2024

Система Эгида-Аргус

Инструкция по эксплуатации

ООО «ИнфоЗонт»
https://infozont-group.ru
+7 (962) 577-24-67

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(Эгида-Аргус)
СА – Системный администратор
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

Содержание

Оглавление

Система Эгида и модуль Эгида-Аргус....1
Инструкция по эксплуатации....1
Обозначения и сокращения....2
Содержание....2
1. Введение....4
1.1. Область применения....4
1.2. Краткое описание возможностей....4
1.3. Состав и квалификация персонала подсистемы....4
1.4. Общее описание подсистемы....5
1.4.1. Комплекс управления средствами оценки состояния....5
1.4.2. Комплекс оценки состояния....6
2. Администрирование подсистемы....7
2.1. Модель администрирования....7
2.2. Периодические работы, выполняемые СА....7
2.2.1. Проведение процедуры резервного копирования конфигурационных файлов оборудования....8
2.3. Периодические работы, выполняемые АБИ....8
2.3.1 Подготовка и сохранение резервных копий данных, их периодическая проверка и уничтожение....9
2.3.2 Периодическое практическое тестирование защищенности системы....10
2.4. Непериодические работы, выполняемые СА....11
2.4.1. Первоначальная настройка Эгида-Аргус, внесение изменений в настройки, настройка групп УРМ, настройка подключений к точкам управления....11
2.4.1.1. Настройка УРМ....11
2.4.1.2. Заведение УРМ....14
2.4.1.3. Заведение агента ACMS....14
2.4.1.4. Конфигурирование подключения к точке управления траффиком (ACMS)....14
2.4.1.4. Управление доступом УРМ....16
2.4.1.5. Создание Групп УРМ....17
2.4.2. Документирование произведенных настроек....18
2.4.3. Проведение проверок актуальности документации....18
2.4.4. Восстановление работоспособности....18
2.4.5. Редактирование правил и групп доступа....18
2.4.6. Управление разрешениями УРМ....22
2.4.7. Управления ролями и полномочиями пользователей....22
2.4. Непериодические работы, выполняемые АБИ....24

2.4.1. Поддержание системы в рамках утвержденной политики безопасности 24
2.4.2. Создание и поддержание в актуальном состоянии пользовательских учётных записей.....25
2.4.3. Отслеживание информации об уязвимостях системы и своевременное принятие мер.....25

1. Введение

1.1. Область применения

Данное руководство предназначено для администраторов подсистемы оценки состояния Эгида-Аргус (далее – ПОС).

Руководство содержит в себе перечень сведений и действий, необходимых для установки, настройки и эксплуатации комплексов ПОС (Эгида-Аргус).

1.2. Краткое описание возможностей

1. Проведение процедуры оценки состояния УРМ в соответствии с установленными требованиями корпоративной политики ИБ;

2. Выявление нарушений (несоответствий требованиям установленной корпоративной политики ИБ) на устройствах пользователей защищенного удаленного доступа (УРМ);

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

4. Уведомление пользователей и администраторов о нарушениях, выявленных в рамках прохождения процедуры оценки состояния.

1.3. Состав и квалификация персонала подсистемы

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

1.4. Общее описание подсистемы

ПОС Эгида-Аргус включает в свой состав следующие комплексы:

1. Комплекс управления средствами оценки состояния;
2. Комплекс оценки состояния;

1.4.1. Комплекс управления средствами оценки состояния

Комплекс управления средствами оценки состояния предназначен для:

1. Предоставления возможности настройки проверок, выполняемых на УРМ в рамках процедуры оценки состояния оборудования пользователей УРМ;
2. Предоставления возможности просмотра статуса выполнения оценки состояния устройств в интерфейсе управления средств оценки состояния;
3. Предоставления возможности настройки правил МЭ на шлюзе удаленного доступа ПЗУД для ограничения/разрешения доступа к ресурсам корпоративной сети, пользователям, проходящим процедуру оценки состояния;
4. Предоставления возможности создания пользовательских скриптов, выполняемых на удаленных машинах пользователей, производящих процедуру оценки состояния;
5. 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).
6. 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:

1. Сервер управления ИнфоЗонт Эгида Аргус (далее – Сервер управления);
2. Сервер СУБД PostgreSQL (далее – Сервер СУБД).

1.4.2. Комплекс оценки состояния

Комплекс оценки состояния выполняет следующие функции:

1. Осуществление автоматизированной проверки соответствия фактической конфигурации УРМ целевой конфигурации установленным в политиках ИБ;

2. Принятие решений и управление доступом УРМ ко внутренней (доверенной) сети;

3. Предоставление возможности исправления конфигурации УРМ в автоматизированном режиме;

4. Ограничение доступа в инфраструктуру для УРМ, не соответствующих требованиям установленной политики ИБ;

5. Регистрация событий, связанных с прохождением оценки соответствия УРМ;

Комплекс оценки состояния состоит из следующих компонентов:

1. Агент оценки состояния ИнфоЗонт Эгида Аргус (далее – Агент оценки состояния);

2. Оркестратор агентов ИнфоЗонт Эгида Аргус (далее – Оркестратор);

3. Агент управления конфигурациями ИнфоЗонт Эгида Аргус (далее – Агент управления конфигурациями);

4. Брокер ИнфоЗонт Эгида Аргус (далее – Брокер);

2. Администрирование подсистемы

2.1. Модель администрирования

Модель администрирования ПОС Эгида-Аргус предполагает наличие двух выделенных ролей администраторов:

1. Системный администратора (далее – СА);
2. Администратор безопасности информации (далее – АБИ);

Работы, выполняемые при администрировании подсистемы, подразделяются на следующие:

1. Периодические работы;
2. Непериодические работы;

2.2. Периодические работы, выполняемые СА

Периодические работы по администрированию ПОС Эгида-Аргус, выполняемые СА, приведены в таблице ниже (Таблица 4.1).

Таблица 4.1 – Периодические работы по администрированию ПОС Эгида-Аргус, выполняемые СА

№ п/п	**Описание обязанностей**	**Периодичность**	**Пункт описания**
	Проведение процедуры резервного копирования конфигурационных файлов оборудования	Еженедельно	2.2.1

2.2.1. 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

2.3. Периодические работы, выполняемые АБИ

Периодические работы по администрированию ПОС Эгида-Аргус, выполняемые АБИ, приведены в таблице ниже (Таблица 4.2).

