Система контроля сетевого доступа к ресурсам
ПУМА

Руководство пользователя

ООО «ЦРП»
2020

Оглавление

+7 (812) 339-28-14
195220, г. Санкт-Петербург, Непокоренных пр., 49А, оф. 410
contact@crplab.ru
www.crplab.ru

Введение

Настоящий документ предназначен для пользователей, осуществляющих настройку системы контроля сетевого доступа к информационным ресурсам автоматизированной информационной системы ПУМА (в дальнейшем .
В состав документа включена информация об архитектуре Системы, назначении отдельных модулей, принципах работы, а так же информация необходимая для настройки.
В **Главе 2** описана архитектура системы.
В **Главах 3 - 7** представлена информация по настройке модулей Системы.
В **Главе 8** представлена информация об ограничениях ознакомительной версии Системы.

Архитектура системы

Система построена по модульному принципу и разделена на следующие функциональные модули:

- каталог;
- управление пользователями;
- менеджер загрузки;
- центр администрирования;
- защиты АРМ;
- управления политиками доступа;
- управления межсетевыми экранами.

Модули системы

Каталог

Модуль **Каталога** обеспечивает возможность построения многоуровневой иерархической структуры Системы, обеспечивающей возможность корректного взаимодействия основных и подчиненных подразделений организации.

Управление пользователями

Модуль **Управление пользователями** обеспечивает контроль доступа в Систему.

Менеджер загрузки

Менеджер загрузки обеспечивает запуск модулей на серверах, а так же мониторинг их состояния и настройку адресов.

Центр администрирования

Центр администрирования предоставляет возможность управления системой с использованием WEB-интерфейса.

Защиты АРМ

Модуль **Защиты АРМ** обеспечивает процессы взаимодействия с автоматизированными рабочими местами пользователей (АРМ):

- Управление списком АРМ;
- настройку политик контроля;
- взаимодействие с клиентским ПО на АРМ;
- формирование управляющих сообщений для сервиса управления политиками доступа.

Управления политиками доступа

Модуль **управления политиками доступа** обеспечивает функции управления составом политик, формирование наборов правил фильтрации для МЭ, формирование управляющих сообщений сервису управления МЭ для настройки оборудования.

Управления межсетевыми экранами

Сервис управления межсетевыми экранами (МЭ) обеспечивает управление списком МЭ, взаимодействием и настройкой оборудования.

Развертывание системы

Система может быть развернута в локальном варианте, когда все модули системы расположены на одном физическом или виртуальном сервере или в виде иерархической структуры, обеспечивающей гибкость в управлении, распределении прав доступа, удобства эксплуатации.

Доступ в систему

Для доступа в систему Администратор должен

- запустить браузер. Требования к браузеру указаны ниже;
- ввести в адресной строке браузера адрес настроенный на сервер Пума. IP адрес по умолчанию: 192.168.7.1

- войти в систему используя имя пользователя и пароль. По умолчанию в систему есть пользователь со следующими данными: имя пользователя: admin, пароль: 111111.

Требования к браузеру

Система обеспечивает работу со следующими браузерами:
- Chrom;
- Yandex browser;
- Microsoft Edge;
- Firefox.

Модуль управления пользователями

Общая информация

Модуль управления пользователями обеспечивает возможность управления учетными записями администраторов системы, аутентификацию администраторов, авторизацию прав доступа к модулям системы.
По умолчанию, модуль содержит одного пользователя с именем пользователя: **admin** и паролем: **111111**. Данного пользователя нельзя удалить из системы, однако возможно переименовать.

Управление пользователями

Модуль позволяет обеспечить выполнение следующих действий:
- добавление пользователя;
- просмотр пользователя;
- редактирование пользователя;
- удаление пользователя.

Все действия по управлению пользователями осуществляются во вкладке пользователи интерфейса управления модулем.

Добавление пользователя

Для добавления пользователя Администратор должен выбрать кнопку **Добавить** и заполнить обязательные свойства: имя пользователя и пароль.
Имя пользователя служит для идентификации пользователя и должно быть уникально среди пользователей модуля.

Просмотр пользователя

Для просмотра пользователя Администратор должен выбрать соответствующего пользователя в списке пользователей. Для просмотра доступна следующая информация:

- имя пользователя.

Редактирование пользователя

Модуль позволяет обеспечить редактирование имени пользователя и его пароля. При вводе пароля необходимо обеспечить ввод подтверждения пароля, для контроля правильности ввода.

Удаление пользователя

Модуль обеспечивает возможность удаления пользователей системы, при этом пользователь установленный по умолчанию не может быть удален.

Модуль Защиты АРМ

Общая информация

Модуль **Защита автоматизированного рабочего места** (в дальнейшем **Защита АРМ**) предназначен для управления автоматизированными рабочими местами пользователей (**АРМ**), обеспечения контроля состояния их защищенности, предоставления информации о возникновении инцидентов другим модулям системы. Модуль Защита АРМ обеспечивает выполнение следующих задач:

- управление политиками контроля;
- управление группами АРМ;
- управление списком АРМ;
- управление инцидентами;
- передачу информации об АРМ и инцидентах в другие модули системы;
- формирование и отображение регистрационной информации;
- настройку параметров модуля.

Управления политиками контроля

Модуль Защиты АРМ обеспечивает контроль защищенности АРМ, при этом анализируются состав запущенных процессов на соответствие правилам, заданным в политиках контроля.

Режимы работы

Политика контроля обеспечивает хранения информации о том, какие процессы необходимо контролировать на АРМ. При контроле обеспечивается работа в следующих режимах:

- обязательные процессы;
- запрещенные процессы;
- разрешенные процессы.

Режим: Обязательные процессы

При работе в этом режиме, процессы заданные в списке при настройке режима должны быть запущены на АРМ. Если же один или несколько из процессов не запущено, будет сформирован инцидент.

Как один из примеров использования данного режима можно использовать контроль запуска на АРМ программных средств защиты информации, таких как антивирусное программное обеспечение, средства контроля доступа к USB-портам и т.д.

Режим: Запрещенные процессы

При работе в этом режиме будет сформирован инцидент если на АРМ запущен хотя бы один процесс из указанных при настройке режима.

Данный режим может быть использован для предупреждения запуска программного обеспечения легально установленного на АРМ, однако, нежелательного к использованию.

Режим: Разрешенные процессы

При работе в этом режиме будет сформирован инцидент, если на АРМ запущен хотя бы один процесс не указанный при настройке режима.

