contoso.com;

}

- В сегменте **location /odata/** в свойство **proxy_pass** необходимо выставить схему и адрес развёртывания API. Например:

  location /odata/ {

  proxy_pass https://api-egida.contoso.com;

  }

8. Создание файла-ссылки для импорта конфигурации веб-сервера для передачи статических файлов и проксироваия запросов API к приложениям.

   Сделать это можно при помощи следующей команды

   ln -s %etc%/nginx/egida_spa.conf /etc/nginx/sites-enabled/egida_spa.conf

9. Применение конфигурации веб-сервера nginx

   Сделать это можно при помощи следующей команды

   /sbin/nginx –s reload