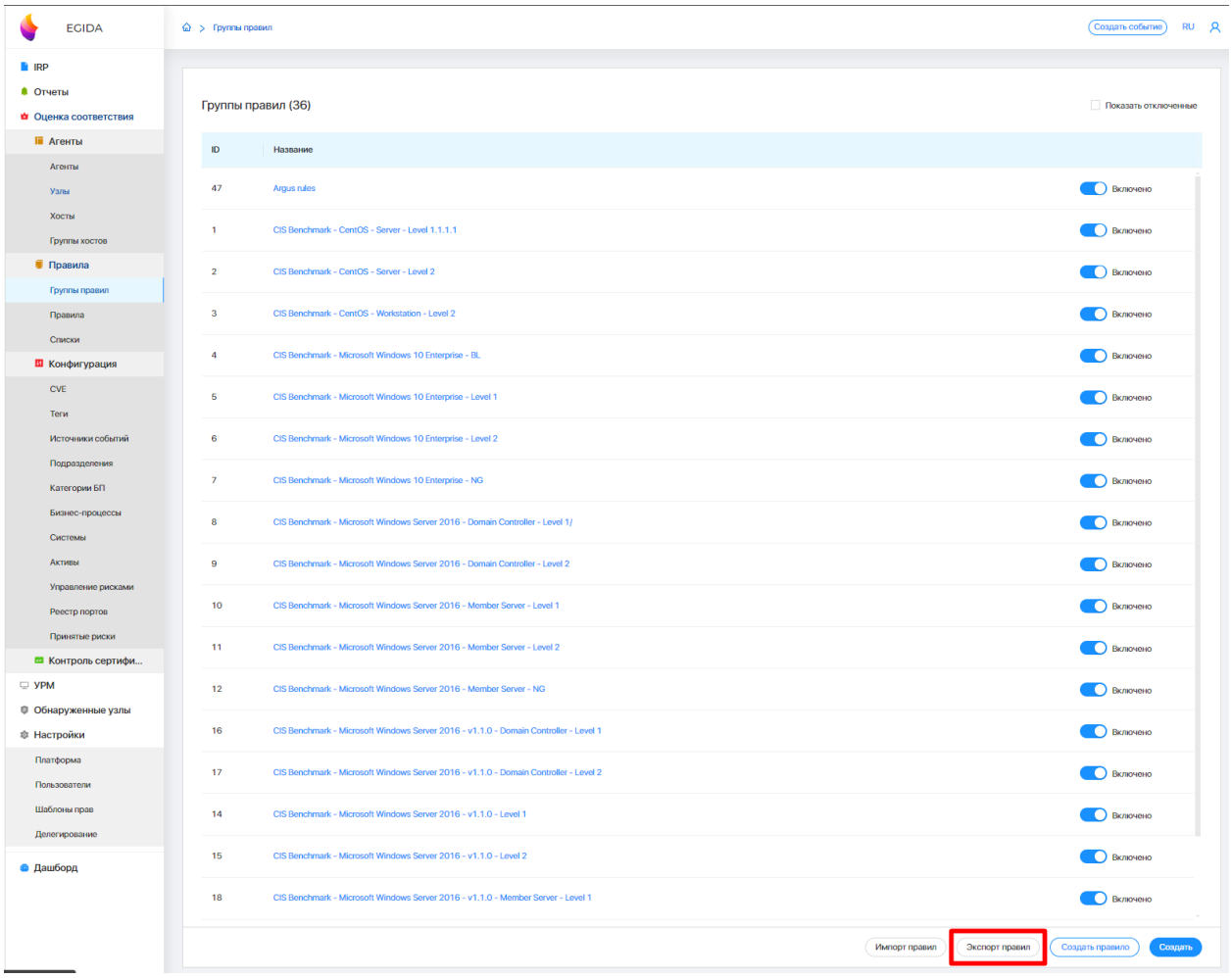
Таблица 4.2 – Периодические работы по администрированию ПОС Эгида-Аргус, выполняемые АБИ

№ п/п	Описание обязанностей	Периодичность	Пункт описания
1	Подготовка и сохранение резервных копий данных, их периодическая проверка и уничтожение;	ежеквартально	2.3.1
2	Периодическое практическое тестирование защищенности системы	ежегодно	2.3.2

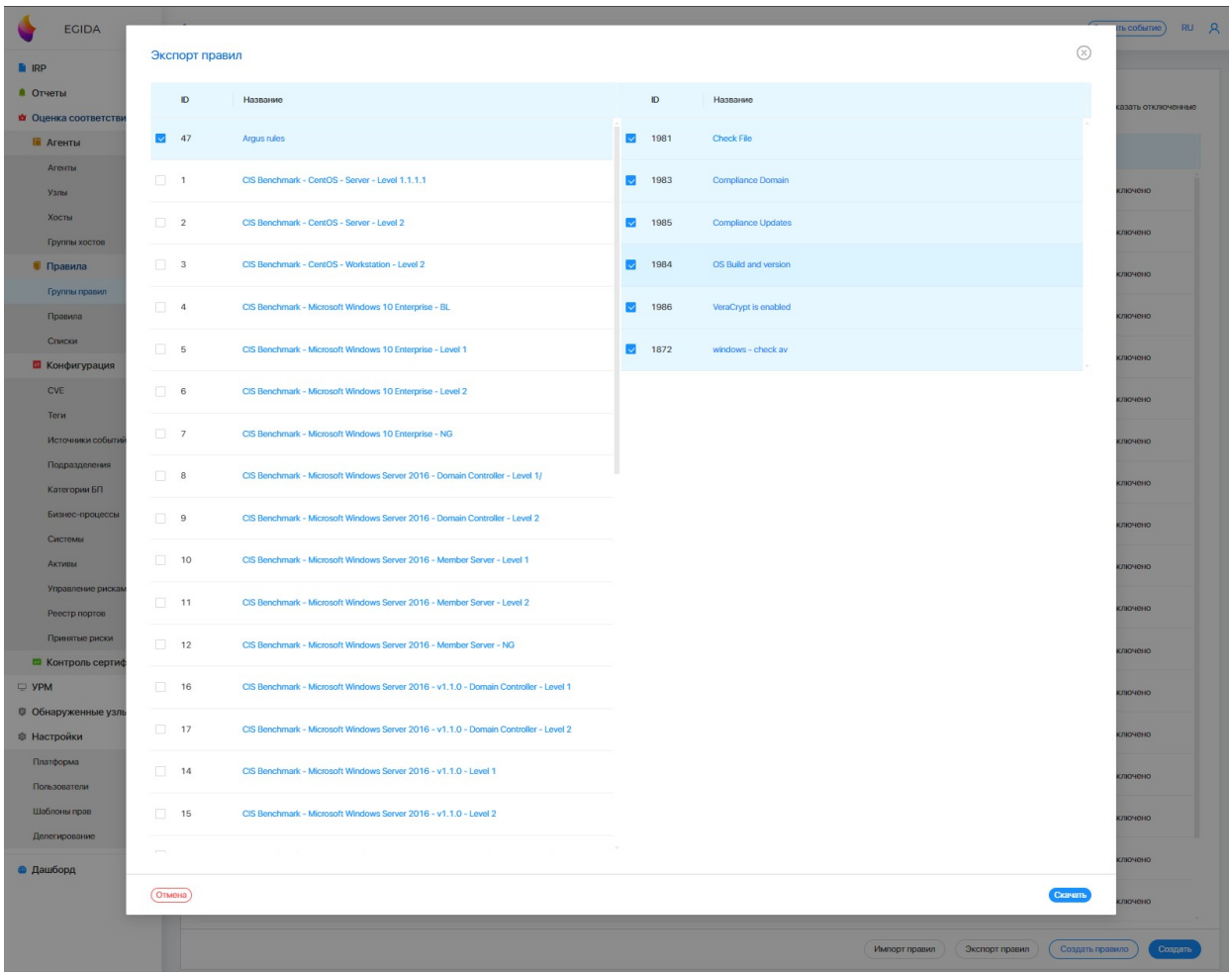
2.3.1 Подготовка и сохранение резервных копий данных, их периодическая проверка и уничтожение

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

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



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.