Данный режим может быть использован, когда в организации точно известен состав программных средств используемых на АРМ и не допускается запуск другого ПО.

Настройка политики контроля

При настройке политики Администратор системы задает режим работы, а так же состав контролируемых процессов.

Управление группами АРМ

Система позволяет создавать группы и в них добавлять АРМ. Группы позволяют Администратору системы задавать параметры один раз для всех элементов. К таким параметрам относится, например, Политика контроля.

Управление списком автоматизированных рабочих мест

Система позволяет Администратору управлять составом АРМ, состояние защищенности которых контролируется модулем Защиты АРМ. Доступны функции:

- добавления нового АРМ - регистрация;
- изменение параметров;
- удаление.

Управление инцидентами

Модуль Защиты АРМ, в процессе работы, формирует инциденты, связанные с нарушениями политик контроля. Обеспечивается:

- ведение перечня инцидентов
- формирование инцидента при нарушении требований политики контроля
- снятие инцидента при восстановлении состояния защищенности АРМ
- снятие инцидента по запросу Администратора

Передача информации об АРМ и инцидентах в другие модули системы

Модуль Защиты АРМ обеспечивает передачу информации об АРМ и сформированных инцидентах в другие модули. В качестве модулей, для которых требуются данные, является, например модуль Управления политиками доступа, который обеспечивает формирование политик доступа на основании информации о состоянии АРМ и инцидентах.

Формирование и отображение регистрационной информации

Модуль обеспечивает регистрацию информации о возникающих инцидентах, действиях Администратора по настройке системы, изменении состояния АРМ и т.д. Регистрационная информация передается в модуль Журанлирования для хранения и может быть получена для анализа.

Управление политиками контроля

Политика контроля задает требования к защищенности АРМ. Под защищенностью АРМ понимается состояние АРМ, при котором обеспечено соответствие требуемому составу запущенных процессов.

Режимы работы политик контроля

Для работы модуля в политике контроля должен быть задан режим работы. Допустимы следующие режимы работы:

- Обязательные процессы;
- Запрещенные процессы;

- Разрешенные процессы.

Обязательные процессы

При работе в этом режиме, процессы заданные в списке при настройке режима должны быть запущены на АРМ.

Запрещенные процессы

При работе в этом режиме будет сформирован инцидент если на АРМ запущен хотя бы один процесс из указанных при настройке режима.

Разрешенные процессы

При работе в этом режиме будет сформирован инцидент, если на АРМ запущен хотя бы один процесс не указанный при настройке режима.

При работе в данном режиме, если Администратор не задал в настройках ни одного процесса или задал небольшое их количество, возможна ситуация снижения производительности системы, т.к. на каждый процесс будет считаться инцидентом и между модулями системы будет передаваться большой объем информации.

Так для операционных систем MS Windows количество одновременно запущенных процессов составляет порядка 200 шт., соответственно при пустом списке будет сформировано соответствующее число инцидентов на каждый АРМ.

Особенности работы модуля при использовании нескольких режимов

Модуль позволяет работать при включении нескольких режимов одновременно, т.е. контролировать запуск обязательных процессов, отсутствие запрещенных и запуск не разрешенных.

Комбинирование режимов позволяет добиться повышенного уровня защищенности АРМ, однако необходимо учитывать, что некорректная настройка может привести к формированию инцидента, который будет активен всегда. Данная ситуация возможна при задании одного и того же процесса списках обязательных и запрещенных или запрещенных и разрешенных процессов.

Свойства политики контроля

При работе с политиками контроля должны быть заданы следующие свойства:

- Наименование;
- Описание;
- Режим Обязательные процессы;
- Список обязательных процессов;
- Режим Запрещенных процессы;
- Список запрещенных процессов;
- Режим Разрешенных процессы;
- Список разрешенных процессов.

Наименование

Наименование политики контроля служит для идентификации политики при администрировании модуля: редактировании политики, назначении политики на АРМ или группу и т.д.

Наименование должно быть уникальным в пределах одного модуля и не может быть пустым.

Описание

Описание политики контроля служит для хранения краткой справки о назначении политики.

Режим Обязательные процессы

Включение свойства обеспечивает работу политики в режиме Обязательных процессы.

Список обязательных процессов

Режим Запрещенных процессы

Включение свойства обеспечивает работу политики в режиме Запрещенных процессы.

Список запрещенных процессов

Режим Разрешенных процессы

Включение свойства обеспечивает работу политики в режиме Разрешенных процессы.

Список разрешенных процессов

Управление политиками

Управление политиками контроля осуществляется во вкладке Политики интерфейса управления модуля Защиты АРМ.

Вкладка разбита на следующие части:

- список политик;
- управление выбранной политикой.

Администратору доступны следующие действия:

- добавление политики контроля;
- просмотр политики контроля;
- редактирование политики контроля;
- удаление политики контроля.

Добавление политики контроля

Для добавления политики контроля Администратор должен выбрать кнопку **+** (Добавить), расположенную над списком политик.

При добавлении обязательно должно быть задано наименование политики, иначе она не будет сохранена. Необходимо учитывать, что значение данного свойства должно быть уникально.

Дальнейшие действия Администратора могут быть выполнены как на этапе создания, так и при редактировании политики.

Администратор может задать режимы работы и заполнить списки процессов.

Подробная информация о выполнении этих действий доступна в разделе Редактирование политики доступа.

Для сохранения политики Администратор должен выбрать кнопку сохранить, расположенную в правом верхнем углу окна.

Если Администратор решил отказаться от создания политики он имеет возможность в любой момент выбрать кнопку Отмена.

Просмотр политики контроля

Для просмотра политики контроля Администратор должен выбрать политику в окне списка контроля.

Редактирование политики контроля

Для редактирования политики доступа Администратор должен перейти к просмотру политики и выбрать кнопку Редактировать.

При редактировании Администратор имеет возможность изменить все свойства политики.

Редактирование списка процессов

При редактировании списка процессов Администратор может

- добавить процесс
- удалить процесс
- импортировать список процессов
- экспортировать список процессов

Для добавления процесса в список необходимо в поле **Укажите процессы** вбить имя процесса и нажать кнопку Ввод.

Для удаления процесса из списка необходимо найти требуемый процесс и выбрать в соответствующей строке кнопку удалить.

Для импорта списка процессов необходимо выбрать кнопку **Импортировать список процессов**, выбрать файл, содержащий список процессов, выбрать кнопку **ОК**.