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.

2.3.2 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 соответствует установленной политике.

2.4. Непериодические работы, выполняемые СА

Непериодические работы по администрированию ПОС Эгида-Аргус, выполняемые СА, приведены в таблице ниже (Таблица 4.3).

Таблица 4.3 – Непериодические работы по администрированию ПОС Эгида-Аргус, выполняемые СА

№ п/п	**Описание обязанностей**	**Пункт описания**
1	2	3
1.	Первоначальная настройка Эгида-Аргус, внесение изменений в настройки, настройка групп УРМ, настройка подключений к точкам управления	2.4.1
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

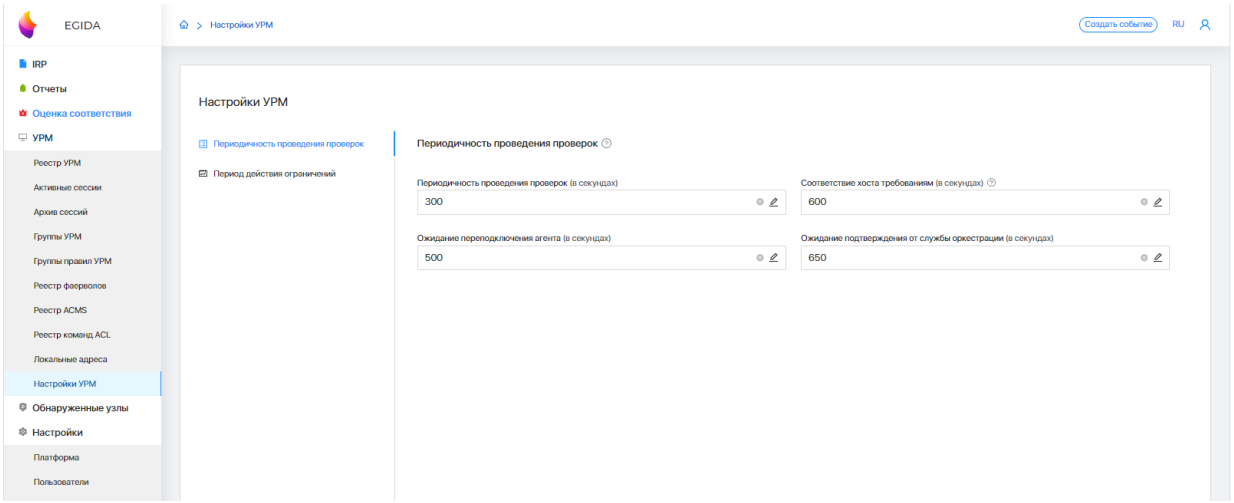
2.4.1. Первоначальная настройка Эгида-Аргус, внесение изменений в настройки, настройка групп УРМ, настройка подключений к точкам управления

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

Первоначальная настройка Эгида-Аргус включает в себя настройку работы модулей УРМ, первичное конфигурирование ПОС Эгида-Аргус и настройку подключений к точкам управления сетевым трафиком.

2.4.1.1. Настройка УРМ

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



Рекомендованные значения уже установлены по умолчанию (Рисунок 3)

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.

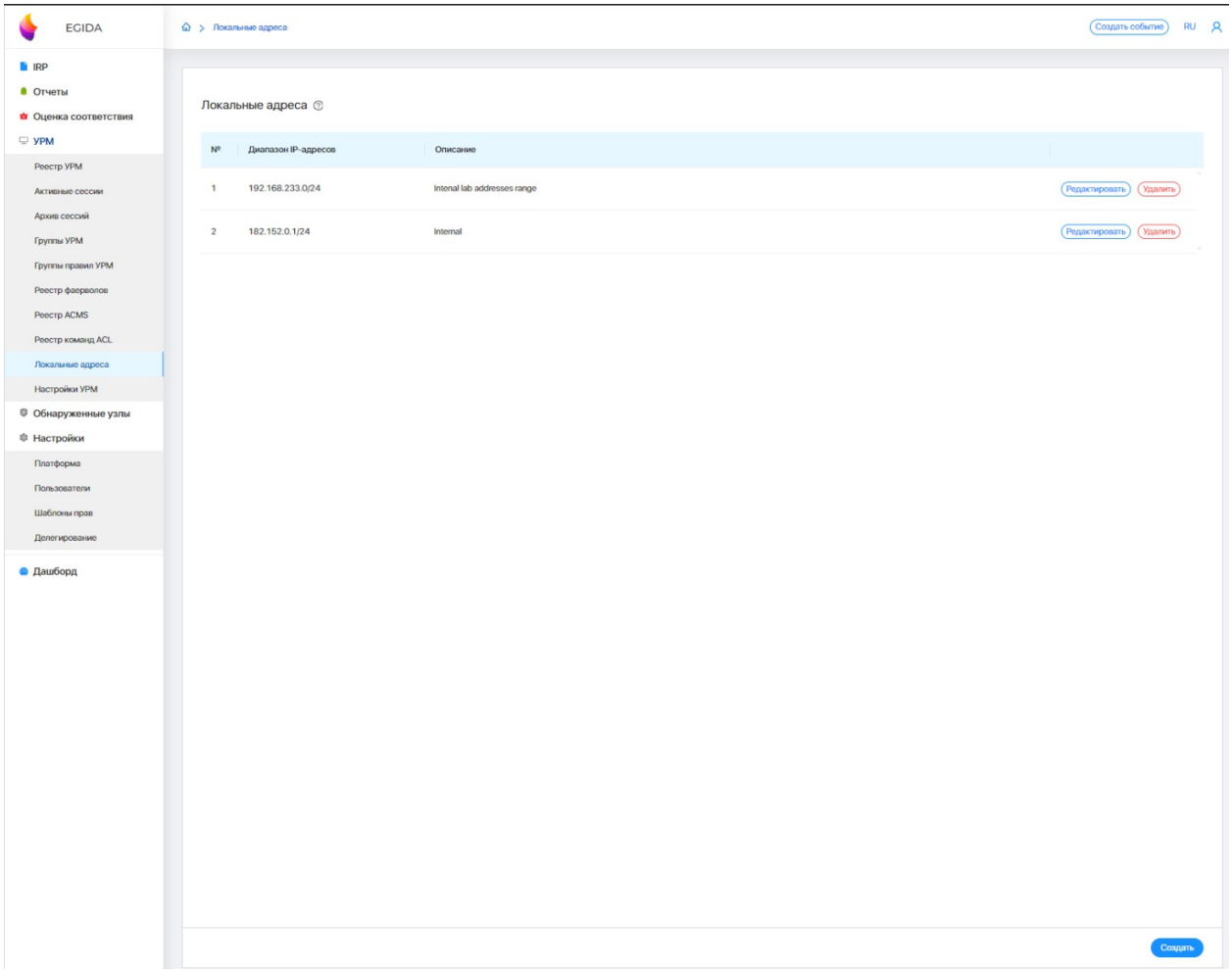


Рисунок 4 – Локальные адреса

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.

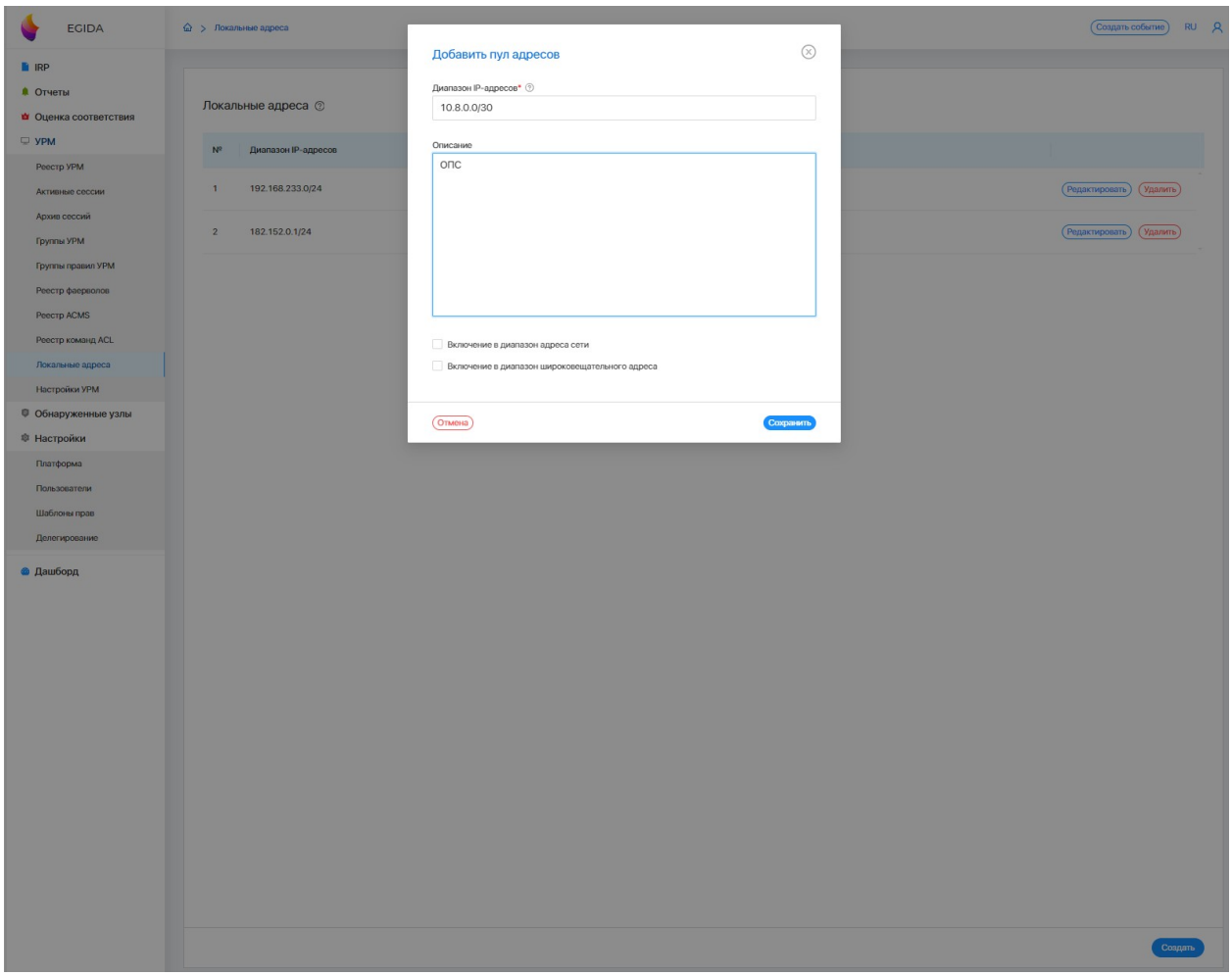


Рисунок 5 – Добавление пула адресов

Примечания:

1. Пул IP-адресов выделяемых VPN шлюзом не должен попадать в пул локальных адресов;

2. В рамках взаимодействия между VPN шлюзом и локальной сетью не должна применяться технология NAT;

3. Все подключения узла не из локальных пулов адресов рассматриваются как УРМ. В этом случае подключаемый АРМ автоматически регистрируется как устройство УРМ;

2.4.1.2. 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.

2.4.1.3. Заведение агента ACMS

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

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

2.4.1.4. 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 трафиком.

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

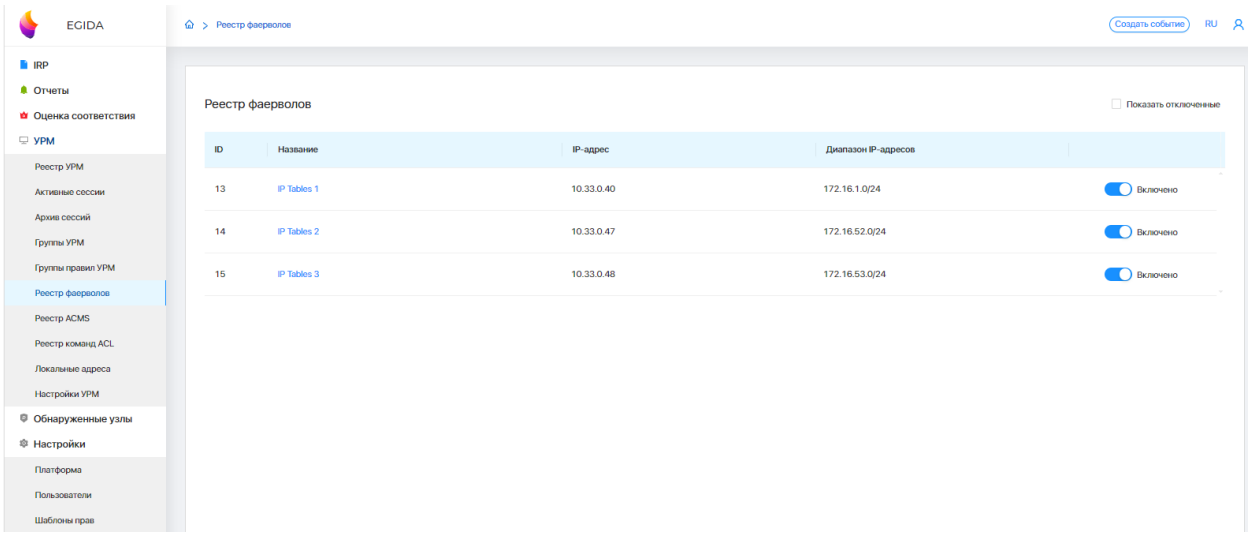


Рисунок 6 – Реестр фаерволов

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 трафиком.
Скрипт необходим на случай восстановления состояния из-за перебоев и/или потери связи с точкой управления или ACMS.

Для корректного заведения точки управления трафиком обязательным является назначение ответственного ACMS для конкретной точки управления (Рисунок 7).

Один ACMS может управлять только одной точкой управления трафиком.