Для экспорта списка процессов необходимо выбрать кнопку **Экспортировать список процессов**, задать имя файла, выбрать кнопку ОК.

Удаление политики контроля

Для удаления политики доступа Администратор должен перейти к просмотру политики и выбрать кнопку **Удалить**.

Политика, назначенная на АРМ или группу, не может быть удалена.

Управление группами АРМ

Модуль позволяет создавать группы и задавать принадлежность АРМ к группе, что позволяет:

- упростить администрирование за счет визуальной группировки АРМ;
- задавать параметры не для каждого АРМ, а для всех АРМ группы.

При регистрации нового АРМ в системе, АРМ автоматически добавляется в группу по умолчанию. Выбор группы по умолчанию осуществляется в настройках модуля.

Свойства групп

Для группы можно задать следующие свойства:

- наименование;
- описание;
- политику контроля.

Наименование

Наименование служит для идентификации группы в процессе администрирования

Описание

Описание позволяет задать произвольную текстовую информацию, которая может помочь в дальнейшем Администратору.

Политика контроля

Политика контроля позволяет задать политику контроля для всех АРМ входящих в группу.

Действия над группами

Модуль позволяет производить следующие действия:

- добавление группы;
- просмотр группы;
- редактирование группы;
- удаление группы.

Добавление группы

Для добавления группы Администратор должен выбрать кнопку **+** (**Добавить**), расположенную над списком групп.
При создании, необходимо указать наименование группы, если его не задать, то группу создать не удастся.
Так же на данном шаге можно задать описание и выбрать из выпадающего списка политику контроля.

Просмотр группы

Для просмотра группы Администратор должен выбрать в списке групп соответствующее наименование.
Будет отражена следующая информация:

- наименование;
- описание;
- является ли группа, группой по умолчанию;
- привязанная к группе политика;
- список АР/М входящих в состав группы.

Редактирование группы

Для редактирования группы Администратор должен перейти к просмотру группы и выбрать кнопку **Редактировать**.

Удаление группы

Для удаления группы Администратор должен перейти к просмотру группы и выбрать кнопку **Удалить**.
Группа, выбранная в настройках модуля в качестве группы по умолчанию не может быть удалена.

Установка агента Пума на АРМ

Для работы системы необходимо установить агент Пумы (**Клиент**) на АРМ и обеспечить его настройку.

Последовательность установки

Для установки Клиента необходимо проделать следующие шаги:

- сформировать конфигурационный файл;
- скопировать файл дистрибутива и файл конфигурации на АРМ;
- запустить инсталлятор;
- скопировать файл конфигурации;
- перезагрузить АРМ.

Сформировать конфигурационный файл
Конфигурационный файл содержит параметры подключения к серверу Пума. Он может быть сформирован перед началом установки Клиента, тогда файл будет скопирован при инсталляции и использоваться для корректной работы службы Клиента или может быть скопирован позже, на шаге скопировать файл конфигурации. Вариант с формированием файла перед началом установки более удобный и является предпочтительным для использования.
Для корректной работы Клиента в файле необходимо задать следующие параметры:
server - ip-адрес сервера Пума, на котором запущен модуль Защита АРМ
port - порт, используемый для работы сервером Пума. По умолчанию значение данного параметра задается 5555, изменение данного значения может потребоваться в ситуации, когда сервер Пума расположен за NAT.
Скопировать файл дистрибутива и файл конфигурации на АРМ
Для запуска инсталлятора, необходимо обеспечить его доступность с АРМ. Если выбран вариант автоматического копирования файла конфигурации, то необходимо удостовериться, что файл конфигурации лежит в той же папке что и инсталлятор.
Запустить инсталлятор

Для установки Клиента необходимо запустить инсталлятор. Пользователь, от имени которого осуществляется запуск, должен обладать соответствующими правами для выполнения данной операции.

Скопировать файл конфигурации

Если на этапе формирования файла конфигурации был выбран вариант с копированием файла при установке, данный шаг необходимо пропустить, в противном случае необходимо:

- сформировать файл конфигурации в соответствии с требованиями п. Формирование файла конфигурации;
- скопировать файл конфигурации на АРМ.

Место расположения файла:

Архитектура	Путь
x86	C:\ProgramFiles\puma\config.yml
x64	C:\ ProgramFiles(x86)\puma\config.yml

Перезагрузить АРМ

Для корректного запуска службы Клиента необходимо перезагрузить АРМ.

Настройка ПО Клиента

Настройка ПО Клиента осуществляется с помощью конфигурационного файла расположенного по следующему пути:

Архитектура	Путь
x86	C:\ProgramFiles\puma\config.yml
x64	C:\ ProgramFiles(x86)\puma\config.yml

После изменений параметров конфигурационного файла необходимо перезапустить службу puma или перезагрузить АРМ.

Для настройки доступны следующие параметры конфигурационного файла:

Параметр	Назначение	Обязательный	Значение по умолчанию
server	IP-адрес сервера с установленным модулем Защита АРМ	да	-
port	порт используемый модулем Защита АРМ	да	5555
loglevel	уровень логирования	нет	info
logfile	путь к файл логирования	нет	-
processes_working_period	период опроса процессов	да	200
interfaces_working_perio	период опроса адресов	да	500

d	сетевых интерфейсов		
keepalive_period	период контроля доступности сервера	да	1000
keepalive_max	максимальное количество неудачных проверок доступности	да	10
keepalive_reconnect_timeout	период попыток переподключения к серверу	да	20000

Для корректной работы Клиента необходимо обеспечить настройку параметров server и port, изменение остальных параметров может привести к снижению производительности АРМ или модуля Защиты АРМ.

Управление списком АРМ

Обеспечивается возможность управления списком АРМ, что позволяет Администратору выбирать с какими рабочими станциями работает Модуль, назначать политики контроля, просматривать информацию о состоянии защищенности АРМ.
Для работы с определенным АРМ необходимо:

- обеспечить установку ПО Клиент Пума на АРМ;
- зарегистрировать АРМ;
- назначить политику контроля;

Если не будет пройдена процедура регистрации, то Модуль не будет взаимодействовать с АРМ
Контроль состояния защищенности АРМ осуществляется в соответствии с активной политикой контроля, которая назначается по следущему принципу: если на АРМ назначена политика, то она и является активной, если нет, то используется политика назначенная на группу, если политика не назначена ни на АРМ, ни на группу, то активная политика не назначена.