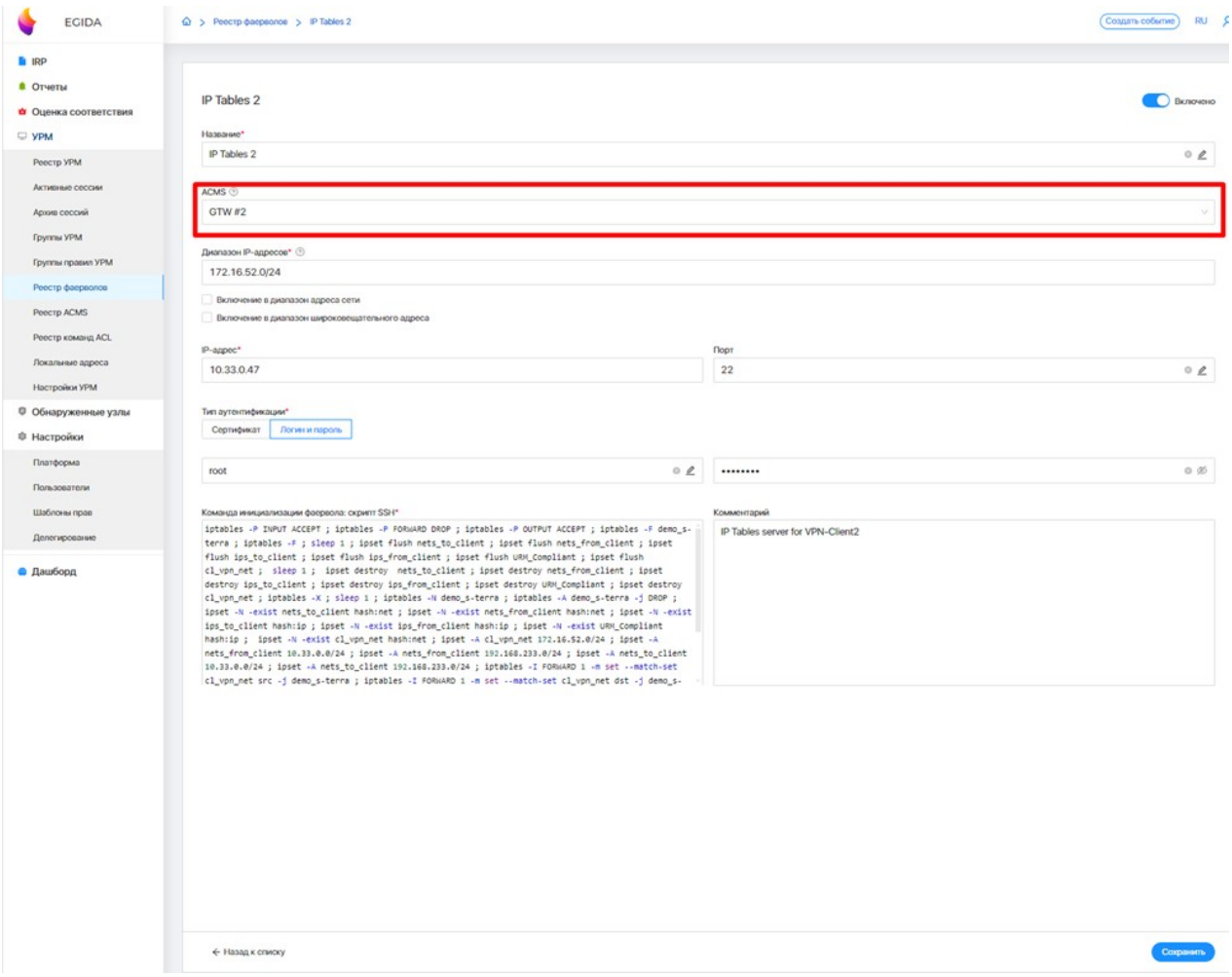


Рисунок 7 – назначение ACMS

2.4.1.4. Управление доступом УРМ

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

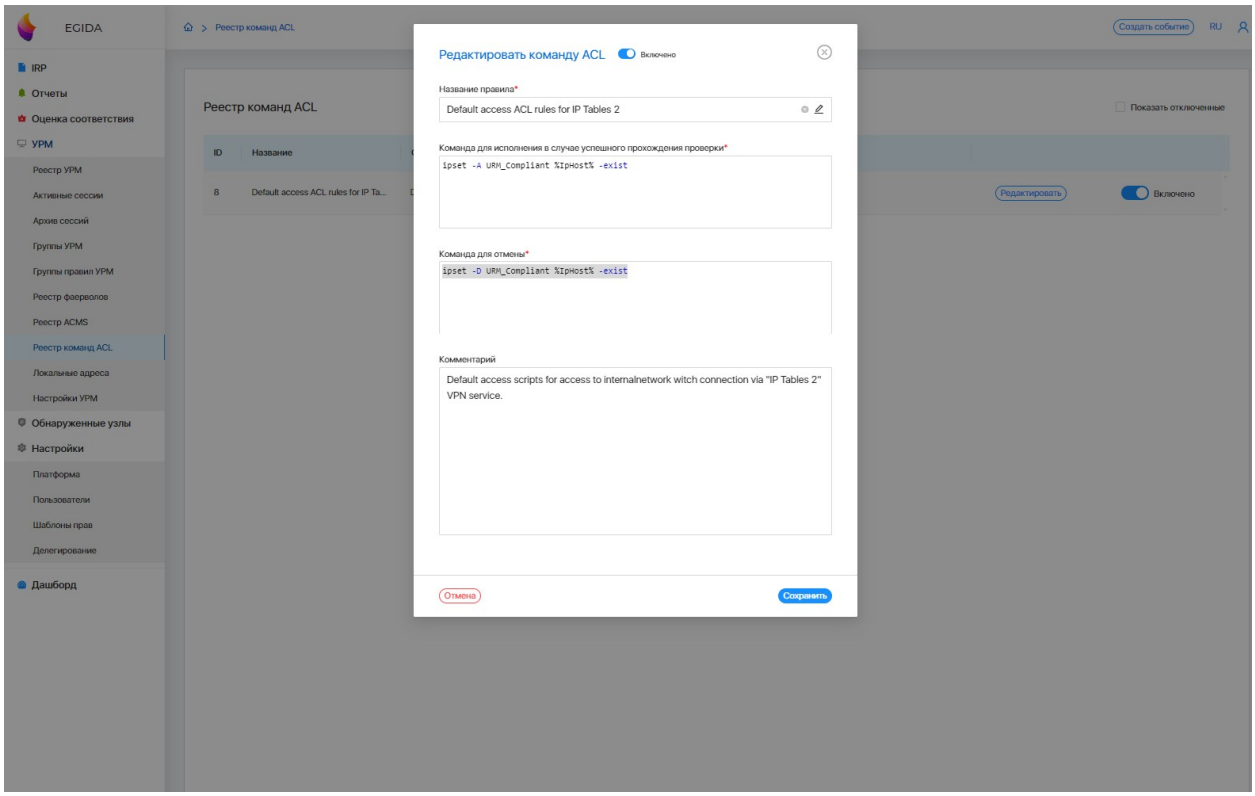


Рисунок 8 – Реестр команд ACL

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.

2.4.1.5. 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.

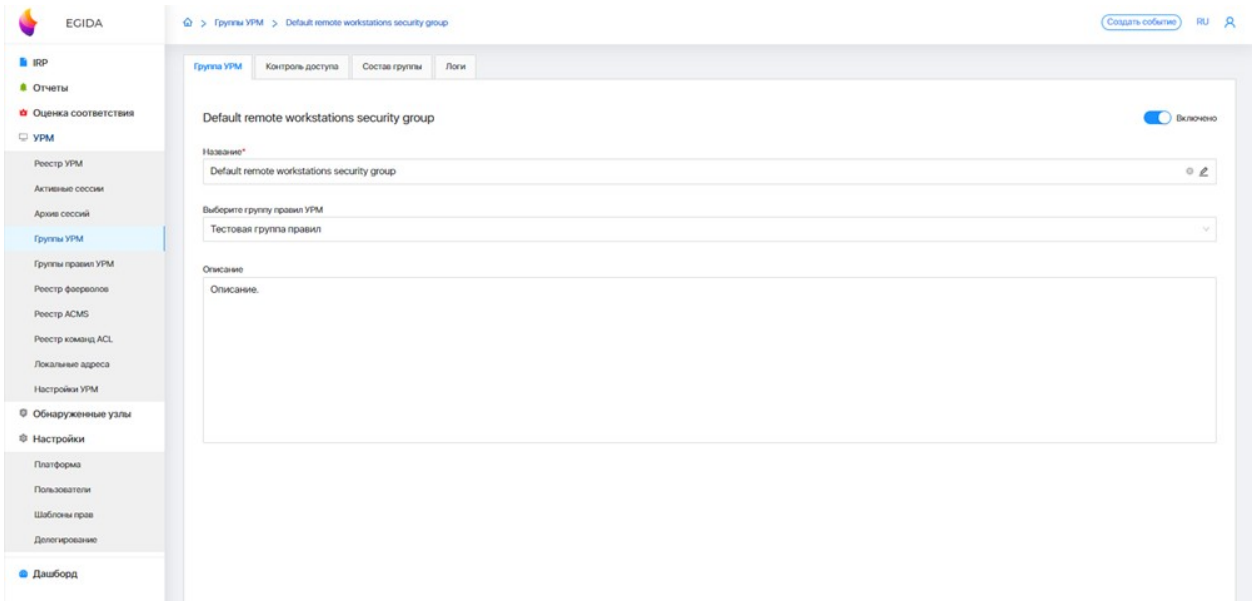


Рисунок 9 – Просмотр группы УРМ

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

1. Проверка наличия/отсутствия определённого установленного **ПО**;
2. Проверка наличия/отсутствия определённых запущенных служб;
3. Проверка наличия/отсутствия определённых значений в реестре;
4. Проверка выполнения обновления ОС (**Windows**);
5. Проверка шифрования диска (**Bitlocker**);
6. 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.

2.4.2. 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.

2.4.3. 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.

2.4.4. 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.

2.4.5. Редактирование правил и групп доступа

Процесс управления доступами описан в разделах 2.4.1.3 — 2.4.1.4.

Процедура создания пользовательских правил:

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

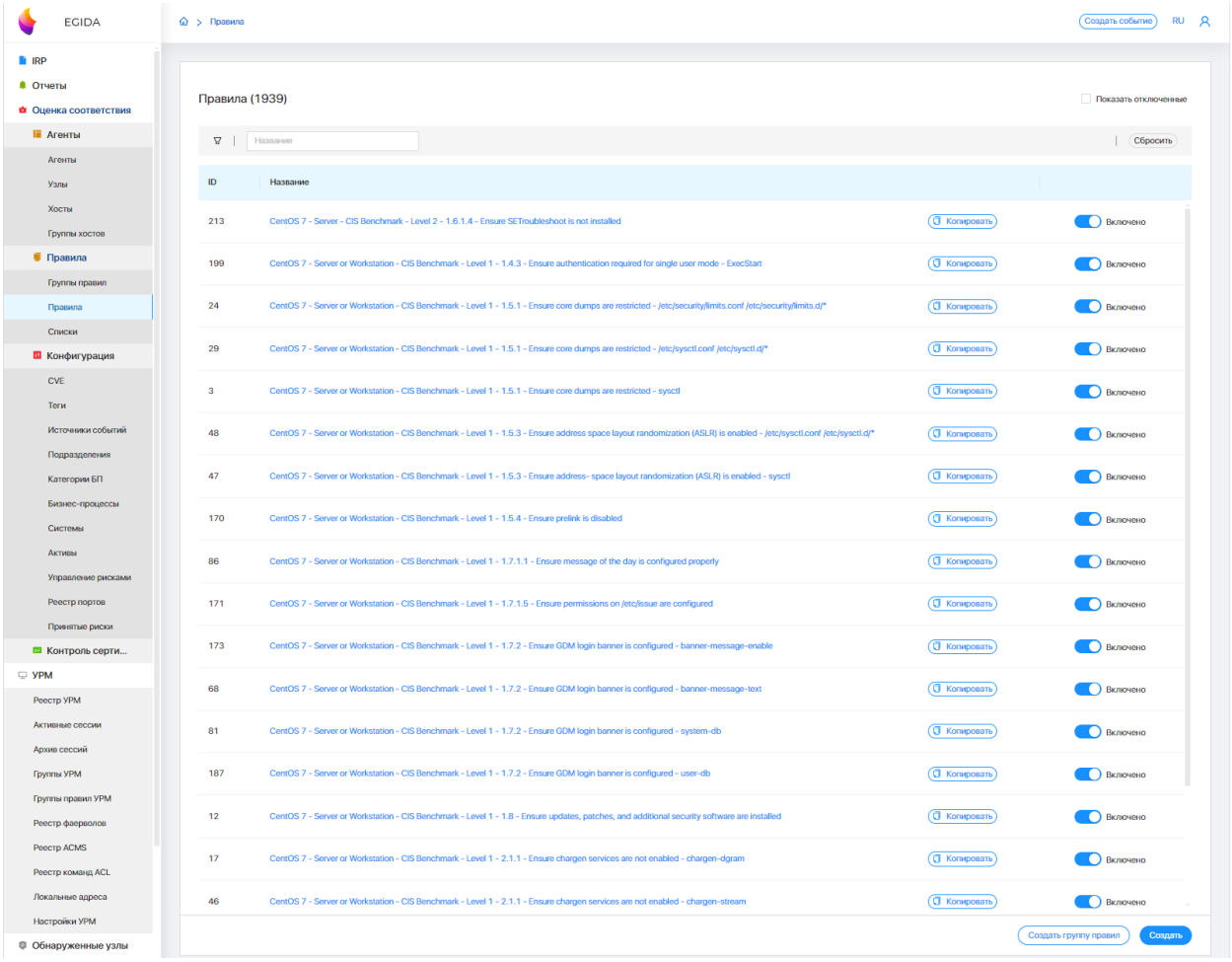


Рисунок 10 – Правила оценки соответствия

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.