Действия

При работе со списком АРМ предусмотрен следующий набор действий:

- добавление АРМ в список новых;
- регистрация нового АРМ;
- просмотр АРМ;
- редактирование АРМ;
- деактивация АРМ;
- удаление АРМ.

Добавление АРМ в список новых

Добавление АРМ в список новый осуществляется автоматически, после установки ПО Клиент Пума, настройки конфигурационного файла и запуска сервиса или перезагрузки операционной системы рабочей станции.

Регистрация нового АРМ

Модуль обеспечивает регистрацию в двух режимах:

- регистрация АРМ Администратором;
- автоматическая регистрация АРМ.

В процессе регистрации, осуществляется назначение АРМ в группу по умолчанию. Выбор группы, в качестве группы по умолчанию осуществляется во вкладке Настройки интерфейса управления Модулем.
После прохождения регистрации АРМ готов к работе и, в случае, когда на группу по умолчанию настроена политика контроля, осуществляется контроль состояния защищенности АРМ.

Регистрация АРМ Администратором

Режим регистрации АРМ Администратором является предпочтительным для повседневной эксплуатации Модуля при котором обеспечивается небольшая защищённость системы. В данном режиме для регистрации АРМ требуется, что бы Администратор перешёл в список Новых АРМ и выбрал кнопку Зарегистрировать.

Автоматическая регистрация АРМ

Режим автоматической регистрации АРМ является более удобным в процессе внедрения системы и позволяет быстрее начать работу в условиях, когда необходимо добавить в Модуль большое число АРМ одновременно. В данном режиме, регистрация АРМ осуществляется автоматически после подключения ПО Клиент Пума к Модулю.
Включение режима осуществляется во вкладке Настройки интерфейса управления Модулем.

Просмотр АРМ

Для просмотра информации об АРМ необходимо выбрать соответствующий АРМ в списке АРМ.
Администратору доступна следующая информация:

- наименование;
- состояние;
- описание;
- имя хоста;
- имя активного пользователя;
- IP адреса сетевых интерфейсов;

- список инцидентов;
- список запущенных процессов;
- журнал зарегистрированных событий.

Часть информации отображается только для включенных рабочих станций: имя активного пользователя, IP адреса сетевых интерфейсов, список запущенных процессов.

Редактирование АРМ

При редактировании АРМ доступно изменение следующих параметров:

- наименование;
- описание;
- группа;
- политика контроля.

Наименование

Наименование служит для идентификации АРМ Администратором и передается в модуль управления политиками доступа.

Описание

Описание предназначено для хранения произвольной текстовой информации, позволяющей упростить Администратору работу со списокм АРМ в дальнейшем.

Группа

АРМ привязан к одной из групп. Непосредственно после регистрации АРМ привязывается в группу по умолчанию.

Группы служат для группировки АРМ, что бы визуально разделить АРМ разных отделов, назначения, а так же для группового назначения политики контроля на все АРМ группы.

Политика контроля

Администратор может выбрать политику контроля, на основании которой будет осуществляться контроль защищенности АРМ.

Деактивация АРМ

В ситуации, когда работа с АРМ должна быть остановлена на время, но данные, связанные с АРМ необходимо сохранить, возможна деактивация. В этом случае АРМ переводится в список Новые АРМ и ожидает повторной регистрации.

Для деактивации, необходим перейти в режим просмотра АРМ и выбрать кнопку Деактивация.

Удаление АРМ

В ситуации, когда АРМ не планируется в дальнейшем контролировать, например если он выведен из эксплуатации, модуль позволяет удалить всю информацию кроме регистрационной.
Для этого необходимо перейти в режим просмотра АРМ и выбрать кнопку Удалить.

Управление инцидентами

Модуль Защита АРМ обеспечивает возможность управления инцидентами, при этом доступны следующие возможности:

- просмотр всех инцидентов;
- просмотр инцидентов АРМ;
- снятие инцидента;
- снятие всех инцидентов АРМ;
- снятие всех инцидентов.

Просмотр всех инцидентов

Модуль позволяет просмотреть полный список инцидентов для всех АРМ заведённых в систему.
Полный список инцидентов доступен на вкладке АРМ, при этом отображается следующая информация:

- АРМ;
- политика контроля;
- режим политики контроля;
- информация о процессе;
- дата и время возникновения инцидента.

По любому из полей доступна фильтрация. Для поиска необходимо вбить искомое выражение в поле ввода **Поиск**.

Просмотр инцидентов АРМ

Модуль позволяет просматривать информацию об инцидентах для конкретного АРМ. Для этого необходимо перейти в режима просмотра информации об АРМ (см. пп.1.5). Во вкладке информацию отображается информация об инцидентах. Состав полей аналогичен полному списку инцидентов.

Снятие инцидента

Снятие определенного инцидента возможно двумя способами: из общего списка инцидентов или из списка инцидентов для определенного АРМ.
При снятии инцидента необходимо найти инцидент в таблице и выбрать кнопку **Снять инцидент**.

Снятие всех инцидентов АРМ

Для того что бы снять все инциденты АРМ, необходимо перейти в режим просмотра АРМ и в списке инцидентов выбрать кнопку **Удалить все инциденты**.

Снятие всех инцидентов

Для того что бы снять все инциденты зарегистрированные модулем, в общем списке инцидентов выбрать кнопку **Удалить все инциденты**.

Анализ регистрационной информации

Модуль обеспечивает регистрацию информации о:

- процессе настройки: добавлении или удалении АРМ, изменении политик контроля, изменения групп и т.д.
- изменении состояния АРМ: включение или выключение АРМ, формировании и снятии инцидентов.

Для просмотра событий необходимо:

- перейти в режим просмотра соответствующего элемента;
- перейти ко вкладке События;
- выбрать интересующее событие для просмотра детальной информации.

Настройка модуля

При настройке модуля доступны следующие параметры:

- включить автоматическую регистрацию АРМ;
- группа по умолчанию;
- выводить сообщение клиенту АРМ при возникновении инцидента;
- текст сообщения для пользователя АРМ.

Включить автоматическую регистрацию АРМ

Включение данного параметра позволяет автоматически проводить регистрацию новых АРМ без дополнительных действий администратора.

Группа по умолчанию

Группа по умолчанию задает группу в которую попадает АРМ после регистрации.

Выводить сообщение клиенту АРМ при возникновении инцидента

Параметр задает возможность вывода пользователю АРМ сообщения или работу в "тихом" режиме, когда пользователю не предоставляется информация об инцидентах. Работа данного режима так же зависит от версии программного обеспечения установленного в качестве агента на АРМ пользователя.

Текст сообщения для пользователя АРМ

Параметр задает текст сообщения, выводимый пользователю в случае возникновения инцидента.

Модуль Управления политиками доступа

Общая информация

Модуль Управления политиками доступа предназначен для управления политиками доступа, реагирования на инциденты АРМ и формирования правил для межсетевых экранов (**МЭ**).
Модуль обеспечивает следующий набор возможностей:

- управление политиками доступа;
- управление АРМ;
- управление МЭ;
- задание топологии;
- формирование правил.

Управление политиками доступа

Политика доступа представляет собой набор правил, задающих разрешение или запрещение сетевого доступа к информационным ресурсам со стороны АРМ или других информационных ресурсов.
Правила политики доступа формируется на основании следующих объектов:

- сервис;
- ресурс;
- АРМ;

- триггер;
- действие.

Сервис
Сервис позволяет задать объект характеризующий совокупность протоколов и портв, который может использоваться в дальнейшем для формирования политик доступа.
Ресурс
Ресурс позволяет задать совокупность адресной информации и сервисов для последующего использования в политиках доступа.
АРМ
Указание в политике доступа объекта АРМ, позволяет привязать правила политики доступа к IP-адресу сетевого интерфейса АРМ.
Триггер
Правила политики доступа формируются в не активном режиме, т.е. правила сформированы, но не применяются в процессе контроля доступа. В активный режим правила переводятся при определенных условиях, называемых триггером. Доступны следующие триггеры:

- включение;
- процесс.

Триггер **включение** срабатывает при переходе АРМ в состоянии включен.
Триггер **процесс** срабатывает при регистрации инцидента политики контроля на какой-либо процесс, при этом при настройке триггера возможно задание имени процессов для которых срабатывает триггер, что дает возможность настроить активацию правил как на любой инцидент, так и на инцидент связанный с определенным процессом.

Управление АРМ

Модуль обеспечивает получение информации об АРМ и инцидентах, связанных с ними, от одного или нескольких модулей Защиты АРМ. В модуле доступна информация об имени АРМ, возникших инцидентах, сетевых интерфейсах и назначенных IP-адресах.
Перечень модулей Защиты АРМ, с которыми работает модуль, задается в процессе настройки модуля.

Управление МЭ

Модуль обеспечивает получение информации о МЭ от одного или нескольких модулей Управления МЭ. Доступна информация об имени МЭ и составе его фильтрующих интерфейсов.

Задание топологии

Для корректной работы модуля и формирования правил, необходимо задать топологию соединений: взаимосвязи между интерфейсами АРМ и фильтрующими интерфейсами МЭ. Топология может быть задана как для каждого АРМ в отдельности, так и для группы АРМ.

Формирование правил

Формирование правил осуществляется на основании сформированных политик доступа и информации об активности, а так же инцидентах зарегистрированных на АРМ. Сформированные правила передаются для применения в модуль Управления МЭ для их выполнения.

Сервисы

Модуль предоставляет возможность Администратору управлять сервисами, объектами которые задают связь между протоколами и номерами портов для дальнейшего переиспользования в описании ресурсов.

Свойства сервисов

Данный объект имеет следующие свойства:

- имя;
- описание;
- одно или несколько правил.

Правило задает соответствие:

- протокола;
- портов.

Имя уникальное имя сервиса, используемое администратором при описании ресурсов.
Описание параметр, который позволяет сохранить произвольную текстовую информацию.
Протокол имя или номер протокола. Зарезервированы следующие слова: **TCP**, **UDP**, **ICMP**, **ANY**. Зарезервированное слово **ANY** соответствует любому протоколу.
Порт номер протокола. Может задаваться как отдельный номер, перечисление номеров или диапазон.

Действия

Управление сервисами осуществляется во вкладке Сервисы интерфейса администрирования модуля.

Доступны следующие действия при управлении сервисами:

- создание;
- просмотр;
- редактирование;
- удаление.

Создание

Для создания сервиса администратор должен выбрать кнопку **Добавить**. После чего, необходимо задать свойства объекта.
Обязательным для заполнения является свойство **Имя**.

Просмотр

Для просмотра сервиса необходимо выбрать соответствующий сервис в списке сервисов. Для просмотра доступна следующая информация:

- имя;
- описание;
- правила: порты и связанные с ними номера портов;
- события - действия Администратора по изменению объекта сервиса.

Редактирование

Для редактирования сервиса необходимо перейти в режим просмотра соответствующего сервиса и выбрать кнопку **Редактировать**.
При завершении редактировании Администратор может принять изменения, выбрав кнопку **Сохранить** или отказаться от них, выбрав кнопку **Отменить изменения**.

Удаление

Для удаления сервиса необходимо перейти в режим просмотра соответствующего сервиса и выбрать кнопку **Удалить.** В случае, если действие проводилось ошибочно, Администратор имеет возможность отказаться от действия в диалоговом окне подтверждения действия.

Ресурсы

Модуль предоставляет возможность Администратору управлять ресурсами, объектами которые задают связь между IP-адресами и сервисами для дальнейшего переиспользования в политиках доступа.

Свойства ресурсов

Данных объект имеет следующие свойства:

- имя;
- описание;
- одно или несколько правил;

Правило:

- адресная информация;
- сервисы.

Имя уникальное имя ресурса, используемое администратором при задании правил политик доступа.
Описание параметр, который позволяет сохранить произвольную текстовую информацию.
Адресная информация параметр, который задает адрес ресурса одним из следующих способов:

- IP адрес;
- IP подсеть;
- доменное имя ресурса.

Сервисы параметр, который задает один или несколько сервисов заданных администратором ранее.

Действия

Управление ресурсами осуществляется во вкладке Ресурсы интерфейса администрирования модуля.
Доступны следующие действия при управлении ресурсами:

- создание;
- просмотр;
- редактирование;
- удаление.

Создание

Для создания ресурса администратор должен выбрать кнопку **Добавить**. После чего, необходимо задать свойства объекта.
Обязательным для заполнения является свойство **Имя**.

Просмотр

Для просмотра ресурса необходимо выбрать соответствующий ресурс в списке ресурсов. Для просмотра доступна следующая информация:

- имя;

- описание;
- правила: адресная информация и связанные с ней сервисы;
- события - действия Администратора по изменению объекта ресурса.