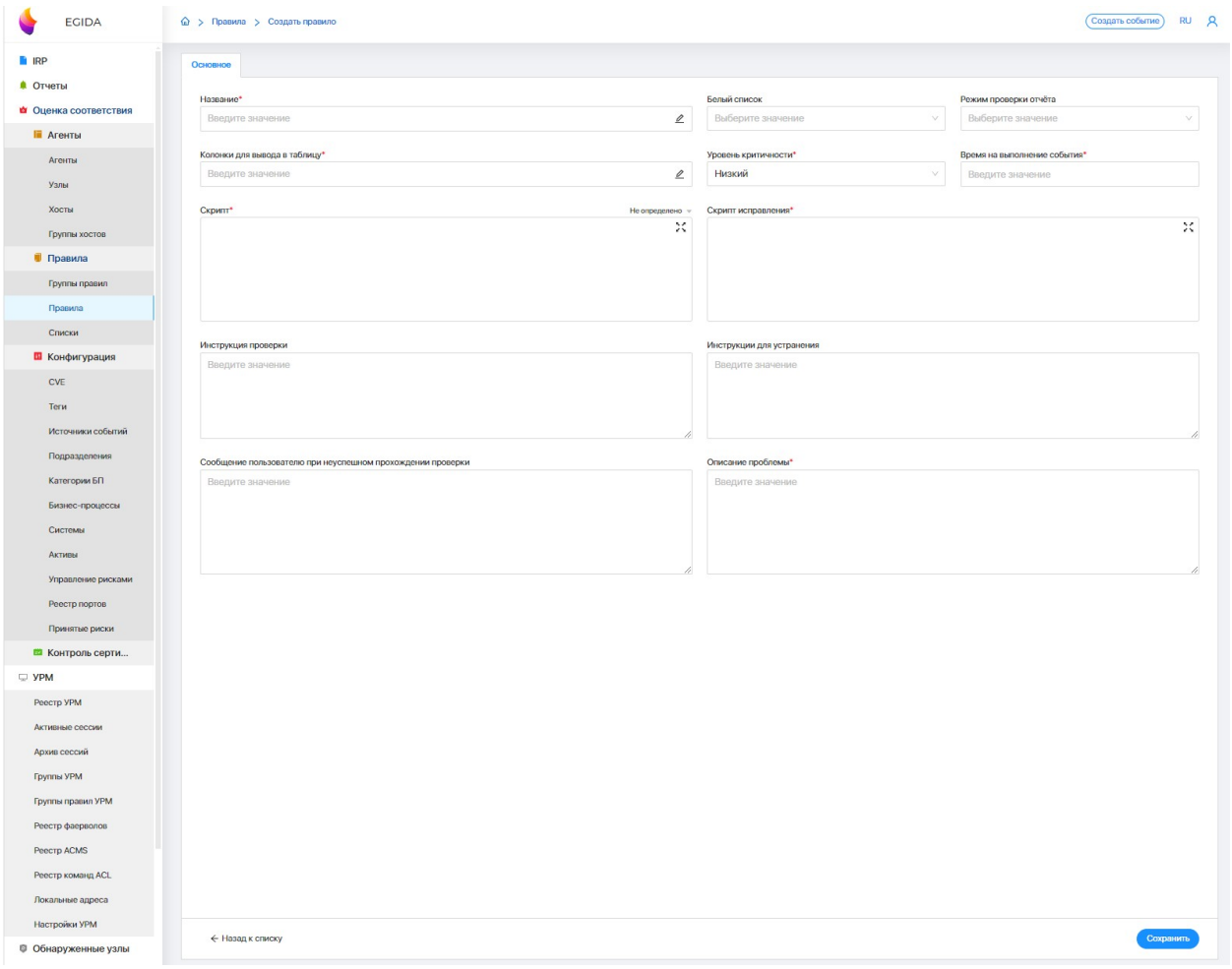


Рисунок 11 – Создание правила оценки состояния

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

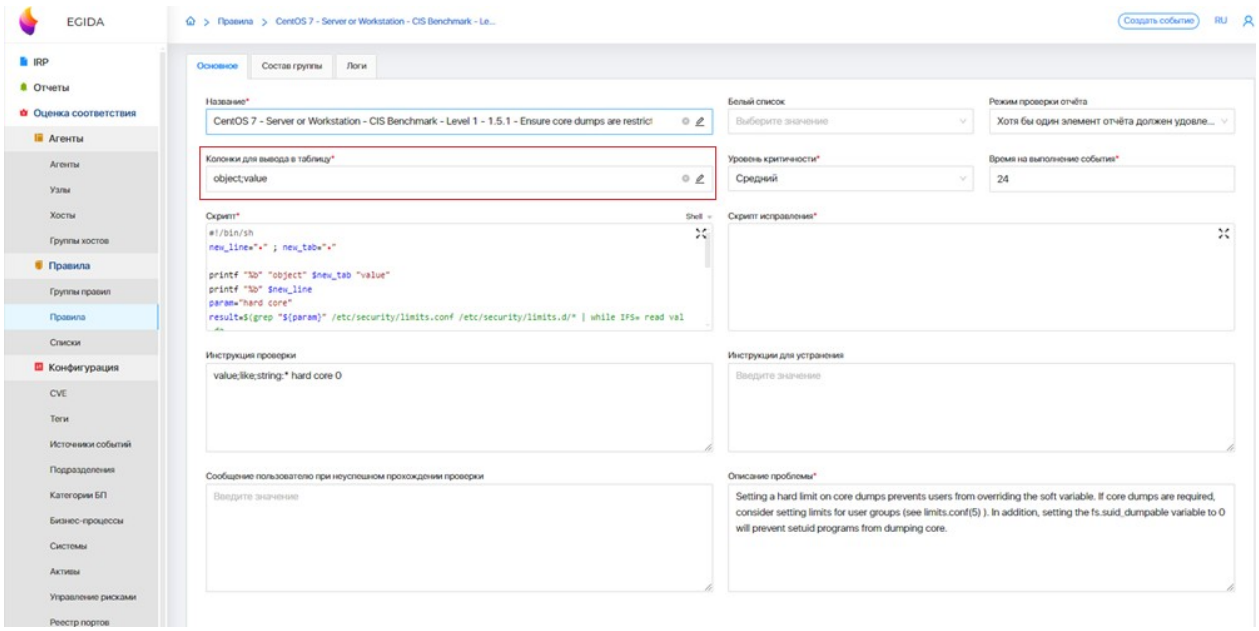


Рисунок 12 – Указание ключей для вывода в таблицу

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

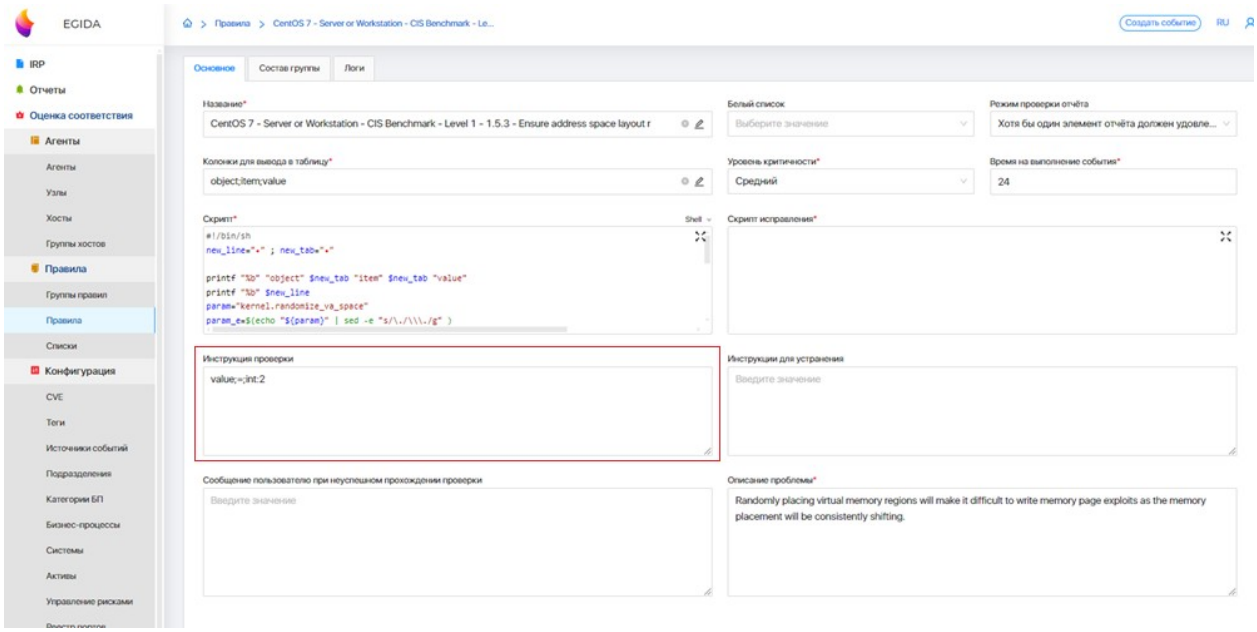


Рисунок 13 – Инструкция проверки

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.

2.4.6. 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.

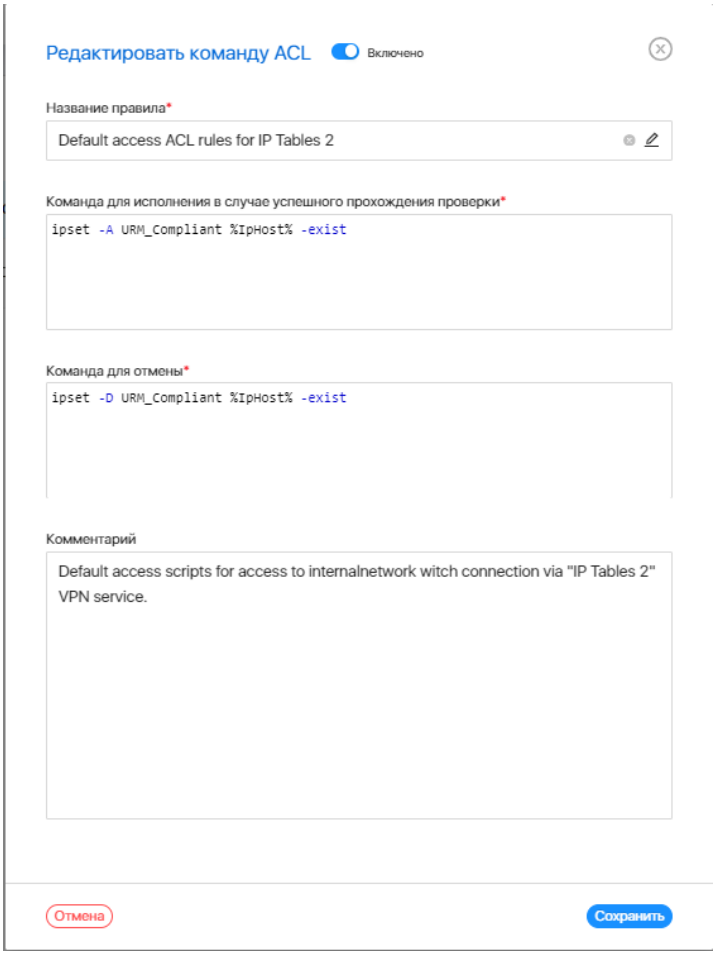


Рисунок 14 – Управление разрешениями УРМ

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

2.4.7. 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 ПОС.

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.

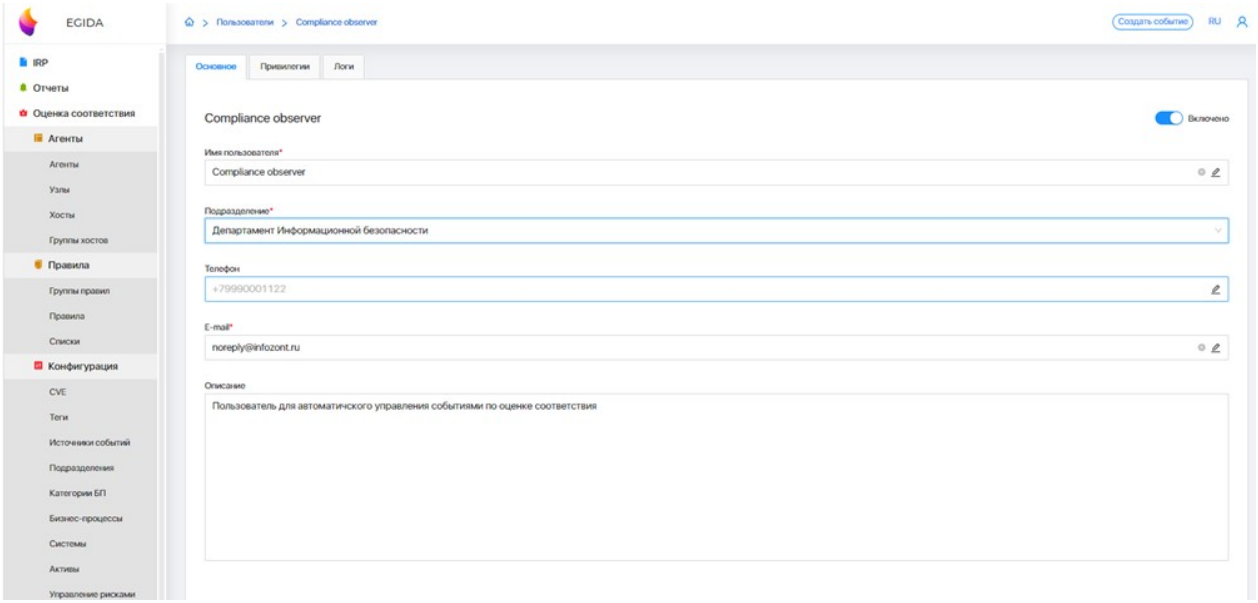


Рисунок 15 – Создание пользователя ПОС

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

1. «Пользователь УРМ» - для пользователей, которые могут осуществлять просмотр интерфейсов управления УРМ;

2. «Администратор УРМ» - для администраторов, осуществляющих управление настройками подключения к ACMS.

2.4. Непериодические работы, выполняемые АБИ

Непериодические работы по администрированию ПОС, 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	2.4.1
2.	Создание и поддержание в актуальном состоянии пользовательских учётных записей	2.4.2
3.	Отслеживание информации об уязвимостях системы и своевременное принятие мер	2.4.3

2.4.1. 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.

2.4.2. 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 ПОС Эгида-Аргус.

Управление учетными записями осуществляется в разделе веб-интерфейса ПОС Эгида-Аргус «Настройки» – «Пользователи» (см. раздел 2.4.7).

2.4.3. 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.