Редактирование

Для редактирования ресурса необходимо перейти в режим просмотра соответствующего ресурса и выбрать кнопку **Редактировать**.
При завершении редактировании Администратор может принять изменения, выбрав кнопку **Сохранить** или отказаться от них, выбрав кнопку **Отменить изменения**.

Удаление

Для удаления ресурса необходимо перейти в режим просмотра соответствующего ресурса и выбрать кнопку **Удалить.** В случае, если действие проводилось ошибочно, Администратор имеет возможность отказаться от действия в диалоговом окне подтверждения действия.

Управление политиками доступа

Свойства политики доступа

Политика доступа характеризуется следующими свойствами:
- наименование;
- описание;
- правила.

Наименование уникальное имя политики, используемое администратором при задании политики доступа для АРМ или группы.
Описание параметр, который позволяет сохранить произвольную текстовую информацию.
Правила набор из одного или нескольких правил, задающих разрешенное или запрещенное сетевое взаимодействие. При задании правил используются следующие параметры:
- номер;
- действие;
- источник;
    - тип;
    - имя ресурса;
- приемник;
    - тип;
    - имя ресурса;
- триггер;

- список процессов.

Номер порядковый номер правила, позволяющий задать последовательность просмотра правил при фильтрации.

Действие свойство описывающее что будет происходить с сетевым трафиком подпадающим под правило. Допустимы следующие действия;

- пропустить;
- удалить.

Источник тип характеризует какая информация будет использоваться в качестве IP адреса источника в правиле. Допустимые варианты:

- АРМ – используются IP адреса сетевых интерфейсов АРМ;
- Ресурс – используется IP адреса ресурса.

При использовании типа источника АРМ, состав интерфейсов используемых в правиле определяется на основании топологии.

Источник имя ресурса используется только при типе источника Ресурс и задает имя ресурса, адресная информация которого будет использована в правиле.

Приемник тип характеризует какая информация будет использоваться в качестве IP адреса приемника в правиле. Допустимые варианты:

- АРМ – используются IP адреса сетевых интерфейсов АРМ;
- Ресурс – используется IP адреса ресурса.

При использовании типа приемника АРМ, состав интерфейсов используемых в правиле определяется на основании топологии.

Приемник имя ресурса используется только при типе приемника Ресурс и задает имя ресурса, адресная информация которого будет использована в правиле.

Триггер задает причину активации правила. Допустимые варианты:

- при включении – правило активируется непосредственно после включения АРМ;
- при инциденте – правило остается активным пока есть инцидент.

Список процессов задает при каких инцидентах будет активировано правило. Если список процессов пуст, то правило активируется при любом инциденте.

Действия

Администратору доступны следующие действия при работе с политиками доступа:

- создание;
- просмотр;
- редактирование;
- удаление.

Все действия над политиками контроля производятся во вкладке **Политики доступа** интерфейса управления модулем.

Создание

Администратор может создать политику доступа, для этого он должен выбрать кнопку + (Добавить), расположенную над списком политик.
При создании политики обязательным для заполнения является свойство Наименование. Все дальнейшие действия по настройке правил аналогичны действиям при редактировании политики доступа и описаны в соответствующем разделе настоящей документации.

Просмотр

Администратор может просмотреть политику доступа, для этого он должен выбрать соответствующую политику доступа в списке политик.
При просмотре будет доступна следующая информация:

- наименование;
- описание;
- список правил;
- подробная информация о каждом правиле;
- активные правила;
- зарегистрированные события.

При отображении списка правил отображается основанная информация по каждому из правил, для получения подробной информации необходимо выбрать соответствующее правило и информация будет представлена в раскрывшемся элементе списка.
Модуль отображает активные правила – правила полученные на основании подстановки в правила политики доступа информации о ресурсах и сервисах, удалении несовместимых значений, если такие есть. Примером несовместимых значений является заданные в источнике и приемнике ресурсы с разными протоколами.

Редактирование

Для редактирования политики доступа Администратор должен прейти в режим просмотра соответствующей политики и выбрать кнопку **Редактировать**.
Для редактирования доступны следующие параметры:

- наименование;
- описание;
- правила.

При редактировании наименования необходимо учитывать требование уникальности наименования.
Редактирование правил

Для редактирования правила необходимо выбрать соответствующее правило и изменить требуемые параметры правила. Все параметры, кроме списка процессов, являются параметрами, значение которых может быть выбрано только из существующих вариантов и не предусматривает возможности задания в виде текстовой строки. Список процессов задается администратором в виде текстовой строки с значениями заданными через запятую.

Редактирование последовательности правил (номера правила)

Номер правила не может быть задан в ручную, для изменения номера Администратор должен перетащить правило вверх или вниз по списку.

Удаление

Для удаления политики доступа Администратор должен перейти в режим просмотра соответствующей политики и выбрать кнопку **Удалить.** Будет выведен запрос подтверждения удаления политики доступа. Политика будет удалена после положительного ответа Администратора в запросе.

Политика доступа, назначенная на АРМ, группу или МЭ не может быть удалена.

Управление группами

Модуль позволяет создавать группы и задавать принадлежность АРМ к группе, что позволяет:

- упростить администрирование за счет визуальной группировки АРМ;
- задавать параметры не для каждого АРМ, а для всех АРМ группы.

При регистрации нового АРМ в системе, АРМ автоматически добавляется в группу по умолчанию. Выбор группы по умолчанию осуществляется в настройках модуля.

Свойства групп

Для группы можно задать следующие свойства:

- наименование;
- описание;
- политику доступа;
- топологию.

Наименование

Наименование служит для идентификации группы в процессе администрирования

Описание

Описание позволяет задать произвольную текстовую информацию, которая может помочь в дальнейшем Администратору.

Политика контроля

Политика контроля позволяет задать политику контроля для всех АРМ входящих в группу.

Топология
Топология служит для задания перечня межсетевых экранов к которым подключены АРМ данной группы.

Действия над группами

Модуль позволяет производить следующие действия:

- добавление группы;
- просмотр группы;
- редактирование группы;
- редактирование топологии группы;
- удаление группы.

Управление группами осуществляется во вкладке **Группы АРМ** интерфейса управления модулем.

Добавление группы

Для добавления группы Администратор должен выбрать кнопку **+** (**Добавить**), расположенную над списком групп.
При создании, необходимо указать наименование группы, если его не задать, то группу создать не удастся.
Так же на данном шаге можно задать описание и выбрать из выпадающего списка политику контроля, задать топологию во вкладке **топология**.

Просмотр группы

Для просмотра группы Администратор должен выбрать в списке групп соответствующее наименование.
Будет отражена следующая информация:

- наименование;
- описание;
- является ли группа, группой по умолчанию;
- привязанная к группе политика;
- список АР/М входящих в состав группы;
- топология группы;
- события связанные с настройкой данной группы.

Редактирование группы

Для редактирования группы Администратор должен перейти к просмотру группы и выбрать кнопку **Редактировать**.
Для редактирования доступны следующие поля:

- наименование;
- описание;
- привязанная к группе политика.

Редактирование привязанной к группе политики

Изменении привязанной к группе политики, приведет к тому, что для всех АРМ привязанных к данной группе будет изменена политика доступ и, в зависимости от настроек АРМ, может привести к полному изменению правил фильтрации на МЭ.

Редактирование топологии группы

Для редактирования топологии группы Администратор должен перейти во вкладку Топология и выбрать кнопку **Редактировать**. При редактировании Администратор должен выбрать в начале МЭ, к которому подключены АРМ группа, а затем фильтрующий интерфейс этого МЭ. В случае, если список фильтрующих интерфейсов МЭ пуст, означает, что **Модуль управления МЭ** еще не осуществлял подключения к МЭ и не получал информацию о составе фильтрующих интерфейсов.
Если используется конфигурация с несколькими МЭ и в топологии группы необходимо предусмотреть подключения к нескольким МЭ, Администратор должен выбрать кнопку **+** (**Добавить**) и провести заполнение строки аналогичным образом.
Для удаления строки топологии группы Администратор должен выбрать кнопку **Удалить.**

Удаление группы

Для удаления группы Администратор должен перейти к просмотру группы и выбрать кнопку **Удалить**.
Группа, выбранная в настройках модуля в качестве группы по умолчанию не может быть удалена.

Управление списком АРМ

Обеспечивается возможность управления списком АРМ, что позволяет Администратору выбирать с какими рабочими станциями работает Модуль, назначать политики доступа, просматривать информацию о состоянии защищенности АРМ.
Для работы с определенным АРМ необходимо обеспечить настройку модуля на получение информации от одного или нескольких Модулей Защиты АРМ. Подробная информация о настройке описана в разделе **Настройка**. АРМ зарегистрированные в модуле Защиты АРМ будут автоматически добавлены в список АРМ Модуля управления политиками доступа.

Действия

При работе со списком АРМ предусмотрен следующий набор действий:

- просмотр АРМ;
- редактирование АРМ;
- настройка топологии;
- удаление АРМ.

Все действия над АРМ осуществляются во вкладке **АРМ** интерфейса управления Модулем.

Просмотр АРМ

Для просмотра информации об АРМ необходимо выбрать соответствующий АРМ в списке АРМ.
Администратору доступна следующая информация:

- наименование;
- статус;
- описание;
- имя хоста;
- имя группы;
- политика АРМ;
- политика ;группы
- имя модуля Защиты АРМ;
- IP адреса АРМ;
- события;
- топология;
- активные правила.

Редактирование АРМ

При редактировании АРМ доступно изменение следующих параметров:

- группа;
- политика доступа.

Группа
АРМ привязан к одной из групп. Непосредственно после добавления АРМ привязывается в группу по умолчанию.
Группы служат для группировки АРМ, что бы визуально разделить АРМ разных отделов, назначения, а так же для группового назначения политики доступа на все АРМ группы.
Политика
Администратор может выбрать политику доступа, на основании которой будет осуществляться контроль защищенности АРМ.

Настройка топологии

Для редактирования топологии АРМ Администратор должен перейти в режим просмотра соответствующего АРМ, перейти во вкладку Топология и выбрать кнопку **Редактировать**. При редактировании Администратор должен:

1. выбрать сетевой интерфейс АРМ для которого будет настраиваться связь;
2. выбрать МЭ, к которому подключен АРМ;
3. выбрать фильтрующий интерфейс этого МЭ.

В случае, если список фильтрующих интерфейсов МЭ пуст, означает, что **Модуль управления МЭ** еще не осуществлял подключения к МЭ и не получал информацию о составе фильтрующих интерфейсов.
Если используется конфигурация с несколькими МЭ и в топологии АРМ необходимо предусмотреть подключения к нескольким МЭ, Администратор должен выбрать кнопку **+** (**Добавить**) и провести заполнение в соответствии с пп 2-3.
Для удаления строки топологии группы Администратор должен выбрать кнопку **Удалить.**

Удаление АРМ

В ситуации, когда АРМ не планируется в дальнейшем контролировать, например если он выведен из эксплуатации, модуль позволяет удалить всю информацию кроме регистрационной.
Для этого необходимо перейти в режим просмотра АРМ и выбрать кнопку Удалить.

Управление списком МЭ

Модуль обеспечивает возможность управления списком МЭ.
Для добавления МЭ в Модуль необходимо настроить связь между Модулем управления политиками доступа и Модулем управления МЭ. Связь настраивается на стороне модуля управления МЭ. Подробная информация о настройке описана в соответствующем разделе.

Действия

При управлении списком МЭ доступны следующие действия:

- просмотр МЭ;
- редактирование МЭ.

Просмотр МЭ

При просмотре МЭ доступна следующая информация:

- наименование;

- статус;
- описание;
- сервис управления МЭ;
- политика доступа;
- дата создания;
- правила;
- события.

Для просмотра МЭ Администратор должен выбрать соответствующий МЭ в списке.

Редактирование МЭ

Для редактирования МЭ Администратор должен прейти в режим просмотра соответствующего МЭ и выбрать кнопку **Редактировать**.
Для редактирования доступен параметр **Политика доступа**.

Настройка модуля

Администратор имеет возможность обеспечить настройку следующих параметров Модуля управления политиками доступа:

- модули Защиты АРМ;
- группа по умолчанию.

Для просмотра настроек Администратор должен перейти во вкладку **Настройки** интерфейса управления модуля управления политиками доступа.
Для редактирования настроек администратор должен прейти в режим просмотра настроек и выбрать кнопку **Редактировать**. В режиме редактирования Администратор может сохранить настройки с помощью кнопки **Сохранить** или отменить внесенные в процессе редактирования изменения с помощью кнопки **Отменить**.

Модули Защиты АРМ

Данная настройка позволяет задать список модулей Защиты АРМ от которых будет поступать информация об АРМ, их состоянии и возникающих инцидентах.
Для добавления Модуля Защиты АРМ необходимо ввести полное имя сервиса в строку ввода группы **Сервисы Защиты АРМ** и выбрать кнопку **Подтвердить**.
Для удаления Модуля Защиты АРМ необходимо выбрать кнопку **Удалить** в столбце **Действия** для соответствующей модулю защиты арм строке таблицы.

Модуль управления МЭ

Общая информация

Модуль **Управления межсетевыми экранами** обеспечивает ведение списка МЭ, управления правилами фильтрации установленными на МЭ. Поддерживается возможность управления МЭ ССПТ-4А1, ССПТ-4В1.
Модуль обеспечивает выполнение следующих действий:

- управление учетными данным;
- управление списком МЭ;
- формирование правил фильтрации;
- контроль состояния МЭ;
- управление правилами фильтрации на МЭ.

Управление учетными данным

Модуль обеспечивает возможность управления набором из имени пользователя и пароля для обеспечения дальнейшего управления межсетевыми экранами.

Управление списком МЭ

Модуль обеспечивает управление списком МЭ, при этом хранится информация необходимая для обеспечения доступа к управляющим интерфейсам МЭ, ссылки на учетные данные, вспомогательная информация.

Формирование правил фильтрации

Модуль обеспечивает формирование правил фильтрации из правил полученных от модуля управления политиками доступа. Правила транслируются в формат правил МЭ ССПТ. Обеспечивается проверка корректности правил.

Контроль состояния МЭ

Модуль обеспечивает периодический опрос состояния МЭ, получение справочной информации о составе технических средств, а так же о состоянии контролируемых параметров, таких как загрузка процессора, памяти, носителей информации.
В случае, когда МЭ не доступен или попытка аутентификации с указанными для соответствующего МЭ учетными данными оказалась не успешной, формируется информация о проблемах с доступом к оборудованию.

Управление правилами фильтрации на МЭ

Модуль обеспечивает загрузку правил фильтрации на МЭ, удаление устаревших правил, контроль соответствия правил на МЭ правилам политики доступа.

Управление учетными данными

Модуль обеспечивает возможность сохранения именованного объект со следующими свойствами:

- наименование;
- описание;
- имя пользователя;
- пароль.

Действия

Для управления учетными данными доступны следующие действия:

- добавление;
- просмотр;
- редактирование;
- удаление.

Все действия над учетными данными осуществляются во вкладке **Учетные данные интерфейса** управления Модулем.

Добавление

Для добавления учетных данных Администратор должен выбрать кнопку **Добавить** и ввести обязательные для заполнения параметры: наименование, имя пользователя и выбрать кнопку **Сохранить**.

Просмотр

Для просмотра учетных данных Администратор должен выбрать соответствующие учетные данные в списке. Для просмотр доступна следующая информация:

- наименование;
- описание;
- имя пользователя.

Редактирование

Для редактирования учетных данных Администратор должен прейти в режим просмотра соответствующих учетных данных и выбрать кнопку **Редактировать**.

Для Редактирования доступны следующие параметры:

- наименование;
- описание;
- имя пользователя;
- пароль.

При изменении пароля необходимо выбить подтверждение пароля.

Удаление

Администратор имеет возможность удалить учетные данные, для этого он должен перейти в режим просмотра соответствующих учетных данных и выбрать кнопку **Удалить**.

Управление списком МЭ

Модуль обеспечивает управление списком МЭ. Администратору доступны действия по добавлению, просмотру, редактированию и удалению МЭ.
Для работы с МЭ должна быть заполнена следующая информация:

- наименование;
- описание;
- хост FNP (IP адрес управляющего интерфейса МЭ);
- порт FNP (по умолчанию 2434);
- порт HTTPS (по умолчанию 443);
- порт SSH (по умолчанию 22);
- учетные данные для чтения;
- учетные данные для управления;
- мониторинг (по умолчанию включен).

Контроль состояния МЭ

После запуска модуля или добавления МЭ в список, в ситуации, когда параметр Мониторинг находится во включенном состоянии, Модуль обеспечивает подключение к МЭ с использованием учетных данных для чтения и получения информации о состоянии устройства. Шаг получения информации выполняется периодически.
Модуль обеспечивает индикацию состояния с помощью цветовых маркеров:

- серого цвета – мониторинг отключен;
- красного цвета – ошибка подключения;
- желтого цвета – ошибка аутентификации пользователя;
- зеленого цвета – готов к работе: МЭ исправен, соединение установлено успешно.

Формирование правил фильтрации

Формирование правил фильтрации осуществляется после перехода МЭ в состояние готов к работе. Формирование правил фильтрации осуществляется в следящей последовательности:

- формирование правил фильтрации **По умолчанию** – правила обеспечивающие возможность работы Модуля с МЭ;
- запрос, получение и формирование правил политики доступа для МЭ – правила, которые должны быть загружены на МЭ независимо от состава и состояния АРМ для обеспечения корректной работы сети;
- получение и формирование правил политики доступа для АРМ – правила формируемые при запуске АРМ и переходе его в состояние активен;
- получение и формирование правил политики доступа для АРМ в случае инцидента – правила обеспечивающие изменение доступности ресурсов сети при возникновении инцидента;
- удаление правил фильтрации при остановке модуля – обеспечивается удаление только при корректном выключении модуля.

Модуль формирует три группы правил: по умолчанию, для МЭ и динамические правила для АРМ.

Управление правилами фильтрации

Модуль обеспечивает загрузку сформированных правил фильтрации на МЭ, при этом осуществляется хранение правил фильтрации в модуле, а так же хранение соответствия правил фильтрации правилам политики доступа, что позволяет проводить:

- удаление или редактирование только необходимых правил, а не всего набора;
- проверку корректности набора правил фильтрации на МЭ.

Ограничения тестовой версии

Тестовая версия предназначена для ознакомления с функциональными возможностями системы и ее интерфейсом управления.
Не допускается использование тестовой версии Системы для других целей.
Тестовая версия имеет следующие ограничения:

1. Фиксированный IP адрес

Для управления системой задан IP адрес по умолчанию: 192.168.7.1. Данный адрес не может быть изменен. Исходя из этого необходимо учесть и ограничения накладываемые на конфигурационный файл ПО клиента, устанавливаемого на АРМ: в качестве IP адреса сервера в конфигурационном файле должен быть задан фиксированный адрес, указанный выше.

2. Система предоставляется в тестирование без МЭ

В виду того, что система обеспечивает управления МЭ стороннего производителя, ООО «ЦРП» не может предоставить в пользование физический или виртуальный МЭ для задач тестирования данного функционала.